ANY.RUN Integrates with ThreatQ to Bring Expanded Threat Coverage to SOCs and MSSPs

DUBAI, DUBAI, UNITED ARAB EMIRATES, October 23, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis solutions, today announced the launch of its game-changing connector for ThreatQ Threat Intelligence Platform (TIP). The new connector enables ThreatQ users to seamlessly integrate ANY.RUN's high-fidelity Threat Intelligence Feeds directly into their existing security operations, delivering real-time indicators of compromise (IOCs) from live sandbox investigations across more than 15,000 organizations worldwide.

□□□□□□□□□□ □□□□□□□□ □□□ □□□□□□□□□□

As threat volumes continue to surge, SOC teams face mounting pressure to process increasing amounts of security data while maintaining high detection accuracy.

The ANY.RUN ThreatQ connector directly addresses these challenges by providing pre-processed, reliable threat intelligence with near-zero false positives, enabling security teams to focus resources on genuine threats rather than alert fatigue.

· □□□□□ □□□□□□□□□: IOCs added to TI Feeds as soon as they emerge from live sandbox analyses, enabling proactive identification of new threats in your SOC.

· □□□□□□□□ □□□□□□ □□□□□□□□: 99% unique indicators from global attacks □(e.g., phishing, malware) provide visibility into threats traditional feeds miss.

· □□□□□□□□ □□□□□□□□: Each IOC comes enriched with a link to a sandbox report, showing the full attack being detonated on a live system, providing SOCs with actionable context for fast mitigation.

· □□□□□□□ □□□□□□□□: Filtered for malicious alerts, cutting Tier 1 analysis time spent on false positives.

The connector utilizes industry-standard STIX/TAXII protocols and leverages ThreatQ's existing infrastructure to ensure seamless deployment within enterprise environments.

For detailed information and instructions on enabling the connector, visit ANY.RUN 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 solutions 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
