Cortex XSOAR and ANY.RUN Malware Analysis and Threat Intelligence Services

Automate and Improve Threat Detection and Hunting in Your SOC for a Swift Response

Key Benefits

- Slash incident response time with automated, secure malware analysis in Cortex XSOAR®.
- Increase detection rates via interactive sandboxing across Windows, Linux, and Android.
- Improve proactive security with fresh indicators of compromise (IoCs) from 15,000 SOCs, updated every 2 hours.
- Enhance incident context with threat analysis results right in Cortex XSOAR.
- Reduce SOC workload by automating threat triage and response tasks.
- Help ensure compliance with SOC 2/GDPR via a secure, private analysis mode.

The Challenge

Modern SOCs are overwhelmed with incident alerts and lack fast, reliable ways to assess and prioritize them effectively. This leaves critical infrastructures vulnerable to attacks like ransomware and data theft, which might slip through security gaps and cause major damage and downtime.

The Solution

Proactive sandbox analysis of suspicious indicators, files, and URLs plus real-time threat intelligence empower SOCs to address the problem of accurately identifying high-risk attacks without additional effort. Here's how:

- Automated detonations of malware inside a safe, isolated, and fully private environment help ensure a higher chance of detection.
- Fresh threat data helps correlate the incoming alerts with a vast database of known malicious indicators to catch attacks before they spread.
- Clear insights into the current threat landscape of the organization improve visibility, response speed, and accuracy—enabling teams to focus on stopping threats effectively and efficiently.

ANY.RUN Content Pack for Cortex XSOAR

The Palo Alto Networks Cortex XSOAR and ANY.RUN integration enables SOCs to automate triage, expand threat coverage, and increase the detection rate, including hidden and missed malware.

With the ANY.RUN content pack for Cortex XSOAR, your organization can:

- Submit files and URLs to a secure sandbox for analysis across Windows, Ubuntu, and Android to streamline triage.
- Retrieve detailed reports in JSON, HTML, or IoC formats for incident response.
- Ingest fresh threat data every 2 hours from over 15,000 organizations for threat hunting.
- Query threat details for IoCs, indicators of attack (IoAs), and indicators of behavior (IoBs) to enrich incident investigations.
- Automate workflows using Cortex XSOAR playbooks to reduce manual workload.

Palo Alto Networks Cortex XSOAR

Cortex XSOAR is the industry's most comprehensive SOAR platform, unifying workflow automation, case management, and threat intel management on a single platform. With Cortex XSOAR, security teams can take actions on threat intelligence, standardize processes, and automate repeatable tasks to efficiently manage incidents across their product stack and reduce response times.

Palo Alto Networks and ANY.RUN Early Threat Detection

The Palo Alto Networks Cortex XSOAR and ANY.RUN integration helps SOCs improve their performance. The integration also helps them:

- **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 an enriched threat context for a quicker, more accurate response.
- **Reduce alert overload** by automating analysis and response, saving SOC time.
- **Help ensure compliance** with secure, private workflows for safe operations.
- **Strengthen security posture** by integrating sandboxing, threat data, and Cortex XSOAR automation.

Use Case 1: Improve Low Detection Rates

Challenge

Poor detection capabilities allow evasive threats to slip through security systems, risking breaches.

Solution

ANY.RUN Malware Sandbox in Cortex XSOAR enables interactive, real-time file and URL analysis across multiple operating systems, boosting the detection of complex malware and phishing attacks. Fresh threat data from threat intelligence services helps SOCs expand threat coverage, improving detection accuracy and proactively addressing high-risk incidents.

Use Case 2: Reduce Alert Overload for Focused Response

Challenge

Alert overload overwhelms SOCs, slowing response and missing high-priority threats.

Solution

ANY.RUN has automated sandboxing available inside Cortex XSOAR that analyzes files and URLs, powering effective playbooks to handle alerts. This reduces the workload, letting teams focus on high-priority incidents while helping ensure a fast, accurate response.

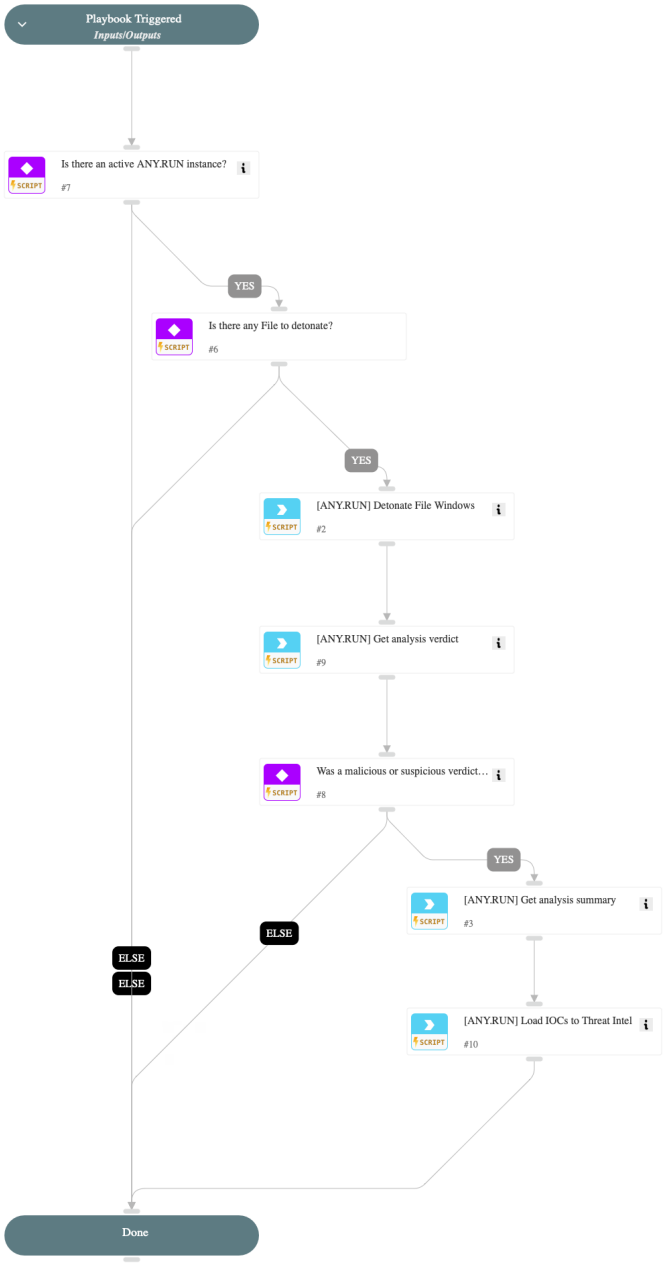

Figure 1. ANY.RUN playbook for file analysis in Windows Sandbox

Palo Alto Networks and ANY.RUN Integrations

Product integrations between Palo Alto Networks and ANY.RUN include:

- Malware Sandbox
- Threat Intelligence Lookup
- Threat Intelligence Feeds

About ANY.RUN

ANY.RUN services are used by SOC teams at over 15,000 organizations across different industries, including finance, manufacturing, healthcare, and technology. Malware Sandbox helps businesses ensure fast and accurate analysis of cyberthreats, while TI Lookup and TI Feeds allow businesses to expand threat coverage and detection. For more information, visit https://any.run.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_pb_any-run_082225