




SOLUTION BRIEF  
HYAS Insight

# HYAS Insight & Splunk Enterprise Integration: Uncover Hidden Threats with Infrastructure Intelligence

**Empower Your Security Operations with Deeper, Actionable Intelligence**

As cyber threats grow more sophisticated and persistent, security teams need more than just alerts — they need context. They need to understand the infrastructure behind the attack, who is running it, and how it connects to broader campaigns. The integration of HYAS Insight with Splunk Enterprise gives security teams the ability



to enrich and correlate events with world-class infrastructure intelligence — all within the Splunk environment they already use every day.

HYAS Insight is trusted by global security teams to provide exclusive, real-time visibility into adversary infrastructure — including domains, IPs, malware hashes, SSL certificates, and more — giving analysts the context they need to make faster, more confident decisions.

## Key Benefits of the Integration

### Unmatched Infrastructure Context

HYAS Insight delivers intelligence beyond traditional feeds — exposing the infrastructure and relationships behind malicious domains, IPs, and threat actors. This intelligence provides deeper attribution, links disparate events, and reveals the full scope of malicious campaigns.

### Native Splunk Integration

HYAS Insight integrates directly into Splunk Enterprise via a dedicated app, enabling users to enrich events and alerts without switching tools. Custom search commands and pre-built dashboards make it easy to pivot from indicators to insights in seconds.

### Accelerated Investigations

With real-time data from HYAS Insight embedded into Splunk, analysts can go from detection to full infrastructure mapping faster than ever. Pre-integrated with Splunk Enterprise Security (ES), users can trigger adaptive response actions to enrich alerts as they come in.

### Reduce Analyst Burnout

By providing meaningful context and eliminating manual research, HYAS Insight helps SOC teams focus on what matters — responding to threats instead of chasing down leads.



“HYAS Insight is trusted by global security teams to provide exclusive, real-time visibility into adversary infrastructure.”

## Core Capabilities

- **Search-Powered Threat Enrichment**

Use HYAS's custom Splunk search commands to enrich IOCs (domains, IPs, hashes, emails, phone numbers) with detailed infrastructure intelligence — including passive DNS, WHOIS, C2 attribution, malware associations, SSL details, and more.

- **On-Demand Lookups**

Quickly investigate individual indicators through a user-friendly enrichment dashboard in Splunk. Select your indicator type, submit a query, and view contextual intelligence instantly.

- **Splunk ES Adaptive Response**

For customers using Splunk Enterprise Security, HYAS Insight adds enrichment actions to the Incident Review panel, allowing teams to trigger insights inline with alert triage — no pivoting required.

- **Support for a Wide Range of Indicators**

HYAS Insight enables lookups across domains, IP addresses (IPv4/IPv6), email addresses, phone numbers, and file hashes (SHA256, SHA1, MD5, SHA512).





## Example Use Cases

### Threat Hunting

Start with a suspicious domain or IP and use HYAS Insight data to map related infrastructure, identify connected malware, and uncover deeper threat patterns.

### Incident Response

During investigations, instantly enrich IOCs with passive DNS, WHOIS, and malware associations to determine impact and attribution.

### Alert Triage

Use HYAS's adaptive response actions in Splunk ES to add critical context to alerts, reducing false positives and enabling faster decision-making.

### Campaign Attribution

Link seemingly unrelated indicators to shared infrastructure or threat actors using exclusive HYAS datasets.s.

## How to Get Started

### 1. Download the App

Find the HYAS Insight App for Splunk on [Splunkbase](#).

### 2. Install & Configure

Set up the app in your Splunk Enterprise environment and configure your HYAS Insight API credentials.

### 3. Start Enriching

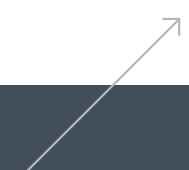
Use the pre-built dashboards, custom search commands, and Splunk ES integration to start enriching data and accelerating investigations immediately.

## 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](mailto:info@hyas.com) or visit [www.hyas.com](http://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 



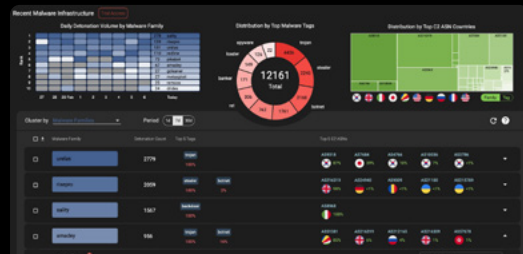
## THREAT INTELLIGENCE & INVESTIGATION

### 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 



Contact Us For a Demo  
[hyas.com/contact](https://hyas.com/contact)



## 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.