ANY.RUN Unveils Detonation Actions to Help Businesses Simplify Cyber Threat Analysis and Boost Detection Rate

DUBAI, DUBAI, UNITED ARAB EMIRATES, June 19, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has launched Detonation Actions, a new feature that guides analysts with real-time hints during sandbox sessions, helping security teams, SOC analysts, and incident responders trigger malicious behavior faster and investigate with greater confidence.

□□□□□□ □□□□□□□ □□□□□□□ □□□□□□ □□ □□□□□□

Threat analysis isn't always straightforward. Some malware only reveals itself after very specific user actions, opening a document, extracting a file, clicking a fake button. Miss a step, and you might miss the threat entirely.

□□□□□□□□□□ □□□□□□□ remove the guesswork. They guide analysts through the exact steps needed to activate malicious behavior, saving time and helping detect more threats in less time.

□□□□ □□□ □□□□□□□□□□ □□□□□□□?

Detonation Actions are intelligent hints that appear alongside the process tree during a sandbox session in ANY.RUN. These hints are designed to highlight key actions needed to detonate malware, like launching a file, clicking a link, or enabling macros.

They work in both:

· [illegible]: Analysts follow the guided steps and choose which actions to approve or reject.

· [illegible]: The sandbox handles each step for you, running actions in real time with no manual input needed.

Detonation Actions are available across all plans. Free users can follow the hints manually during analysis, while paid users unlock full automation through Automated Interactivity, including API access and complete visibility into every action performed during the session.

[illegible]

Detonation Actions bring measurable improvements to threat analysis by:

· [illegible] with guided steps that reduce manual effort

· [illegible] by ensuring critical actions aren't missed

· [illegible] through faster triage and clearer visibility

· [illegible] with transparent, action-based workflows

· [illegible] with intuitive hints for junior analysts

· [illegible] for scalable, high-efficiency analysis

To learn more about how Detonation Actions can enhance your team's detection workflow and how to get started, head over to the ANY.RUN blog.

[illegible]

ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, empowers more than 15,000 companies worldwide to detect, analyze, and respond to threats with precision. Its solutions enable real-time, hands-on investigation of suspicious files, URLs, and malware across Windows, Linux, and Android environments, helping SOCs and security teams uncover threats faster and with greater confidence.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media: