De Samenwerking

Snyk en SentinelOne werken samen om verbeterde zichtbaarheid te bieden in applicatierisico's van bouwfase tot runtime.

Liftpitch

Realtime runtime bescherming van SentinelOne, gecombineerd met build-time context van Snyk, stroomlijnt de incidentrespons en helpt om runtime-problemen bij de bron op te lossen. De integratie van SentinelOne en Snyk combineert SentinelOne's realtime CWPP (Cloud Workload Protection Platform) met Snyk containerafbeelding kwetsbaarheidsanalyse. Klanten gebruiken deze informatie om de analyse te stroomlijnen en beveiligingsproblemen (die operationele processen beïnvloeden) vroeg in het ontwikkelingsproces op te lossen. Deze gesloten feedbackloop leidt tot veiligere applicaties in productie.

Waarom zijn we een samenwerking aangegaan?

Beveiligingsteams hebben doorgaans zicht op runtime-bedreigingen, maar missen context als het gaat om kwetsbaarheden in code en containerafbeeldingen. Omgekeerd hebben ontwikkelaars inzicht in code en kwetsbaarheden tijdens het bouwproces, maar geen zicht op runtime-bedreigingen en uitgerolde omgevingen. We zijn een samenwerking aangegaan om deze twee verschillende perspectieven gedurende de levenscyclus van de applicatie te combineren, zodat hoog-risico problemen snel kunnen worden opgelost en geen van beide teams tijd verspilt aan problemen van weinig belang. Dit stelt teams voor cloudbeveiliging, applicatiebeveiliging en ontwikkelaars in staat om effectiever samen te werken en de oorzaak van deze problemen aan te pakken.

Gezamenlijke Waardepropositie

Het Singularity Cloud Workload Security-product van SentinelOne detecteert realtime dreigingen, waaronder ransomware, zero-day exploits en fileless aanvallen, en automatiseert responsacties. Snyk helpt ontwikkelaars om kwetsbaarheden in hun applicaties te vinden, prioriteren en verhelpen. Door de twee te combineren, kunnen beveiligings- en applicatieontwikkelaars nu:

Kwetsbaarheden die door Snyk tijdens het bouwproces zijn ontdekt automatisch correleren met runtime-bedreigingen in SentinelOne, zodat CloudSec-, AppSec- en ontwikkelaars teams samen kunnen werken om kwetsbaarheden te vinden en te verhelpen;

- Sneller de oorzaak van runtime-bedreigingen identificeren die verband houden met de apps door exploiteerbare kwetsbaarheden te identificeren die ermee verband houden;
- De oorzaak van bedreigingen bij de bron verhelpen
- Proactief op zoek gaan naar bedreigingen en automatiseren van responsacties om de verspreiding te stoppen
- Continue feedback en monitoring benutten om te voorkomen dat kwetsbaarheden in productie komen en misconfiguraties in runtime te verifiëren om een veiliger productieomgeving op te bouwen.

Gebruiksgevallen

1 Onderzoek / Incidentrespons
De integratie combineert zichtbaarheid van kwetsbaarheden tijdens het bouwproces binnen containerafbeeldingen van Snyk met runtime-bedreigingen gedetecteerd door SentinelOne CWPP, zodat klanten risico's beter kunnen beheren en kritieke problemen kunnen oplossen.

2 Kwetsbaarheidscontext tijdens het bouwproces
Snyk Container helpt bij het beveiligen van containerafbeeldingen door ontwikkelaars en DevOps in staat te stellen kwetsbaarheden te vinden, prioriteren en verhelpen gedurende de gehele SDLC, voordat workloads in productie gaan. Met Snyk Container kunt u basisafbeeldingen automatisch herstellen, blootstelling minimaliseren en de tijd om te herstellen verkorten, en continu monitoren om de afbeelding te beschermen na de initiële scan.

3 Threat Hunting
Beveiligingsprofessionals kunnen proactief op zoek gaan naar bedreigingen binnen de SentinelOne Singularity Data Lake, die details bevat die zijn verkregen uit Snyk Container. Bijvoorbeeld, eerder geïdentificeerde runtime-bedreigingen kunnen zijn gecorreleerd met een specifieke afbeelding kwetsbaarheid; een threat hunter kan naar die kwetsbaarheid zoeken om verder risico te identificeren.