Die Partnerschaft

EXCLUSIVE NETWORKS | nuaware An Exclusive Networks Company

Snyk und SentinelOne arbeiten zusammen, um eine verbesserte Transparenz von Anwendungsrisiken von der Entwicklungsphase bis zur Laufzeit zu gewährleisten.

Elevator Pitch

Echtzeitschutz zur Laufzeit von SentinelOne plus Build-Time-Kontext von Snyk optimieren die Incident Response und helfen dabei, Laufzeitprobleme an der Basis zu lösen.
Die Integration von SentinelOne und Snyk kombiniert SentinelOne's Echtzeit-CWPP (Cloud Workload Protection Platform) mit der Schwachstellenanalyse von Snyk für Container-Images. Kunden nutzen diese Informationen, um die Analyse zu optimieren und Sicherheitsprobleme (die den Betrieb beeinträchtigen) frühzeitig im Entwicklungsprozess zu lösen. Dieses geschlossene Feedback führt zu sichereren Anwendungen in der Produktion.

Warum sind wir eine Partnerschaft eingegangen?

Sicherheitsteams haben typischerweise Einblick in Laufzeitbedrohungen, aber es fehlt ihnen der Kontext in Bezug auf Schwachstellen in Code und Container-Images. Umgekehrt haben Entwickler Einblick in Code- und Build-Time-Schwachstellen, aber keinen Einblick in Laufzeitbedrohungen und bereitgestellte Umgebungen. Wir sind eine Partnerschaft eingegangen, um diese beiden unterschiedlichen Perspektiven über den gesamten Anwendungslebenszyklus hinweg zu vereinen, damit hochriskante Probleme schnell beseitigt werden können und kein Team Zeit mit unbedeutenden Problemen verschwendet.
Dies ermöglicht es, dass Cloud-Sicherheits-, Anwendungssicherheits- und Entwicklerteams, effektiver zusammenarbeiten und die Grundursache dieser Probleme beheben.

Gemeinsames Wertversprechen

Das Produkt Singularity Cloud Workload Security von SentinelOne erkennt Laufzeitbedrohungen, einschließlich Ransomware, Zero-Day-Exploits und dateifreier Angriffe, in Echtzeit und automatisiert Reaktionsmaßnahmen. Snyk hilft Entwicklern, Schwachstellen in ihren Anwendungen zu finden, zu priorisieren und zu beheben. Durch die Kombination beider Lösungen können Sicherheits- und Anwendungsentwickler nun

- automatisch Schwachstellen, die von Snyk zur Build-Time entdeckt werden, mit Laufzeitbedrohungen in SentinelOne korrelieren, sodass CloudSec, AppSec und Entwickler zusammenarbeiten können, um Schwachstellen zu finden und zu beheben;
  die Ursache von Laufzeitbedrohungen schneller identifizieren, indem sie ausnutzbare Schwachstellen im Zusammenhang mit den Anwendungen erkennen;
- die Ursache von Bedrohungen an der Basis bereits beheben;
- proaktiv nach Bedrohungen suchen und Reaktionsmaßnahmen automatisieren, um die Ausbreitung zu stoppen und
- kontinuierliches Feedback und Monitoring zu nutzen, um zu verhindern, dass Schwachstellen in die Produktion gelangen, und um Fehlkonfigurationen während der Laufzeit zu überprüfen, um eine sicherere Produktionsumgebung aufzubauen.

Anwendungsfälle

1 **Untersuchung /Reaktion auf Vorfälle**
Die Integration kombiniert die Sichtbarkeit von Schwachstellen zur Build-Time innerhalb von Container-Images von Snyk mit Laufzeitbedrohungen, die von SentinelOne CWPP erkannt werden, sodass Kunden Risiken besser managen und kritische Probleme beheben können.

2 **Schwachstellenkontext zur Build-Time**
Snyk Container hilft dabei, Container-Images zu sichern, indem es Entwicklern und DevOps ermöglicht, Schwachstellen während des gesamten SDLC zu finden, zu priorisieren und zu beheben, bevor Arbeitslasten in die Produktion gelangen. Mit Snyk Container können Sie Basis-Images automatisch beheben, die Exposition minimieren und die Zeit zur Behebung verkürzen sowie kontinuierlich überwachen, um das Image nach dem initialen Scan zu schützen

3 **Bedrohungssuche**
Sicherheitsexperten können proaktiv nach Bedrohungen im SentinelOne Singularity Data Lake suchen, der Details von Snyk Container enthält. Zum Beispiel können zuvor identifizierte Laufzeitbedrohungen mit einer spezifischen Image-Schwachstelle korreliert worden sein; ein Sicherheitsexperte kann nach dieser Schwachstelle suchen, um weiteres Risiko zu identifizieren.