EINPRESSWIRE

ANY.RUN Launches Microsoft Defender Connectors to Accelerate Threat Response and Reduce Alert Noise

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 30, 2025 /EINPresswire.com/ -- ANY.RUN, a leader in interactive malware analysis and threat intelligence, today announced new connectors for Microsoft Defender that empower Security Operations Centers (SOCs) to automate alert enrichment, cut false positives, and respond to threats faster without leaving the Defender workspace.

□□□.□□□ & □□□□□□□□□ □□□□□□□□
□□□□□□□□□□
SOCs using Microsoft Defender can seamlessly connect ANY.RUN's solutions into their existing workflows, boosting their ability to combat advanced threats seamlessly and without disrupting existing processes.

The ANY.RUN connectors include:
□ □□□□□□□□□□□ □□□□□□□ □□□□□□□□□: Automates the analysis of suspicious files and URLs, delivering detailed behavioral insights and IOCs directly within Microsoft Defender.
□ □□□□□□ □□□□□□□□□□□□ □□□□□ □□□□□□□□□: Provides real-time, actionable indicators of compromise (IOCs) to enable proactive threat detection.

□□□ □□□□□□□□ □□□ □□□ □□□□□
The connectors empower SOC teams to triage alerts efficiently, detect elusive malware, and resolve incidents with speed, all while reducing operational overhead.
□ □□□□□□ □□□□□□□□ □□□□□□□□□□: Automated sandbox analysis reduces mean time to respond (MTTR) by tens of percent per incident.

□ □□□□□□□□□ □□□□□□ □□□□□□□□□: Real-time Threat Intelligence Feeds from 15,000+ organizations uncover evasive malware missed by signature-based tools.
□ □□□□□□□ □□□□□□□ □□□□□□□: Automation slashes Tier 1 workload by 20%, freeing teams for high-priority tasks.
□ □□□□□□□□ □□□□□□□□□: Pre-built playbooks embed ANY.RUN’s Interactive Sandbox and TI Feeds directly into Microsoft Defender, preserving existing workflows.

Learn more and see how to set up the connectors on ANY.RUN’s blog.

□□□□□ □□□.□□□
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

This press release can be viewed online at: https://www.einpresswire.com/article/853887040