

ANY.RUN & Palo Alto Networks Cortex XSOAR Empower SOCs to Boost Incident Detection

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 16, 2025 /EINPresswire.com/ -- [ANY.RUN](#), a leading provider of interactive malware analysis and threat intelligence, has announced an integration with Palo Alto Networks Cortex XSOAR, empowering SOCs to boost threat detection, reduce alert fatigue, and cut response times.

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence, empowering SOCs to boost threat detection, reduce alert fatigue, and cut response times.

ANY.RUN's content pack for Cortex XSOAR includes connectors for the Interactive Sandbox, Threat Intelligence Lookup, and Threat Intelligence Feeds. Thanks to the seamless connection, security teams now can:

- Submit files/URLs to a secure sandbox for analysis across Windows, Ubuntu, Android to streamline triage.
- Retrieve detailed reports in JSON, HTML, or IOC formats for incident response.
- Ingest fresh threat data every 2 hours from 15,000+ organizations for threat hunting.
- Query threat details for IOCs, IOAs, and IOBs to enrich incident investigations.
- Automate workflows using XSOAR playbooks to reduce manual workload.

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence, empowering SOCs to boost threat detection, reduce alert fatigue, and cut response times.



Companies utilizing Cortex XSOAR as part of their security infrastructure now can take advantage of ANY.RUN's advanced capabilities to:

- Detect evasive threats faster with automated sandbox analysis for stronger protection.
- Prevent attacks proactively using real-time threat data to reduce breach risks.
- Clarify incidents with enriched threat context for quicker, more accurate response.
- Reduce alert overload by automating analysis and response, saving SOC time.
- Ensure compliance with secure, private workflows for safe operations.
- Strengthen security posture by integrating sandboxing, threat data, and XSOAR automation.

Learn more about the integration on [ANY.RUN's blog](#).

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/849570415>

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.

