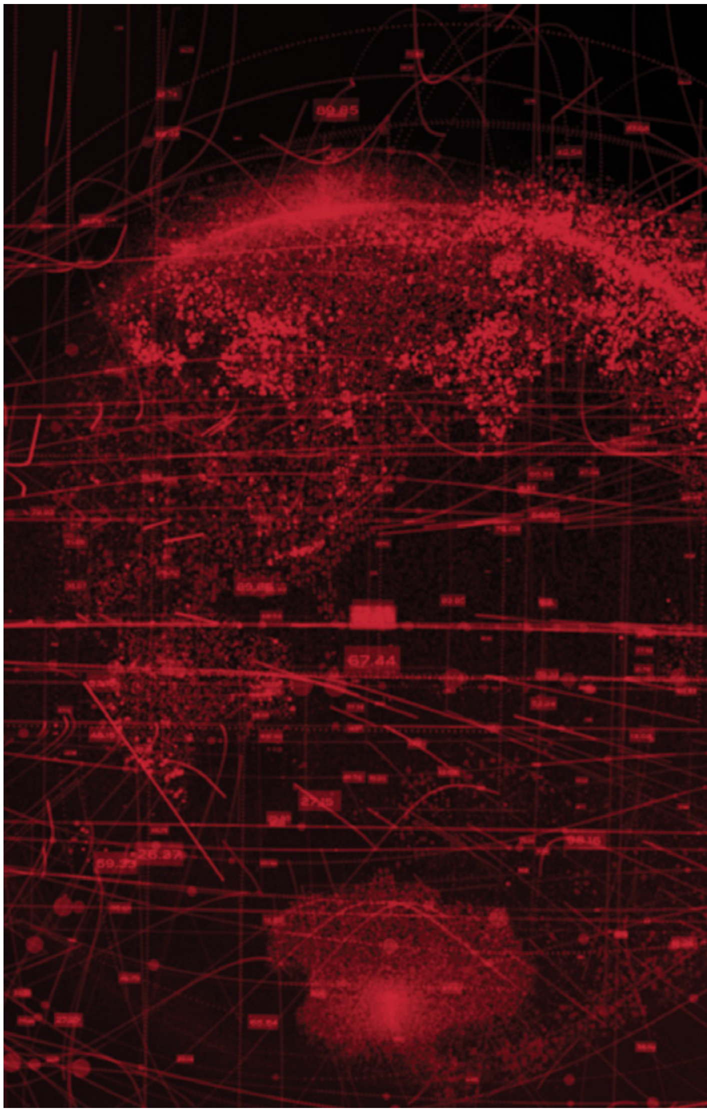
CASE STUDY

Essential Threat Intelligence **for a Leading Global Managed Service Provider**



As one of the largest managed service providers in the world, how can you ensure security not just across your own organization but also for your valued clients?

A leading professional services firm with global reach – known hereafter as MSPGlobal to protect its anonymity – found that its best cybersecurity posture was designed well ahead of implementation. In other words, instead of fighting illegal activity from a defensive position, it made more sense to nail down predetermined technical specifications and build a complete and comprehensive security stack with those specifications firmly in mind.

MSPGlobal* offers clients in 150 countries a variety of managed services – either as a set, combined, or individually – including:

- Security-operations-center (SOC)-as-a-Service (SOCaaS)
- Threat-Hunting-as-a-Service (THaaS)
- Intelligence-as-a-Service (IaaS)

As an international company that offers security services to its customers, the firm's own cybersecurity stance must be unparalleled. The delivery of these services often involves intelligence reports – specific to an array of sectors and industries – backed up with the kind of solid, powerful data that HYAS gathers; namely, intelligence on adversary infrastructure and nefarious domain name system (DNS) activity.

> **"When we onboard the clients, we try to understand what their business is: What they do and what their crown jewels are that they're trained to protect. From there, we can define intelligence requirements."**

Cybersecurity Challenges and Choices

When MSPGlobal's* intelligence team onboards new clients, they want to gain a thorough understanding of each client's sector – both its business and its priorities – e.g., "the crown jewels they're trying to protect," says the consultancy's intelligence manager.

The objective of onboarding is to define intelligence requirements for each client. MSPGlobal* aims to understand what its customers want to achieve by identifying the threats that concern them most. Threats that MSPGlobal's clients' competitors face can also play into these concerns.

MSPGlobal* is then well-positioned to report on the threats to each client, providing deep, unrivaled, industry-specific analysis.

