Product Briefing

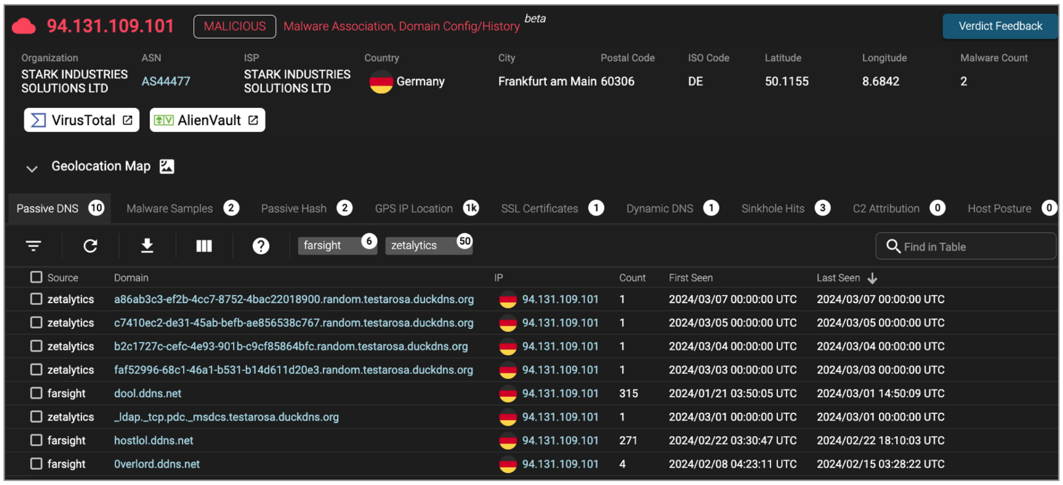
Threat Hunting with HYAS Insight: Insights from the 2024 SANS Institute Survey

March 2024

Today's complex and fast-changing threat environment means security professionals need highly advanced threat hunting technologies to ensure that they're always one step ahead of the bad actors out there. This year's edition of the annual SANS Institute threat hunting survey shows increasing enterprise recognition of the importance, and the challenges, of this essential security discipline.

HYAS Insight

HYAS Insight is an external threat intelligence application used by security professionals worldwide, including threat hunters, security operations center (SOC) analysts, cyber threat intelligence (CTI) teams, and fraud investigators. HYAS' client base includes enterprises across industry verticals like financial services, healthcare, and high-tech, as well as government entities, law enforcement agencies, and even other cybersecurity service providers. HYAS Insight aggregates, analyzes, and distills threat and adversary information from HYAS' adversary infrastructure data lake, which transacts billions of data points daily. HYAS packages this intelligence in highly adaptable and customizable formats that are accessible and actionable for both sophisticated threat hunters and less skilled security practitioners. See Figure 1.



Organization	ASN	ISP	Country	City	Postal Code	ISO Code	Latitude	Longitude	Malware Count
STARK INDUSTRIES SOLUTIONS LTD	AS44477	STARK INDUSTRIES SOLUTIONS LTD	Germany	Frankfurt am Main	60306	DE	50.1155	8.6842	2

□ Source	Domain	IP	Count	First Seen	Last Seen
□ zetalytics	a86ab3c3-ef2b-4cc7-8752-4bac22018900.random.testarosa.duckdns.org	94.131.109.101	1	2024/03/07 00:00:00 UTC	2024/03/07 00:00:00 UTC
□ zetalytics	c7410ec2-de31-45ab-befb-ae856538c767.random.testarosa.duckdns.org	94.131.109.101	1	2024/03/05 00:00:00 UTC	2024/03/05 00:00:00 UTC
□ zetalytics	b2c1727c-cefc-4e93-901b-c9cf85864bfc.random.testarosa.duckdns.org	94.131.109.101	1	2024/03/04 00:00:00 UTC	2024/03/04 00:00:00 UTC
□ zetalytics	faf52996-68c1-46a1-b531-b14d611d20e3.random.testarosa.duckdns.org	94.131.109.101	1	2024/03/03 00:00:00 UTC	2024/03/03 00:00:00 UTC
□ farsight	dool.ddns.net	94.131.109.101	315	2024/01/21 03:50:05 UTC	2024/03/01 14:50:09 UTC
□ zetalytics	_ldap._tcp.pdc._msdcs.testarosa.duckdns.org	94.131.109.101	1	2024/03/01 00:00:00 UTC	2024/03/01 00:00:00 UTC
□ farsight	hostlol.ddns.net	94.131.109.101	271	2024/02/22 03:30:47 UTC	2024/02/22 18:10:03 UTC
□ farsight	0verlord.ddns.net	94.131.109.101	4	2024/02/08 04:23:11 UTC	2024/02/15 03:28:22 UTC

