EINPRESSWIRE

ANY.RUN Releases Connector for Microsoft Sentinel to Deliver Real-Time Threat Intelligence on Emerging Malware

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 5, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence, is thrilled to announce a connector for Microsoft Sentinel, empowering Security Operations Centers (SOCs) and Managed Security Service Providers (MSSPs) with actionable, real-time threat intelligence feeds.

TI Feeds deliver high-fidelity Indicators of Compromise (IOCs) directly into Microsoft Sentinel via the STIX/TAXII, which helps organizations to detect and respond to emerging cyberthreats faster and more effectively.

□□□□□-□□□□□□□□□□ □□□□□□ □□□□ □□□□□□□□□□
□□ □□□□□□□ □□□□□□□□□□□ □□□□□ □□□□□-□□□□□ □□□□□
ANY.RUN’s Threat Intelligence (TI) Feeds provide malicious IPs, domains, and URLs extracted from live sandbox analyses, updated every two hours. Unlike traditional post-incident reports, these feeds offer fresh, high-confidence IOCs derived from real-time attack detonations across 15,000 organizations worldwide.

The connector for MS Sentinel requires no complex setups or custom scripts, making it accessible and efficient for security teams.

Key Benefits:
□ □□□□□□□□□□ □□□□□: Connect ANY.RUN’s TI Feeds to Microsoft Sentinel using a custom API key and the native TAXII connector, ensuring a plug-and-play experience.
□ □□□□□□□□ □□□□□□□□□□: Leverage Sentinel’s playbooks, powered by Azure Logic Apps, to

automate actions like blocking malicious IPs, reducing manual workload and accelerating response times.
□ □□□□ □□□□□□□□□□: Utilize existing Sentinel infrastructure without additional costs, minimizing financial and operational risks from undetected threats.
□ □□□□ □□□□□□□: Each IOC is enriched with links to threat analyses in ANY.RUN’s Interactive Sandbox, enabling deeper investigations and custom rule creation.
□ □□□ □□□□□: Expert pre-processing ensures near-zero false positives, saving valuable time for SOC teams.

□□□□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□ □□□□□□ □□□□□□□□□
ANY.RUN’s TI Feeds give SOCs and MSSPs a competitive edge by delivering fresh, actionable intelligence to detect and mitigate threats before they cause harm. This enhances Sentinel’s analytics, allowing security teams to visualize threats, prioritize incidents, and streamline triage processes.

Automated correlation with logs from EDR systems, network equipment, and other sources ensures rapid alert generation and response, reducing Mean Time to Respond (MTTR) and preventing costly breaches.

□□□ □□□□□□□ □□□□□
Security teams can start leveraging ANY.RUN’s TI Feeds in Microsoft Sentinel with a simple setup process. By accessing the Threat Intelligence TAXII connector in their Sentinel workspace, teams can configure IOC ingestion and unlock powerful threat detection capabilities.

The detailed setup instructions and more information on the connector are available on ANY.RUN’s blog.

□□□□□ □□□.□□□
ANY.RUN is a leading cybersecurity platform trusted by over 500,000 professionals and 15,000 organizations worldwide. Its interactive sandbox and threat intelligence solutions enable security teams to analyze threats in real-time, gain actionable insights, and respond faster to advanced threats. With a mission to simplify and accelerate incident response, ANY.RUN continues to innovate and empower the global cybersecurity community.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
LinkedIn
YouTube
X