

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:

- ▣ Enrich alerts with verdicts, risk scores, and IOCs (IPs, domains, hashes) in seconds.
- ▣ Automate analysis in Windows, Linux, and Android environments automatically via Sentinel playbooks.
- ▣ Provide 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:

■ **Reduce mean time to respond (MTTR):** Cut mean time to respond (MTTR) by 50+ minutes with automated sandbox analysis.

■ **Reduce breach risk:** 100% visibility into threats, including for evasive malware that bypass traditional defenses, reducing breach risk.

■ **Free up analyst time:** Automate repetitive tasks, freeing teams for strategic tasks.

■ **Stay ahead of attacks:** Stay ahead of attacks with real-time threat intelligence feeds from 10,000+ sources to block emerging threats before they execute.

ANY.RUN

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/852411338>

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.

© 1995-2025 Newsmatics Inc. All Right Reserved.