ANY.RUN Malware Analysis and Threat Intelligence & Google Security Operations

Reduce response time and business risk
with evidence-driven investigations

ANY.RUN Content Pack for Google SecOps: Overview

The ANY.RUN Content Pack for Google SecOps enables seamless integration between the solutions, helping SOC teams **analyze alerts faster, validate threats with confidence, and act earlier in the attack lifecycle.**

The Content Pack enhances Google SecOps alerts with:

- Real-time malware analysis of suspicious files and URLs via ANY.RUN's **Interactive Sandbox**,
- Deep threat context from ANY.RUN's **Threat Intelligence Lookup**,
- Continuously updated IOCs from ANY.RUN's **Threat Intelligence Feeds** based on real attacks across 15K organizations.

Each integration addresses critical SOC needs, from fast validation to proactive detection, while enabling analysts to use the pack as a single investigative flow.

Key Benefits

- **Reduce incident response time** with automated malware analysis directly inside Google SecOps
- **Increase detection accuracy** using interactive sandbox analysis across multiple operating systems
- **Lower false positives** with verified indicators sourced from real-world attacks
- **Improve incident clarity** with behavior-based analysis and enriched threat context
- **Reduce SOC workload** by automating triage and enrichment tasks
- **Support compliance requirements** with secure, private analysis workflows (SOC 2 / GDPR)

ANY.RUN Sandbox: Validate Threats with Real Attack Behavior

The ANY.RUN Sandbox Response integration allows analysts to send suspicious files and URLs from Google SecOps alerts directly for dynamic analysis.

Value for SOC:

- Faster verdicts based on real execution, not static signals
- Higher confidence in triage decisions
- Reduced unnecessary escalations

Value for Business:

- Lower breach risk
- Reduced incident handling costs
- Faster containment of real threats

Sandbox analysis results are automatically returned to the alert, including a clear verdict and a detailed HTML report.

Available Actions

	⊞	🐧	🤖
🔗	URL Windows Analysis	URL Linux Analysis	URL Android Analysis
📄	File Windows Analysis	File Linux Analysis	File Android Analysis

Each action supports flexible configuration (analysis duration, privacy, networking), enabling secure and compliant investigations.

Threat Intelligence Lookup: Add Context for Faster Response

The ANY.RUN Threat Intelligence Lookup Response integration enriches Google SecOps alerts with additional threat intelligence from the ANY.RUN database.

Value for SOC:

- Immediate context for indicators
- Better prioritization of alerts
- Faster understanding of scope and relevance

Value for Business:

- Earlier risk awareness
- Fewer missed threats
- More predictable response outcomes

Lookup results are returned directly in the alert, including a verdict and a detailed JSON report.

Available Actions

ANY.RUN TI Lookup

The action automatically builds a query based on the alert entity, with support for advanced customization across 40+ parameters.

Threat Intelligence Feeds: Use Fresh Intel to Detect Attacks Early

The ANY.RUN Threat Intelligence Feeds Response integration enables automated ingestion of verified network IOCs (IPs, domains, URLs) derived from real sandbox analyses conducted manually by over 600K analysts and 15K SOCs.

Value for SOC:

- Continuous access to fresh, high-confidence indicators
- Reduced noise from low-quality intelligence
- Stronger detection coverage

Value for Business:

- Reduced likelihood of successful attacks
- Better protection against emerging campaigns
- Lower operational and downtime risk

IOCs are stored in structured data tables with labels and confidence scores, making them immediately usable for detection and prevention.

Available Jobs

ANY.RUN TI Feeds

The job supports scheduling and query parameters such as Feed Fetch Depth for flexible ingestion.

Prerequisites

- Google SecOps instance
- ANY.RUN license. Contact your ANY.RUN account manager or submit a **request via the website**.