> **"The business case for HYAS is straightforward: To be able to understand and perform research on threat infrastructure, you need a certain amount of datasets – passive DNS and Whois information – to be able to support the DNS team."**

Clients are free to ask questions of MSPGlobal* – which its intelligence manager admits doesn't happen as often as it should. But the global firm's ultimate goal is to update those they serve about the threat landscape at any given time, along with recommendations the clients should apply.

Begin With the End In Mind

MSPGlobal's* intelligence manager says that the business case for HYAS Insight threat intelligence and investigation platform and incident response capabilities is straightforward.

However, the need for an adversary infrastructure platform came up early on when MSPGlobal was building its security-as-software services.
To formulate its collection strategy, MSPGlobal had to answer its own questions about the requirements a company would need to deliver services like SOCaaS, THaaS, and IaaS.

To achieve the objective of being as informative as possible for its clients, the firm needed *a lot* of data – and people who could analyze it. But not just any data. They needed the *right* data.

The Hunger for More Data

Effective threat hunting demands intelligence teams that can understand and research threat, or adversary, infrastructure quickly and thoroughly. A deep understanding of the myriad threats enterprises face today requires as many relevant datasets as possible.

This includes information about passive and dynamic DNS, as well as WHOIS information that cybersecurity teams use to research and stop threats – all in support of their wider organizational functions and missions. Data about DNS and adversary infrastructure are HYAS' bread and butter, ripening the potential for fruitful partnerships with companies likeMSPGlobal.*

Depth of Insight

To stay ahead of attackers and adversaries, HYAS Insight provides a range of benefits, including:

- **Increased case closures** with unique data allowing security teams to pivot between data points and map adversary infrastructure.
- **Authorities assistance,** by providing investigators with the information they need to determine where attacks originated and where bad actors might deploy them next.
- **Progress tracking** for easy reference and navigation with a saveable and shareable trail.
- **Alert settings that notify security teams** about newly registered suspicious domains.
- **The ability to prioritize precautionary measures** by tracking bad actors' activity through account logins, report runs and maintenance performance.

Telling a Better Story

A wide range of datasets isn't enough anymore. Most organizations don't just need more data, they need to be able to do something *meaningful* with the data they have. For MSPGlobal,* they needed not only data enrichment, but context on that data, such as correlation and causation.

By connecting with colleagues across the organization and joining datasets together, MSPGlobal's* intelligence and incident response teams benefit from multiple perspectives on the same observed phenomena.

For example, if one team knows a domain is being used for nefarious activity, they can check a variety of different sources to gain a broader picture about that domain, and perhaps find new data to share within the company, strengthening the organization overall.

> **"HYAS' solution is simple to use: you can get the information that you need. HYAS Insight ... provides access to more data points on a single pane."**

