The Partnership

EXCLUSIVE NETWORKS | nuaware An Exclusive Networks Company

Snyk and SentinelOne partner to provide enhanced visibility into application risks from build time to runtime

Elevator Pitch

Real-time runtime protection from SentinelOne plus build-time context from Snyk streamlines incident response and helps solve runtime issues at the source. The SentinelOne and Snyk integration combines SentinelOne's real-time CWPP (Cloud Workload Protection Platform) with Snyk container image vulnerability scanning. Customers use this info to streamline analysis and resolve security issues (that are impacting operations) early during the development process. This closed-loop feedback leads to more secure applications in production.

Why did we partner?

Security teams typically have visibility into runtime threats, but lack context when it comes to vulnerabilities in code and container images. Conversely, developers have a view into code and build-time vulnerabilities, but no insight into runtime threats and deployed environments. We are partnering to fuse these two disparate views throughout the application lifecycle so that high risk issues can be quickly eliminated and neither team wastes time on issues of little importance. This enables cloud security, application security and developer teams to more effectively collaborate and address the root cause of these issues.

Joint Value Prop

SentinelOne's Singularity Cloud Workload Security product detects runtime threats, including ransomware, zero-day exploits, and fileless attacks, in real-time, and automates response actions. Snyk helps developers find, prioritize, and fix vulnerabilities in their applications. Combining the two, security and application developers can now:

- Automatically correlate vulnerabilities discovered by Snyk at build time to runtime threats in SentinelOne so CloudSec, AppSec and Developers can all collaborate to find and fix vulnerabilities;
- More quickly identify the root cause of runtime threats associated with the apps by identifying exploitable vulnerabilities associated with them;
- Remediate the root cause of threats at their source;
- Proactively hunt for threats and automate response actions to stop the spread; and,
- Leverage continuous feedback and monitoring to prevent vulnerabilities from reaching production and verify misconfigurations in runtime to build a more secure production environment.

Use Cases

1 **Investigation / Incident Response**
The integration combines build-time visibility of vulnerabilities within container images from Snyk with runtime threats detected by SentinelOne CWPP, so that customers can better manage risk and fix critical issues.

2 **Build-time Vulnerability Context**
Snyk Container helps secure container images by allowing developers and DevOps to find, prioritize, and fix vulnerabilities throughout the SDLC, before workloads hit production. With Snyk Container, you can remediate base images automatically, minimizing exposure and reducing time-to-fix and monitor continuously to protect the image after the initial scan.

3 **Threat Hunting**
Security practitioners can proactively hunt for threats within the SentinelOne Singularity Data Lake, which includes details ingested from Snyk Container. For example, previously identified runtime threats may have been correlated to a specific image vulnerability; a threat hunter can search for that vulnerability, to identify any further risk.