Le Partenariat

Snyk et SentinelOne s'associent pour fournir une visibilité accrue des risques applicatifs, de la phase de construction à la phase d'exécution.

Pitch

La protection en temps réel de SentinelOne, combinée au contexte de construction de Snyk, rationalise la réponse aux incidents et aide à résoudre les problèmes d'exécution à la source. L'intégration de SentinelOne et Snyk combine la CWPP (Cloud Workload Protection Platform) en temps réel de SentinelOne avec l'analyse des vulnérabilités des images de conteneurs de Snyk. Les clients utilisent ces informations pour rationaliser l'analyse et résoudre les problèmes de sécurité (impactant les opérations) dès les premières étapes du processus de développement. Ce retour d'information en boucle fermée conduit à des applications plus sécurisées en production.

Pourquoi avons-nous formé ce partenariat ?

Les équipes de sécurité ont généralement une visibilité sur les menaces en temps réel, mais manquent de contexte en ce qui concerne les vulnérabilités dans le code et les images de conteneurs. À l'inverse, les développeurs ont une vue sur les vulnérabilités du code et de la phase de construction, mais n'ont aucune visibilité sur les menaces en temps réel et les environnements déployés. Nous nous associons pour fusionner ces deux perspectives tout au long du cycle de vie des applications afin que les problèmes à haut risque puissent être rapidement éliminés et qu'aucune équipe ne perde de temps sur des problèmes de moindre importance. Cela permet aux équipes de sécurité cloud, de sécurité applicative et aux développeurs de collaborer plus efficacement et de s'attaquer à la cause profonde de ces problèmes.

Proposition de valeur conjointe

Le produit de sécurité des charges de travail cloud Singularity de SentinelOne détecte en temps réel les menaces d'exécution, y compris les ransomwares, les exploits zero-day et les attaques sans fichier, et automatise les actions de réponse. Snyk aide les développeurs à trouver, prioriser et corriger les vulnérabilités dans leurs applications. En combinant les deux, les équipes de sécurité et les développeurs peuvent désormais :

- Corréler automatiquement les vulnérabilités découvertes par Snyk lors de la phase de construction aux menaces d'exécution dans SentinelOne pour que les équipes CloudSec, AppSec et les développeurs puissent collaborer pour trouver et corriger les vulnérabilités ;
- Identifier plus rapidement la cause profonde des menaces d'exécution associées aux applications en identifiant les vulnérabilités exploitables associées ;
- Remédier à la cause profonde des menaces à leur source ;
- Chasser proactivement les menaces et automatiser les actions de réponse pour arrêter leur propagation;
- Tirer parti des retours d'information continus et de la surveillance pour empêcher les vulnérabilités d'atteindre la production et vérifier les mauvaises configurations en phase d'exécution pour créer un environnement de production plus sécurisé.

Cas d'utilisation

1 **Investigation / Réponse aux incidents**
L'intégration combine la visibilité des vulnérabilités au moment de la construction des images de conteneurs de Snyk avec les menaces en temps réel détectées par SentinelOne CWPP, afin que les clients puissent mieux gérer les risques et corriger les problèmes critiques.

2 **Contexte de vulnérabilité au moment de la construction**
Snyk Container aide à sécuriser les images de conteneurs en permettant aux développeurs et aux équipes DevOps de trouver, prioriser et corriger les vulnérabilités tout au long du cycle de vie du développement logiciel (SDLC), avant que les charges de travail n'atteignent la production. Avec Snyk Container, vous pouvez corriger automatiquement les images de base, minimiser l'exposition et réduire le temps de correction, et surveiller en continu pour protéger l'image après l'analyse initiale.

3 **Chasse aux menaces**
Les praticiens de la sécurité peuvent chasser proactivement les menaces dans le Data Lake Singularity de SentinelOne, qui comprend des détails ingérés de Snyk Container. Par exemple, des menaces d'exécution précédemment identifiées peuvent avoir été corrélées à une vulnérabilité d'image spécifique ; un chasseur de menaces peut rechercher cette vulnérabilité pour identifier tout risque supplémentaire.