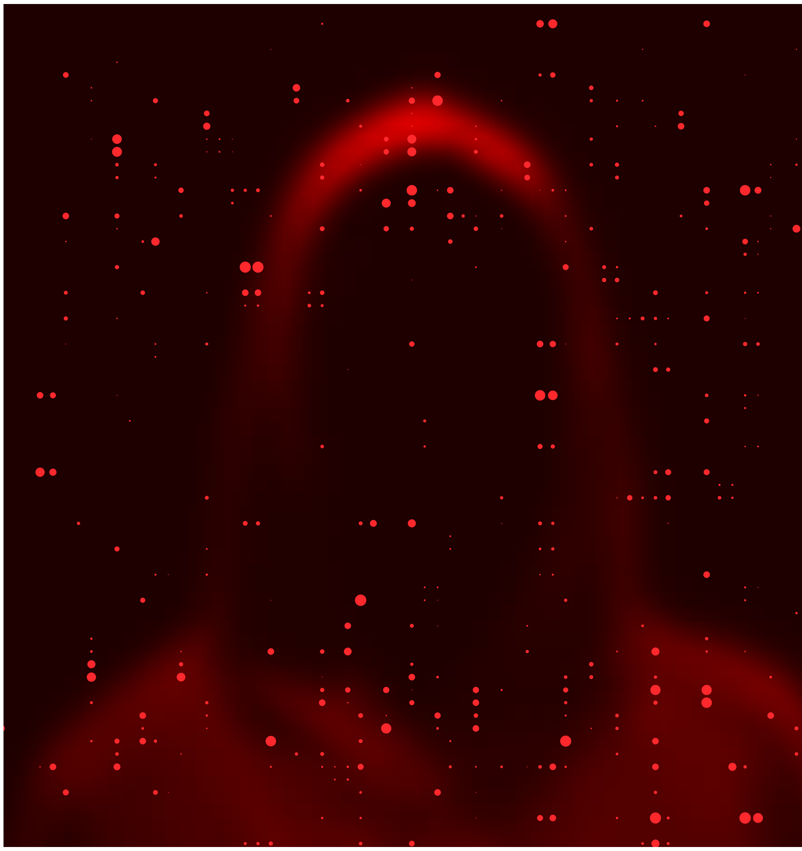
Ultimate Business Use Cases

MSPGlobal's* intelligence team found HYAS Insight threat intelligence and investigation platform to be straightforward to use,, but HYAS Insight comes with more advanced data presentation, features, and capabilities – along with access to additional data points on the same, single pane of glass.

MSPGlobal* was inevitably beholden to budgetary pressure when assessing potential vendors that had the intelligence tools to meet its security goals.

"I like to have multiple data points and sources," the company's intelligence manager explains. "Because the more you have, the better visibility you have."

A deep understanding of adversary infrastructure is critical, and tools like HYAS Insight significantly amplifies the intelligence major players like MSPGlobal* require to stay ahead of the curve when it comes to cyber security and defense. The intelligence manager said the ideal combination would be to leverage the threat intelligence of HYAS Insight and HYAS Protect for its Protective DNS capabilities.



Business Process Workflow

As MSPGlobal's* intelligence team grows and builds automation that better connects its systems, the intelligence manager hopes his team will be able to identify which sources provide which data on a more granular level.

"I should be able to tell which sources are better, more valuable and impactful," he explains.

Meanwhile, MSPGlobal's* intelligence team follows a preset process. Typically, whether the team uses HYAS Insight first or second in the process depends on its goals. If the MSPGlobal* team wants to investigate threats it knows about – cataloged via other intelligence tools – it can use HYAS to respond to each incident and if they want to find out more about a threat, the team can go straight to the platform to investigate.

Augmented Intelligence Infrastructure

HYAS is the company's go-to investigative tool – which is especially critical for expansive digging into adversary infrastructure and botnets.

The Power of Understanding Through Connecting the Dots

"Connecting the dots" is a fundamental part of threat intelligence, and security teams are weaker when they don't (or can't) do this effectively. HYAS Insight provides rich data that can be cross-referenced and molded into "stories" that trace origins, evolutions, and correlations that can identify and stop nefarious activity.

"Different data points help you understand not just what you're looking at, but also what's beyond," MSPGlobal's* intelligence manager says.

Collaborations and integrations between companies like HYAS and Maltego (the latter provides additional tools to MSPGlobal's* intelligence team) further strengthen those stories.

HYAS Delivers the Goods

With HYAS Insight in place, MSPGlobal* has been able to deliver for its clients, add value across its stack and improve its own operational efficiency through:

- **Stopping fraudulent activity:** In one case, a fraudster registered multiple domains to sell fake labeled goods. HYAS Insight's data on these domains enabled the intelligence manager to cross-reference Insight with other tools. He then returned to Insight's social media map – allowing for address inputs – and pinpointed what was necessary to terminate the illegal activity.
- **Dynamic DNS threat hunting:** MSPGlobal* pursued a DNS hijacker based in Iran using HYAS' passive DNS data, including information about the clients and industries the bad actor was most likely to strike next.

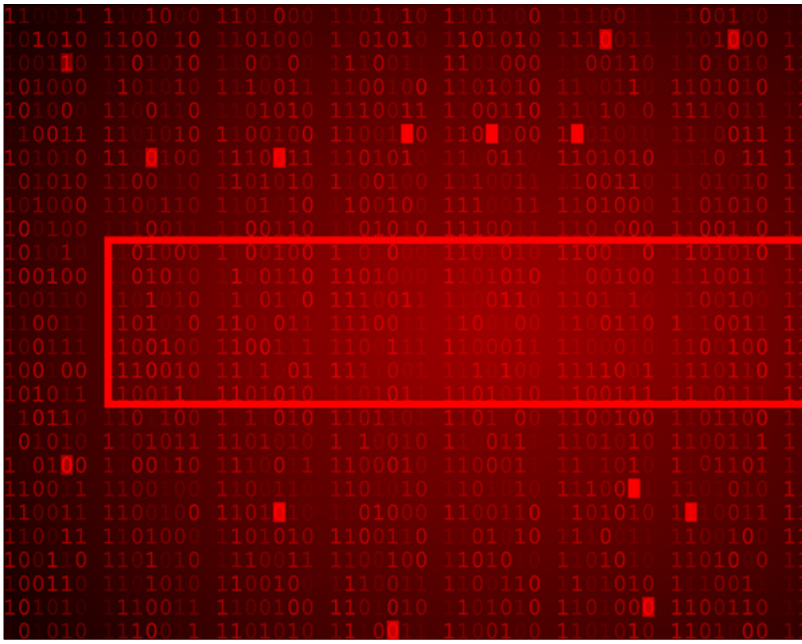
Every win for MSPGlobal* is a win for its clients. Confident reassurance in a strong cybersecurity posture means more focus on daily operations and less on mitigating damage against threat actors.

