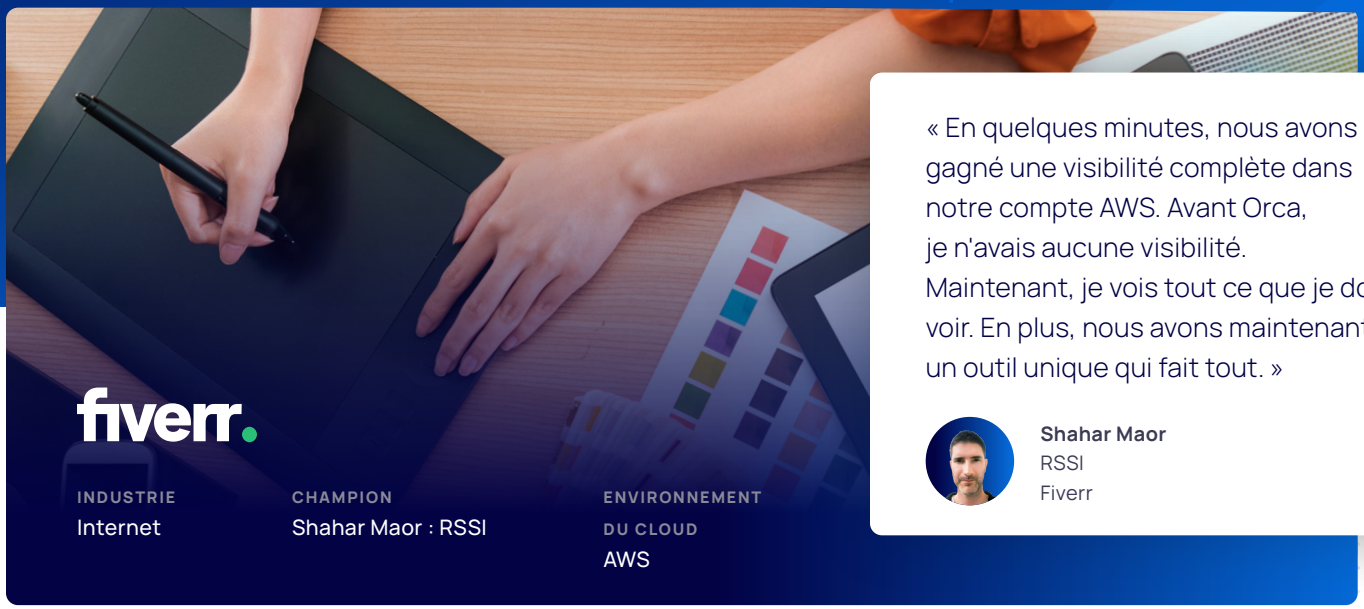
Fiverr remplace plusieurs outils par Orca Security pour obtenir une visibilité immédiate et complète sur ses actifs AWS



fiverr.

INDUSTRIE
Internet

CHAMPION
Shahar Maor : RSSI

ENVIRONNEMENT DU CLOUD
AWS

« En quelques minutes, nous avons gagné une visibilité complète dans notre compte AWS. Avant Orca, je n'avais aucune visibilité. Maintenant, je vois tout ce que je dois voir. En plus, nous avons maintenant un outil unique qui fait tout. »

Shahar Maor
RSSI
Fiverr

Défis de la sécurité du cloud

- Aucun moyen de comprendre le contexte complet de ce qui se passait dans AWS ;
- AWS et les outils open source étaient chronophages et inefficaces ;
- Inondé de milliers d'alertes que personne n'a le temps d'examiner.

Résultats de la sécurité du cloud

- Une inspection approfondie du cloud identifie les logiciels malveillants, les mauvaises configurations, les « secrets », les mots de passe faibles et les informations personnelles ;
- Permet d'économiser des heures de travail par semaine, moins dépendant des DevOps et aucun actif négligé ;
- Les alertes sont désormais hiérarchisées en fonction du contexte environnemental, poussées sur Slack et résolues.

L'expansion mondiale rapide exige la sécurité du cloud AWS à grande échelle

Fondée en 2010 et basée à Tel Aviv, Fiverr (NYSE : FVRR) est un vaste marché mondial en ligne de services indépendants. Sa plateforme permet aux indépendants d'offrir des services aux clients du monde entier tout en aidant les entreprises à trouver les services dont elles ont besoin, en naviguant simplement dans un catalogue ou en effectuant une recherche.

