

# ANY.RUN Announces Its Integration with Splunk for Advanced Threat Analysis

DUBAI, UNITED ARAB EMIRATES,  
September 12, 2024 /

EINPresswire.com/ -- [ANY.RUN](#), a leader in interactive malware analysis, has announced its latest integration with Splunk, a leading platform for data analysis, security information, and event management (SIEM). This collaboration allows Splunk users to use ANY.RUN's Interactive Sandbox and Threat Intelligence Lookup directly within their Splunk SOAR environment, giving them the opportunity to analyze potential cyber threats without leaving their familiar interface.

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

With this integration, Splunk users can now analyze potentially malicious files, URLs, and other suspicious objects in ANY.RUN's sandbox, while also enriching their investigations using ANY.RUN's Threat Intelligence Lookup.

All of this can be done without leaving the familiar Splunk interface, enhancing productivity and efficiency for threat analysts.

□□□ □□□□□□□□ □□ □□□ □□□□□□□□□□□□ □□□□□□□□:

- Comprehensive threat intelligence: Query ANY.RUN's extensive threat intelligence database directly from Splunk SOAR.
- Automated malware analysis: Automatically detonate suspicious files and URLs in ANY.RUN's sandbox as part of a Splunk integration.
- Detailed reporting and IOC extraction: Retrieve key analysis details and threat verdicts, as well as extract Indicators of Compromise (IOCs) for further investigation.
- Advanced threat hunting: Use ANY.RUN's 'get intelligence' action to perform complex queries



on file hashes, IP addresses, domains, or MITRE ATT&CK techniques.

For detailed instructions on the setup process and its real-world applications, visit the [ANY.RUN blog](#).

ANY.RUN

With over 8 years of experience tackling cybersecurity industry challenges, ANY.RUN helps over 400,000 cybersecurity professionals worldwide with its advanced interactive sandbox that simplifies the analysis of threats targeting both Windows and Linux systems. Its Threat Intelligence Lookup, YARA Search, and Feeds allow analysts to investigate and respond to incidents quickly, providing critical insights for faster decision-making.

The ANY.RUN team

ANYRUN FZCO

+1 657-366-5050

[email us here](#)

Visit us on social media:

[X](#)

[YouTube](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/742892030>

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.

© 1995-2024 Newsmatics Inc. All Right Reserved.