HYAS

gettyimages
Credit: SmileStudioAP

SOLUTION BRIEF
HYAS Insight

HYAS Insight & Splunk SOAR Integration: Automated Response Powered by Infrastructure Intelligence

Supercharge Your Playbooks with World-Class Infrastructure Intelligence

In today's high-speed threat landscape, time is your most valuable asset. Security teams using Splunk SOAR need automated, reliable, and deep threat intelligence focused on adversary infrastructure to fuel playbooks, reduce investigation time, and make faster decisions.

The HYAS Insight integration with Splunk SOAR delivers exactly that — industry-exclusive infrastructure intelligence, available in real time, automatically, and at machine speed.

With deep data on adversary infrastructure, command-and-control assets, malware infrastructure, and threat attribution, HYAS Insight becomes a force multiplier for any security automation workflow. By embedding HYAS capabilities directly into Splunk SOAR playbooks, analysts can uncover relationships, attribute attacks, and act with confidence — all without manual lookups or external pivots.

> "By embedding HYAS capabilities directly into Splunk SOAR playbooks, analysts can uncover relationships, attribute attacks, and act with confidence."

Key Benefits of the Integration

Automated Infrastructure Enrichment
HYAS Insight turns Splunk SOAR into a high-powered intelligence engine, automatically enriching indicators with WHOIS, DNS, C2 infrastructure, dynamic DNS, malware associations, and more — no analyst intervention required.

Faster, Smarter Playbooks
Integrate HYAS actions into your playbooks to gain deep intelligence earlier in your detection and response workflows. Eliminate time-consuming manual steps and accelerate investigation timelines.

Reduce Alert Fatigue
With meaningful, context-rich data feeding your automated decisions, you can suppress noise, prioritize high-fidelity alerts, and reduce false positives at scale.

Uncover Hidden Threat Infrastructure
Use HYAS Insight to expose attacker-controlled infrastructure that would otherwise remain invisible — allowing you to see not just the symptom of an attack, but its entire supporting ecosystem.

Supported HYAS Insight Actions in Splunk SOAR

The HYAS Insight app for Splunk SOAR includes a wide range of investigative and enrichment actions that can be easily used in automated playbooks or manually during incident response:

- Command & Control Lookup
- WHOIS Lookup
- Dynamic DNS Lookup
- Sinkhole IP Detection
- Passive DNS Intelligence
- Malware Data
- SSL Certificate Lookup
- OS Indicators & Device Intelligence

Example Use Cases

Automated Infrastructure Enrichment
As alerts are ingested by Splunk SOAR, HYAS Insight enriches indicators with infrastructure intelligence — adding key context around adversary attribution, domain history, malware connections, and more.

Playbook-Driven Attribution
HYAS data can link domains, IPs, and hashes to known threat actors and campaigns, enabling your SOAR platform to prioritize high-risk alerts automatically or escalate them based on intelligence criteria.

Threat Containment and Triage
Investigate and contain threats faster by knowing if an IP or domain is part of a C2 network, a sinkhole, or has been involved in malware campaigns.

Proactive Threat Sweeps
Build scheduled or triggered playbooks that leverage HYAS Insight to sweep your environment for emerging infrastructure tied to specific actors, malware families, or tactics.

gettyimages
Credit: Jacob Wackerhausen

How to Get Started

1. Download the App
Find the HYAS Insight App for Splunk SOAR on Splunkbase.

2. Install & Configure
Follow the in-app steps to connect your Splunk SOAR instance to HYAS Insight using your API credentials.

3. Build Your Playbooks
Start enriching, escalating, and responding with intelligence-powered automation. Use HYAS actions directly in your SOAR workflows to supercharge threat response.

About HYAS

HYAS is the world's premier provider of infrastructure intelligence, enabling organizations worldwide with unparalleled visibility, protection, and the necessary proactive intelligence to address cyber attacks, fraud, and all forms of digital risk. With real-time visibility into adversary infrastructure and their related devices, HYAS Insight allows security teams to track, monitor, and dismantle cyber threats and fraud with unmatched speed and precision.

Want to see it in action?
Contact us at info@hyas.com or visit www.hyas.com to learn more or schedule a demo.

HYAS Products

HYAS security solutions provide the visibility and observability needed to stay in control of your environment. HYAS solutions are easy to deploy, easy to manage, and integrate seamlessly into any security stack.

PROTECTIVE DNS

HYAS Protect

Protective DNS

Our protective DNS solution combines authoritative knowledge of attacker infrastructure and domain-based intelligence to proactively block malicious communication used by cybercriminals to conduct phishing, ransomware, and other forms of cyberattacks.

Explore HYAS Protect →

THREAT INTELLIGENCE & INVESTIGATION

HYAS Insight

Threat Intelligence & Investigation

HYAS Insights allows you to rapidly discover and investigate any IOC and related indicators. Identify and map out the complete cybercriminal campaign architecture and take a proactive stance against future attacks.

Explore HYAS Insight →

Recent Malware Infrastructure
Daily Detonation Volume by Malware Family
Distribution by Top Malware Tags
Distribution by Top C2 ASN Countries
12161
Total

Contact Us For a Demo
hyas.com/contact

HYAS

Protecting Businesses and Solving Intelligence Problems Through Detection of Adversary Infrastructure and Anomalous Communication Patterns

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS is dedicated to protecting organizations and solving intelligence problems through detection of adversary infrastructure and anomalous communication patterns.

We help businesses see more, do more, and understand more in real time about the nature of the threats they face. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable.

HYAS.COM / INFO@HYAS.COM
DUNS #24-735-0333