ANY.RUN Expands Microsoft Sentinel Capabilities to Help SOC Teams Cut Alert Noise and Accelerate Threat Response

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 25, 2025 /EINPresswire.com/ -- ANY.RUN, a leader in interactive malware analysis and threat intelligence, released a connector for Microsoft Sentinel, empowering Security Operations Centers to automate alert triage, reduce false positives, and respond to threats faster.

□□□ □□□□□□□□□□ □□□□□□□: □□□□ □□□□□ □□□□□□□□ □□ □□□□□□□□□□ □□□□□□□□ Manual alert enrichment and tool-switching drain SOC productivity, delaying response to critical threats. ANY.RUN's Microsoft Sentinel connector eliminates these bottlenecks by embedding automated, interactive sandbox analysis directly into Sentinel's environment. Now, security teams can:

□ □□□□-□□□□□□ □□□□□□ with verdicts, risk scores, and IOCs (IPs, domains, hashes) in seconds.
□ □□□□□□□□ □□□ □□□□□□□ □□□□□□□ in Windows, Linux, and Android environments automatically via Sentinel playbooks.
□ □□□□□□□□□□ □□□□-□□□□ □□□□□□□□□ with clear, actionable threat context, preventing alert fatigue.

Learn more about the connector and how to set it up on ANY.RUN's blog.

□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□ □□□□ □□□.□□□'□ □□□□□□□□□□
By embedding ANY.RUN's Interactive Sandbox and Threat Intelligence Feeds into their workflows, organizations gain a competitive edge while maximizing their existing security investments. The

use of the solutions delivers measurable value:

□ □□□□□□ □□□□□□ □□□□□□□□□□□□□□□□: Cut mean time to respond (MTTR) by □□+ □□□□□□□□ □□□□ □□□□□□□□□ with automated sandbox analysis.
□ □□□□□□ □□□□□□□□□□ □□□□□□: □□□ □□% □□□□□□ □□□□□□□□□□ □□□□, including for evasive malware that bypass traditional defenses, reducing breach risk.
□ □□□□□□ □□□□□□□□□□□□ □□□□□□: □□□□□□ □□□□ □ □□□□□□□□□ □□ □□%, freeing teams for strategic tasks.
□□□□□□□□□□ □□□□ □□□□□□□□□□: Stay ahead of attacks with real-time threat intelligence feeds from □□,□□□+ □□□□□□□ □□□□ to block emerging threats before they execute.

□□□□□□ □□□.□□□
ANY.RUN supports over 15,000 organizations worldwide, including sectors like banking, healthcare, telecom, retail, and manufacturing, by helping security teams build stronger, faster, and more resilient cybersecurity operations.

Through its cloud-based Interactive Sandbox, analysts can safely investigate and understand malware behavior across Windows, Linux, and Android systems. Combined with TI Lookup, YARA Search, and Threat Intelligence Feeds, ANY.RUN equips teams with the tools they need to accelerate investigations, reduce security risks, and collaborate more effectively.

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