

SOLUTION BRIEF
HYAS Insight + MISP Integration

Supercharge Threat Intelligence Sharing with Infrastructure Intelligence

The integration of HYAS Insight with MISP (Malware Information Sharing Platform & Threat Sharing) combines HYAS's unique infrastructure intelligence with one of the world's leading open-source threat intelligence platforms. This powerful combination enhances the quality, depth, and operational value of threat intelligence sharing, empowering security teams and communities to collaborate more effectively and respond to emerging threats with speed and precision.



Key Benefits

Enriched Threat Context

HYAS Insight adds unparalleled infrastructure intelligence, including WHOIS, passive DNS, malware attribution, and C2 infrastructure relationships, to indicators shared within MISP.

Accelerated Investigations

Security analysts can pivot rapidly between related indicators, uncovering hidden adversary infrastructure and connections.

Improved Threat Prioritization

Deep context allows better scoring, validation, and prioritization of IOCs, improving operational decision-making.

Strengthened Collaboration

Shared intelligence in MISP is amplified with HYAS Insight's data, enabling participants to benefit from richer, actionable insights.

Proactive Defense

Early visibility into adversary infrastructure allows for earlier detection, threat hunting, and preemptive defense strategies.

Key Features

- API-based enrichment of domains, IP addresses, and file hashes
- Retrieval of WHOIS records, passive DNS data, and malware sample associations
- Infrastructure correlation, including C2 attribution and Dynamic DNS relationships
- Real-time lookups or scheduled batch enrichment jobs
- Full audit trail within MISP to track enrichment actions

How It Works

The integration leverages HYAS Insight's robust API to enrich indicators within MISP. As new IOCs are ingested or shared in MISP, enrichment jobs query HYAS Insight for additional intelligence, which is automatically appended to the original event or IOC records.

Deployment / Getting Started Steps

1. Obtain a HYAS Insight API key from your HYAS administrator..
2. Install or configure the HYAS Insight enrichment module or connector within your MISP instance.
3. Set enrichment rules to automatically query HYAS Insight upon ingestion of new indicators.
4. Validate enrichment data and operationalize within your threat intelligence workflows.
5. Consult HYAS Insight and MISP integration documentation for full deployment details.



Use Cases

IOC Enrichment

Automatically augment shared indicators with deep infrastructure intelligence.

Threat Hunting

Correlate indicators across shared MISP data and HYAS Insight to reveal broader adversary campaigns.

Incident Response

Speed up investigations by providing responders with richer context on involved infrastructure.

Attribution

Connect disparate IOCs to threat actor infrastructure and campaigns using HYAS Insight's unique data.

Community Intelligence Sharing

Empower threat sharing communities with enriched, actionable data.

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.



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 →



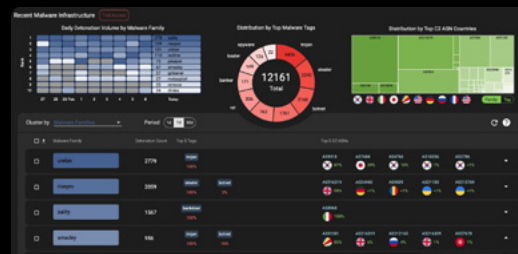
THREAT INTELLIGENCE & INVESTIGATION

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.