EINPRESSWIRE

ANY.RUN Now Lets Users Enrich Data on Active Network Security Threats with Suricata Search

DUBAI, UNITED ARAB EMIRATES, July 9, 2024 /EINPresswire.com/ -- ANY.RUN, a trusted provider of cybersecurity solutions, has made a significant upgrade to its Threat Intelligence Lookup platform by incorporating Suricata search capabilities. This new feature aims to help users identify more network threats with greater precision.

□□□.□□□'□ □□□□□□ □□□□□□□□□□□□ □□□□□□
ANY.RUN's Threat Intelligence Lookup provides access to a comprehensive repository of threat data extracted from public analysis sessions in the ANY.RUN sandbox. This tool enables users to search against its database using individual or combined indicators of compromise (IOCs) to find emerging and active malware, as well as other cyber threats.

□□□□□□□□ □□□□□□
With the introduction of the Suricata Search feature, TI Lookup now lets users hunt for active network security threats using Suricata rule details.

□□□ □□□□□□□□ □□□□□□ □□□□□
Users can create a specific query that includes the rule's class, message, ID, and even threat level (e.g., SuricataThreatLevel:"malicious" and SuricataMessage:"External IP"). Suricata parameters can be combined with other indicators, such as domains, to refine the search.

Once the search query is executed, the service will display all threats that match the query. Each result will contain additional information about the threat, including associated tags (e.g., denoting the APT or malware family) and MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) used by the threat.

To further investigate each threat, users can navigate to the ANY.RUN sandbox for a more detailed analysis.

Learn more about Suricata Search and TI Lookup on ANY.RUN’s blog.

□□□□□ □□□.□□□
With a suite of cybersecurity products that includes an interactive sandbox and a Threat Intelligence portal, ANY.RUN supports 400,000 professionals worldwide. The sandbox offers a streamlined method for analyzing malware and phishing targeting both Windows and Linux systems. ANY.RUN's Threat Intelligence services: Lookup, Feeds, and YARA Search, enable users to quickly collect and enrich their data on currently active threats.

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

This press release can be viewed online at: https://www.einpresswire.com/article/726217083

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.
© 1995-2024 Newsmatics Inc. All Right Reserved.