

ANY.RUN Expands Security Capabilities with IBM Integration, Exclusive Threat Intelligence, and ARM Malware Analysis

DUBAI, DUBAI, UNITED ARAB
EMIRATES, August 4, 2025

/EINPresswire.com/ -- [ANY.RUN](#), the provider of interactive malware analysis and threat intelligence solutions, has announced a series of major product updates. They include an integration with IBM QRadar SOAR, a Free plan for Threat Intelligence Lookup, support for Linux ARM malware analysis, and expanded threat detection rules.

ANY.RUN is a cloud-based interactive malware analysis platform that allows security analysts to safely execute and analyze suspicious files and URLs. The platform provides a detailed view of the malware's behavior, including file system changes, network traffic, and process execution. ANY.RUN also offers a Threat Intelligence Lookup feature, which allows analysts to search for known indicators of compromise (IOCs) and threat actors. The platform is designed to be easy to use and integrate with existing security tools.

The new IBM QRadar SOAR integration enables analysts to detonate suspicious files and URLs in ANY.RUN's interactive sandbox directly from QRadar SOAR, with verdicts, behavioral logs, and indicators of compromise (IOCs) automatically pushed back into incidents. This approach streamlines triage, reduces Mean Time to Respond (MTTR), and helps SOC teams catch stealthy threats earlier.

ANY.RUN is a cloud-based interactive malware analysis platform that allows security analysts to safely execute and analyze suspicious files and URLs. The platform provides a detailed view of the malware's behavior, including file system changes, network traffic, and process execution. ANY.RUN also offers a Threat Intelligence Lookup feature, which allows analysts to search for known indicators of compromise (IOCs) and threat actors. The platform is designed to be easy to use and integrate with existing security tools.

- Lower workload and faster response through automation.
- Improved efficiency across Tier 1 and Tier 2 analysts.
- Smarter decision-making with enriched playbooks and detection rules.
- Early visibility into multi-stage and evasive attacks.



- Greater ROI from existing SOAR investments without additional infrastructure.

The ANY.RUN app is available now on the IBM App Exchange.

000000 000000000000 000000: 0000 000000 00 0000-000000 000000 0000

ANY.RUN's Threat Intelligence Lookup (TI Lookup) now includes a Free plan, providing SOC teams with real-time, actionable threat intelligence from millions of sandboxed malware sessions.

With TI Lookup Free, analysts can:

- Enrich investigations with real-world context.
- Reduce MTTR using live behavioral insights.
- Strengthen proactive defense with early visibility into emerging threats.
- Explore TTPs through the MITRE ATT&CK matrix.
- Develop and refine SIEM, IDS/IPS, and EDR rules.

The Free plan allows unlimited searches across file hashes, URLs, domains, IPs, Suricata IDs, and MITRE ATT&CK techniques. For enterprise needs, TI Lookup Premium offers expanded data, private search, YARA rule matching, alert subscriptions, and API integration.

□□□□□□ □□□ □□□□□□□□: □□□□□□□□ □□□□□□□□ □□ □□□ □□□ □□□□□□□□ □□□□□□□□

To address the rise of ARM-based attacks targeting IoT devices and embedded infrastructure, ANY.RUN now supports **ARMv8 (AArch64, 64-bit)** in its Interactive Sandbox.

This environment allows analysts to:

- Interact directly with ARM-based malware in real time.
- Detect persistence, evasion, and privilege escalation techniques.
- Trace execution paths from dropped files to command-line activity.
- Map behaviors to MITRE ATT&CK for accurate threat classification.

The Debian ARM sandbox is available to Enterprise users.

ANY.RUN is a cloud-based malware analysis and threat intelligence platform. It provides a safe environment to analyze malware samples, track their behavior, and identify threats. ANY.RUN is trusted by over 500,000 cybersecurity professionals worldwide.

In July, ANY.RUN strengthened detection capabilities with:

- 163 new behavior signatures for detecting obfuscation, persistence, and stealth techniques.
- 13 new YARA rules, including coverage for BlackMatter, LockBit4, and Sinobi.
- 2,772 new Suricata rules to improve detection of phishing campaigns and data exfiltration, including Telegram-based exfiltration and fake government domains.

To get more details, visit [ANY.RUN's blog](#).

ANY.RUN is a

ANY.RUN is an interactive malware analysis and threat intelligence platform trusted by over 500,000 cybersecurity professionals worldwide. By combining real-time sandboxing, threat intelligence, and automation, ANY.RUN helps SOC teams investigate incidents faster, stop threats earlier, and strengthen defenses against evolving cyberattacks.

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/836884778>

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.