> **"HYAS is really easy to work with. We have a very good relationship with the entire team."**

Unparalleled Threat Protection

HYAS Insight threat intelligence and investigation platform:

- **Expands threat visibility with unique datasets** by connecting specific attack instances and campaigns to billions of indicators of compromise.
- **Highlights adversary infrastructure –** even if attack origins are hidden behind VPNs – and **detects, identifies, and monitors** that infrastructure with proactive alerts on adversary activity to help preempt attacks prior to their inclusion on conventional blacklists.
- **Provides cybersecurity risk assessment,** backed up by unique, diverse datasets that help prioritize investigations and incident response.
- **Features easy integration with existing toolsets, workflows and security stacks,** quickly and efficiently deployed in minutes.



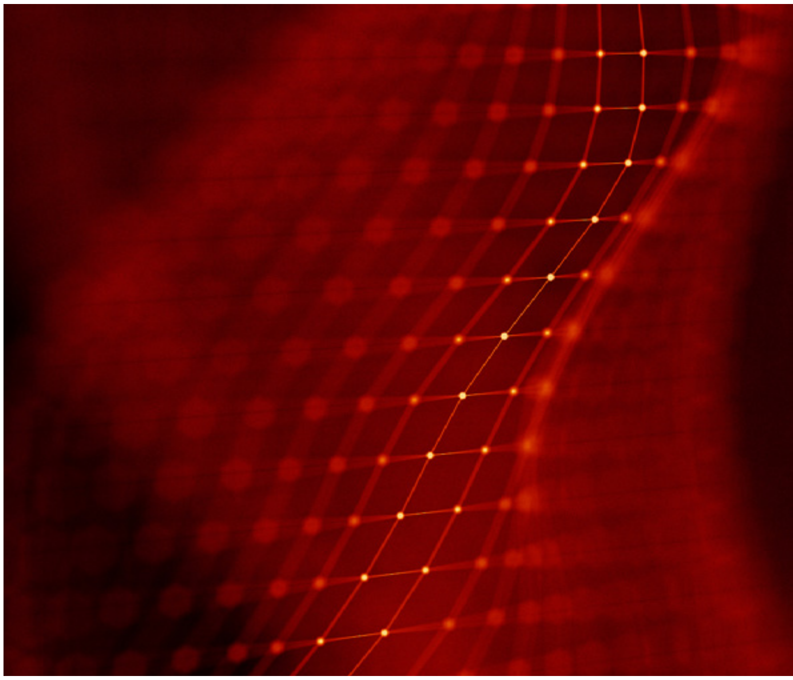
Strengthening Relationships and Defenses in Equal Measure

Behind every large multinational corporation are people working to serve clients and keep them safe.

The MSPGlobal* intelligence team's success is in no small part due to strong relationships with its top vendors, just as MSPGlobal's overall achievements can be credited to going above and beyond for its clients.

MSPGlobal's* intelligence manager says HYAS has always been "really easy to work with," adding that the relationship between the two companies has "always been good."

When companies work well together, the business of keeping people safe gets a whole lot easier.



> **"I've done a lot of investigations around threats using dynamic DNS, so we were able to pursue that with the HYAS solution."**

CONTACT US FOR A DEMO
hyas.com/contact

INVESTIGATE ATTACK
INFRASTRUCTURE FURTHER
AND IDENTIFY FRAUD FASTER

HYAS INSIGHT

An efficient and expedient investigation is the best way to protect your enterprise. HYAS Insight provides threat and fraud response teams with unparalleled visibility into everything you need to know about the attack. This includes the origin, current infrastructure being used and any infrastructure.

*"MSPGlobal" is an alias we used to protect the anonymity and privacy of this international leading professional services firm.

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