ANY.RUN Brings Automated Orchestration and Threat Context to Modern SOC Workflows

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 28, 2026 /EINPresswire.com/ -- ANY.RUN today announced that it is rolling out a native integration with SentinelOne, the AI Security leader, merging real-time malware analysis and threat intelligence with advanced endpoint protection to give defenders the precise context needed to instantly validate high-priority alerts.



By feeding deep behavioral insights and threat telemetry straight into SentinelOne's Singularity™ Platform, this partnership slashes the time wasted on false positives. The result is an optimized workflow that accelerates response times and lifts the daily operational burden from SOC teams and MSSPs.

□□□□□□□□□ □□□□□□□ □□□□□□□□□ □□□ □□□□□□□□□□□□□ □□□□□□□ □□□□□□□□□□□□

Operating directly within SentinelOne's platform, security teams can now deploy automated orchestration rules that eliminate manual triage steps. These playbooks harness ANY.RUN's Interactive Sandbox and Threat Intelligence to automatically cross-reference suspicious files, URLs, and indicators against known malicious behavior.

Instead of pivoting between dashboards, analysts receive immediate threat verdicts, malware family classification, and detailed indicator infrastructure directly inside the SentinelOne incident log. This brings definitive threat data to the analyst's fingertips, ensuring quick decisions without console switching.

□□□□□□□□□ □□□□□□□□□ □□□□ □□□□□□□□□ □□□□□□□□□□□□

This integration delivers clear operational upgrades designed to streamline daily threat management:

• Accelerated Time-to-Verdict: By pulling threat evaluations instantly, the platform cuts investigation delays and helps teams isolate threats before they spread.

• Smart Resource Allocation: Handing off repetitive Tier 1 collection tasks to automated workflows lets current staff absorb higher alert volumes and focus on deeper threat hunting.

• Unified Quality of Evidence: Standardizing the enrichment phase guarantees that every alert is backed by identical threat intelligence, minimizing oversights and leveling up junior analysts.

Read how to get started on ANY.RUN's Cybersecurity Blog.

□□□□□□ □□□.□□□

Trusted by over 700,000 cybersecurity professionals and 16,000+ organizations worldwide, ANY.RUN helps security teams investigate threats faster and with greater accuracy. The solution combines an Interactive Sandbox for real-time analysis of suspicious files across multiple operating systems with Threat Intelligence solutions that provide the context necessary to anticipate and stop advanced attacks.

ANYRUN FZCO
ANYRUN FZCO
+ +1 657-366-5050
email us here
Visit us on social media:
LinkedIn
X

This press release can be viewed online at: https://www.einpresswire.com/article/945782721

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.