



#WeAreExclusive



Snyk & SentinelOne

Technical Integration and Partnership



Security from Code to Cloud

Frictionless collaboration between Developers, AppSec and SecOps



Find and fix vulns in
your source code



Real-time
CWPP



snyk AppSec

Software vulns, image scanning, "shift left"

CSPM

Config management, IaC templates, drift management, etc.



SentinelOne® CWPP

Runtime threat detection, response



CIEM

Identity and entitlements for human and machine roles



DSPM

Data security, malware scans of object storage, etc.





#WeAreExclusive

SentinelOne Console

NETWORK HISTORY

First seen Feb 06, 2023 21:12:35
Last seen Jul 27, 2023 19:28:22

8 times on 4 endpoints
1 Account / 2 Sites / 2 Groups

Find this hash on Deep Visibility
[Hunt Now](#)

THREAT FILE NAME zip.com [Copy Details](#) [Download Threat File](#)

Path	/host/var/lib/docker/overlay2/ac09355200862424112345ca46bde74afb...	Initiated By	Full Disk Scan
Command Line Arguments	N/A	Engine	SentinelOne Cloud
Process User	N/A	Detection type	Static
Publisher Name	N/A	Classification	Malware
Signer Identity	N/A	File Size	308.00 B
Signature Verification	N/A	Storyline	Static Threat - View in DV
Originating Process	N/A	Threat Id	1738434171910197807
SHA1	bec1b52d350d721c7e...		

ENDPOINT **KUBERNETES**

NODE	NAME: kubernetes-vm LABELS: kubernetes.io/hostname: kubernetes-vm.kubernetes.io/os: linux,node-role.kubernetes.io/contr...
NAMESPACE	NAME: sentinelone LABEL: kubernetes.io/metadata.name: sentinelone
CONTROLLER	NAME: s1-agent TYPE: DaemonSet LABELS: managed-by: Helm,release: s1-agent,version: 23.1.2.app: s1-agent.app.kubernetes.io/managed-...
POD	NAME: s1-agent-hx7kj LABELS: controller-revision-hash: 6679f964fc,managed-by: Helm,pod-template-generation: 1,release: s...
CONTAINER	NAME: agent IMAGE: docker.io/cwpp_agent/s1agent:23.1.2-x86_64 ID: 63ef629de777295443e04679bb529
NETWORK STATUS	Connected

THREAT INDICATORS NOTES (1) XDR(5)

Snyk

Snyk
Jul 27, 2023 19:28:25

Summary

Total issues: 2943
217 critical, 687 high, 605 medium, 1434 low

Snyk Project: devangtest/dvwa-testv3
Source: docker-hub
Showing 10 issues out of 2943 issues:

#1 Access Restriction Bypass (view issue in Snyk)

Issue Details:

- Type: vulnerability
- Package: openssl/openssl-client
- Priority Score: 150
- Severity: low
- CVE: CVE-2008-3234
- CWE: CWE-264
- CVSS Score: CVSS 6.3
- Affected Versions: All Versions
- Exploit Maturity: No known exploit
- Language: linux
- Package Manager: debian:10
- How to fix: Fix not available
- Detected by Snyk on: 2023-07-12

#2 Access Restriction Bypass (view issue in Snyk)

Issue Details:

- Type: vulnerability
- Package: shadow/login
- Priority Score: 150
- Severity: low
- CVE: CVE-2007-5686
- CWE: CWE-264
- CVSS Score: CVSS 6.2
- Affected Versions: All Versions
- Exploit Maturity: No known exploit

Runtime Threat Detected by SentinelOne CWPP

Vulns identified by Snyk in workload source code



Customer Benefits



Improve Visibility

Automatically correlate build time vulnerabilities to runtime threats, shown in the same console. Understand root cause quickly.



Better Prioritization & Response

Automate response actions by policies you control to stop the spread. Prioritize vulnerabilities impacting production and solve them at the source.



Better Cloud Security Outcomes

Continuous feedback loop leads to more secure cloud operations. Drive more complete understanding quickly, to slash incident response time and improve risk management.