La plateforme Fiverr a servi plus de 5,5 millions d'entreprises et a facilité plus de 50 millions de transactions. Compte tenu du nombre de personnes qui accèdent à la plateforme, il est essentiel de maintenir une infrastructure AWS sécurisée.

Shahar Maor, le RSSI chez Fiverr, savait que la sécurisation des environnements du cloud était une entreprise complexe

« J'ai été le premier professionnel de la sécurité à plein temps que Fiverr a embauché. » explique Shahar Maor. « Bien que la sécurité ait déjà été profondément ancrée dans la culture de Fiverr »

L'analyse initiale de l'infrastructure AWS qu'avait effectuée Maor révélait des possibilités d'attaques de vecteurs externes, de pirates informatiques, de bots malveillants et de virus. Mais il savait que les environnements cloud recelaient des recoins cachés.

« Les organisations présument souvent qu'il suffit de protéger le périmètre et l'infrastructure du cloud est souvent négligée » explique Maor. « Vous ne réfléchissez pas au fait qu'une mauvaise configuration de la plateforme elle-même pourrait être un problème. C'est une idée fausse que de penser que si vous disposez d'une infrastructure native du cloud, vous la voyez plus clairement. La sécurisation des environnements cloud est très complexe. »

Maor s'inquiétait des mots de passe faibles qu'employaient certains utilisateurs de la plateforme et de la possibilité que des logiciels malveillants soient exécutés sur les serveurs AWS. « Lorsque j'ai initialement cartographié les risques par rapport à nos actifs de grande valeur, il était évident que nous avions des angles morts. De plus, je passais beaucoup trop de temps à surveiller manuellement les actifs, en particulier les compartiments S3 AWS, pour m'assurer que rien n'était exposé. C'était très fastidieux. »

La solution idéale devait fournir une visibilité approfondie sur tous les actifs AWS

Maor entreprit de trouver une solution de sécurité cloud AWS avec ces exigences à l'esprit. « Il nous fallait une solution qui pouvait fournir une visibilité complète sur notre environnement AWS tout en recherchant les logiciels

> « Les organisations présument souvent qu'il suffit de protéger le périmètre et l'infrastructure du cloud est souvent négligée. »
>
> **Shahar Maor**
> RSSI
> Fiverr

malveillants, identifiant les mauvaises configurations et protégeant les données personnelles d'identification. »

L'outil de sécurité cloud optimal serait une solution qui couvrirait tous les risques identifiés et qui fournirait des informations et une valeur exploitables au service informatique, aux DevOps et à l'ingénierie. Les objectifs et les exigences supplémentaires d'une solution de sécurité AWS étaient les suivants :

- Aucun agent à gérer
- Visibilité complète ; aucun actif négligé
- Rechercher et protéger les informations personnelles
- Contrôler l'état des serveurs
- Identifier les mots de passe faibles
- Trouver les mauvaises configurations
- Rechercher des « secrets » laissés dans le code existant
- Surveiller les actifs exposés, comme les compartiments S3
- Simplifier la conformité à la réglementation, notamment concernant la PCI

> « Il nous fallait une solution qui pouvait fournir une visibilité complète sur notre environnement AWS tout en recherchant les logiciels malveillants, identifiant les mauvaises configurations et protégeant les données personnelles d'identification. »
>
> **Shahar Maor**
> RSSI
> Fiverr

Les outils natifs, les analyseurs existants et les approches basées sur des agents ne feraient pas l'affaire

Maor comprit que l'environnement cloud de Fiverr présentait des exigences uniques auxquelles de nombreux outils de sécurité cloud disponibles ne pouvaient pas répondre. « Les outils natifs comme Amazon Inspector ou GuardDuty fournissent des fonctionnalités de base, mais ils n'établissent pas de corrélation logique avec les incidents ou ne comprennent pas complètement le contexte de ce qui se passe. Vous devez toujours analyser les journaux et investir plus de temps pour comprendre les données. Ils sont mieux que rien, comme les outils Open Source, mais ils n'offrent pas de flux de travail permettant de livrer les résultats à vos équipes pour qu'elles prennent des mesures. »

Maor ajoute que les scanners et les outils basés sur des agents sont très limités. « Certains outils commerciaux peuvent analyser un serveur pour détecter ses vulnérabilités, mais c'est tout. En bref, ces outils demandent plus de travail et ils nécessitent une expertise des domaines et des outils supplémentaires pour fonctionner efficacement. »

