




SOLUTION BRIEF  
HYAS Insight

# HYAS Insight + Microsoft Sentinel Integration: Security Operations Elevated by Infrastructure Intelligence

## **Proactively Disrupt Threat Campaigns Before They Escalate**

The integration between HYAS Insight and Microsoft Sentinel transforms traditional reactive security into proactive cyber defense. With direct access to HYAS's proprietary infrastructure intelligence from within the Sentinel ecosystem, security teams can uncover the unseen: adversary



infrastructure connections, reused infrastructure across campaigns, and malicious communication paths that typically go unnoticed.

Whether you're responding to an incident or hunting proactively, this integration allows analysts to detect patterns earlier, understand attacker intent, and dismantle the infrastructure behind threats—faster and with greater certainty.

## Key Features

### Infrastructure Intelligence

Visualize and traverse relationships between IOCs and attacker infrastructure using enriched intelligence sourced directly from HYAS Insight.

### Embedded Investigative Context

HYAS data is embedded in Sentinel incidents to add attribution, historical context, and related infrastructure—without leaving your workspace.

### Customizable Logic App Connectors

Tailor enrichment and response workflows using Azure Logic Apps that trigger HYAS queries based on custom alert thresholds and incident types.



“The integration between HYAS Insight and Microsoft Sentinel transforms traditional reactive security into proactive cyber defense.”

### Search-Driven Threat Analysis

Go beyond basic lookups and uncover the full story behind any domain, IP, nameserver, or infrastructure object. Instantly surface global infrastructure reuse patterns, cross-campaign connections, and crucial context—like when and how an asset was weaponized, whether it poses a threat, and what it means for your organization.

## Benefits

### See the Whole Picture

Move beyond isolated indicators—understand infrastructure relationships and attacker ecosystems.

### Anticipate Threat Behavior


Spot reused infrastructure and uncover dormant or developing campaigns before they cause harm.

### Minimize Investigation Fatigue

Reduce alert overload by adding relevance and confidence through intelligent enrichment.

### Accelerate Time to Containment

Use context-rich data to confirm threats faster, guide automation, and get to containment faster.



## Use Cases

### Campaign Tracking Across Alerts

Correlate new incidents with prior events by linking indicators to known adversary infrastructure and previously seen malicious activity.

### Expose Pre-Weaponized Infrastructure

Reveal “quiet” infrastructure that will support malicious operations but hasn’t yet been weaponized, enabling preemptive defense.

### Investigative Reporting

Export enriched findings for internal teams or executive briefings to illustrate how threats were linked, triaged, and neutralized.

## Integration Details

### Platform:

Microsoft Sentinel (cloud-native SIEM + SOAR)

### Authentication Method:

HYAS Insight API Key required

### Integration Options:

- Azure Logic Apps
- Custom Playbooks
- Data Connector via REST API

### Available Enrichment Endpoints:

- Passive DNS and WHOIS
- Malware infrastructure links
- C2 attribution
- Dynamic DNS usage
- SSL cert relationships

## How to Get Started

1. **Obtain your HYAS Insight API Key** from your HYAS account activation email.
2. **Install the HYAS connector** and deploy Logic Apps or Playbooks using the Sentinel UI.
3. **Test your workflows**, verify successful lookups and enrichment flows.
4. **Tune automation rules** to invoke HYAS lookups for relevant alerts.



## 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](http://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 →



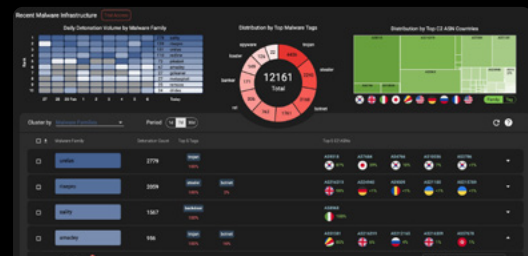
## THREAT INTELLIGENCE & INVESTIGATION

### 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](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.