LEARN MORE:

www.sentinelone.com/partners/snyk

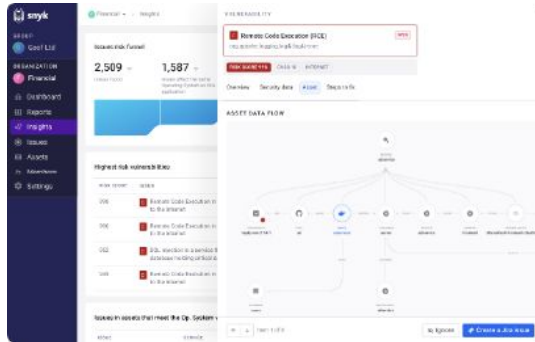


Step by Step Walk-Thru

Snyk & SentinelOne Integration

- Bi-directional integration, in 2 phases, for build time to runtime security
- Deep links to switch between Snyk and SentinelOne consoles

Build Time



- Correlate and contextualize vulnerable container images with runtime threats
- Prioritise and fix build time vulnerabilities and reduce alert fatigue

PHASE: 1

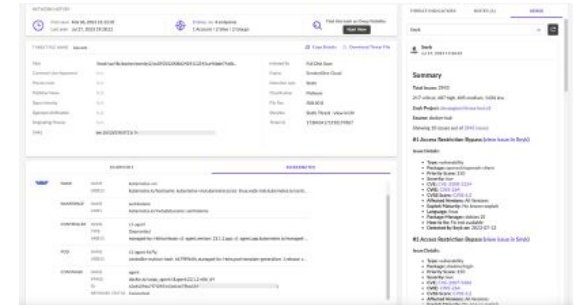
Container image vulnerabilities from Snyk pulled into S1 (Nov 2023)



Runtime threats from S1 pushed to Snyk (H1 2024)

PHASE: 2

Runtime



- Runtime threat enrichment with build-time vulnerability context for improved RCA
- Threat hunting & investigations



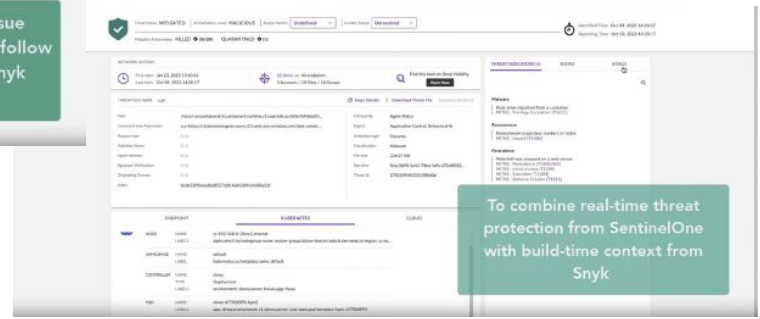
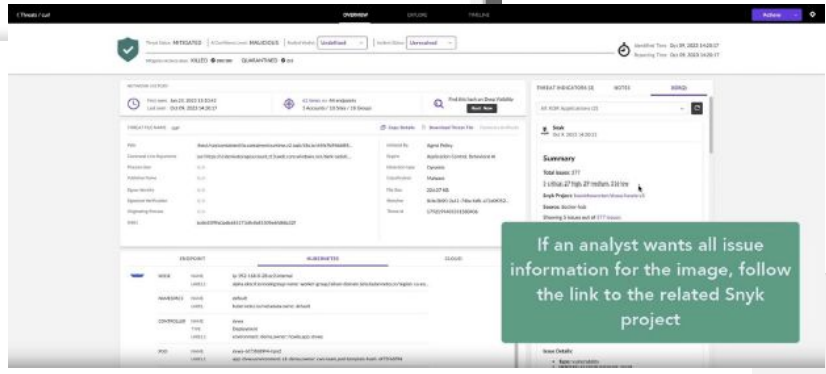
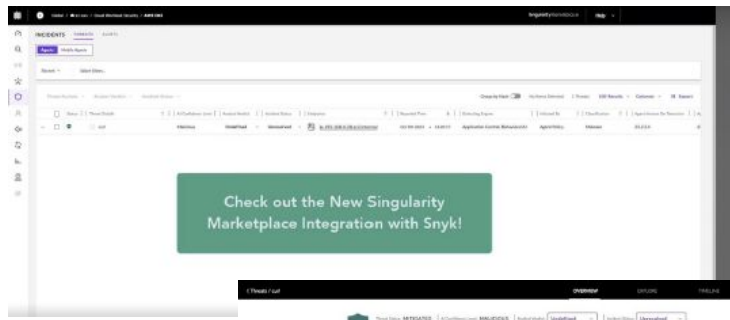
#WeAreExclusive

DEMO



Snyk & SentinelOne Integration

#WeAreExclusive





#WeAreExclusive



Thank You

sentinelone.com/partners/snyk

