




SOLUTION BRIEF HYAS Insight

HYAS Insight & Cortex XSOAR Integration: Automated Response Powered by Infrastructure Intelligence

Proactively Enrich and Accelerate Investigations with Infrastructure Intelligence

The integration of **HYAS Insight** with **Cortex XSOAR** brings unmatched threat context and infrastructure intelligence directly into your automated workflows. By combining HYAS's deep visibility into adversary infrastructure with



XSOAR's leading orchestration and automation capabilities, security teams can accelerate incident response, reduce manual effort, and make smarter, faster decisions.

Key Features

Comprehensive Threat Intelligence

Access detailed intelligence on domains, IPs, malware samples, C2 infrastructure, WHOIS data, and more—all from HYAS Insight's rich dataset.

Automated IOC Enrichment

Automatically add infrastructure context to indicators of compromise (IOCs) during investigation and response workflows within Cortex XSOAR.

Playbook Integration

Leverage HYAS Insight data in your custom XSOAR playbooks to automate triage, enrichment, and response actions.

On-Demand Lookups

Perform real-time queries within the XSOAR interface using pre-built commands—no pivoting or additional tools required.



Benefits

- **Deeper Threat Context:** Get insights beyond basic indicators, including attribution and infrastructure relationships.
- **Streamlined Workflows:** Integrate directly into playbooks to automate enrichment at scale.
- **Faster Response Times:** Automatically enrich incidents and alerts, reducing time to action.
- **Improved Accuracy:** Use infrastructure intelligence to validate and prioritize threats with greater confidence.



Use Cases

Incident Enrichment

Enrich alerts in real time with actionable intelligence on related domains, IPs, C2 infrastructure, and malware activity.

Threat Hunting

Use infrastructure links to proactively investigate suspicious activity and uncover hidden threats.

Phishing Detection

Uncover malicious infrastructure behind suspicious domains using WHOIS and DNS data from HYAS Insight.

Malware Attribution

Understand malware campaigns and infrastructure reuse by analyzing attacker infrastructure and command-and-control relationships.

Integration Details

Supported Platform Versions:

Cortex XSOAR 6.0.0 and later

Authentication:

HYAS Insight API key required

Available Commands:

- hyas-get-passive-dns-records-by-indicator
- hyas-get-whois-records-by-indicator
- hyas-get-malware-sample-records-by-indicator
- hyas-get-c2-attribution-records-by-indicator
- Additional commands for DynamicDNS, passive hash, SSL certificate, and OSINT indicators

How to Get Started

1. **Obtain an API Key** from your HYAS administrator or support team
2. **Configure HYAS Insight** in the Cortex XSOAR integrations settings
3. **Test and Deploy** enrichment workflows or add HYAS commands to existing playbooks

More setup info:

[HYAS Insight Integration Docs](#)

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?

Learn more: www.hyas.com



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 →



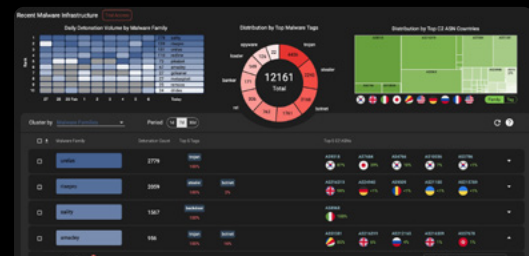
THREAT INTELLIGENCE & INVESTIGATION

HYAS Insight

Threat Intelligence & Investigation

HYAS Insight 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



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.