L'outil unique qui fait tout

Maor considère Orca Security comme un guichet unique pour réduire les risques qui se cachent au sein de l'infrastructure AWS de Fiverr. « Orca fournit une solution holistique pour atténuer les risques dans le centre de données de Fiverr. La méthode unique qu'utilise Orca pour analyser AWS s'est avérée la plus appropriée pour nous et a convaincu notre équipe DevOps. En plus, nous avons maintenant un outil unique qui fait tout. »

Orca SideScanning™ élimine le besoin d'agents et n'affecte pas les performances

L'exécution des agents de sécurité sur des machines virtuelles individuelles nécessite une gestion et une administration continues. Au lieu d'utiliser cette approche, Orca fonctionne comme un service SaaS avec un accès en lecture seule au stockage de blocs d'exécution des charges de travail AWS, Azure ou GCP du client. Elle reconstruit les bits et les octets à partir de l'instantané pour produire une vue virtuelle et en lecture seule des systèmes d'exploitation, des applications et des données, puis les analyse pour détecter les vulnérabilités et les risques.

« La plateforme Orca est extrêmement légère et n'affecte le réseau d'aucune manière » explique Maor. « Vous gagnez de la visibilité sans aucune interférence avec l'instance elle-même. Orca crée simplement une copie, la lit, analyse les conclusions, puis les présente dans un tableau de bord pour que nous puissions les examiner. »

Des alertes significatives et de haute valeur, sans le bruit

La technologie brevetée SideScanning™ d'Orca Security découvre automatiquement chaque actif dans l'environnement d'un client. Cela donne aux équipes de sécurité une visibilité immédiate sur les ressources compromises, les vulnérabilités, les logiciels malveillants et les mauvaises configurations. En combinant ces informations avec des métadonnées environnementales, Orca envoie des alertes dans le contexte afin de hiérarchiser efficacement les priorités.

« Orca envoie des alertes significatives et exploitables en temps réel pour attirer notre attention sur une menace, au lieu de créer de nombreux journaux et des milliers d'alertes que personne ne lit ou n'a le temps d'examiner. Nous recevons des alertes Slack sur chaque conclusion critique. Si Orca découvre une nouvelle vulnérabilité, nous le savons immédiatement. »

Simplifier la conformité à la réglementation

De plus, Orca Security simplifie la conformité à la réglementation. « La norme PCI nous demande d'analyser notre environnement, mais comme il n'utilise pas de serveurs, cela présente des difficultés uniques. La solution d'Orca nous permet d'analyser les conteneurs EKS et ECS et de bien répondre aux exigences de la PCI. »

« Orca Security envoie des alertes significatives et exploitables en temps réel pour attirer notre attention sur une menace. Si Orca découvre une nouvelle vulnérabilité, nous le savons immédiatement. »

Shahar Maor
RSSI
Fiverr

Visibilité complète, effort minimal

Peu après l'implémentation, Orca a découvert des vulnérabilités que l'équipe de Maor a pu résoudre. « Orca Security fournit des informations utiles et la capacité d'étendre la posture de sécurité de Fiverr. Avant Orca, je n'avais aucune visibilité. Maintenant, je vois tout ce que je dois voir. »

Pour Maor, cela confirmait qu'Orca Security répondait à tous ses besoins. « J'ai toujours Orca et un CASB implémentés sur le système, mais lors de ma prochaine actualisation, je supprimerai le CASB parce qu'il ne fournit aucune information » dit-il. « Je m'appuierai uniquement sur Orca pour surveiller l'environnement de production AWS, de bout en bout. »

Économiser des heures par semaine, pas besoin de compter sur DevOps

Maor passe maintenant deux fois moins de temps sur la sécurité du cloud. « Orca élimine chaque semaine des heures de travail de maintenance et d'administration de la sécurité du cloud. En plus, je n'ai pas besoin des DevOps pour obtenir de l'assistance. »

En prime, Maor peut compter sur l'équipe d'Orca Security pour obtenir des recommandations et des conseils d'experts. « L'équipe Orca possède une vaste expérience et des connaissances pratiques en matière de sécurité, ainsi qu'une agilité et une flexibilité incroyables. Nous bénéficions déjà énormément d'Orca et nous sommes heureux de l'adopter comme principale plateforme de sécurité AWS et de grandir avec elle. »

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, 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]