Figure 1. Typical IOC Detail Showing HYAS Insight Verdict, Context Enrichment, and Third-Party Integrations

This is made possible by an API-first architecture with hundreds of endpoints to support specific client use cases, as well as by integration with a broad range of other security technologies, including security incident and event management (SIEM); security orchestration, automation, and response (SOAR); endpoint detection and response (EDR); and data visualization and analysis tools. The result: Enterprises have a straightforward,

Key Findings from the 2024 SANS Threat Hunting Survey

The scarcity of threat hunting skills at all levels remains an overwhelming problem for security organizations, with 50% of survey respondents identifying it as their No. 1 obstacle to improved threat detection and response.

The need for improved contextual awareness is now clearly recognized, with more than half of the respondents planning to refine their threat hunting efforts with better data sources and tools.

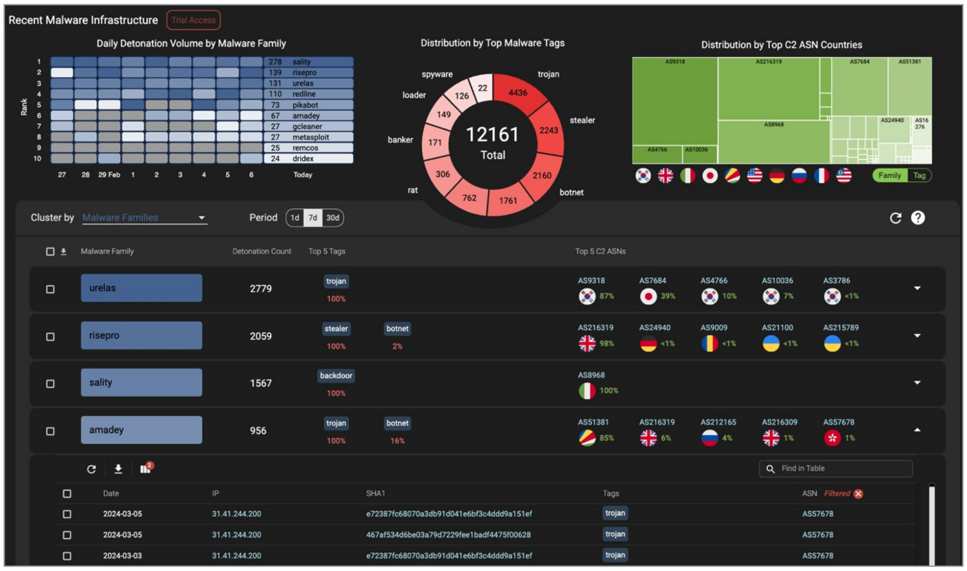
easy-to-use and cost-effective means of leveraging their threat hunting capabilities. Proactively identifying, prioritizing, and addressing threats of all types—whether ransomware attacks, insider threats, or advanced persistent threats (APTs)—becomes achievable *before* they can become weaponized.

HYAS Insight addresses many of the most critical challenges identified by the respondents to this year's SANS threat hunting survey. Let's take a close look at two of the most important:

- **The difficulty of attracting and retaining personnel with threat hunting skills.** Threat hunting is rapidly maturing as a security discipline, but highly skilled threat hunters are still hard to find—and expensive. HYAS Insight helps enterprises make the most of these scarce professionals' skills, by giving them the highly granular threat information they need to act rapidly and efficiently. But HYAS also recognizes the need to enable security professionals with less threat-hunting experience. HYAS Insight provides actionable and relevant intelligence that less experienced operators can use, while providing seasoned operators with detailed technical intelligence that helps them "connect the dots." This makes it possible for SOCs to optimize the resources they have and develop their threat hunting maturity—and does it without increasing headcount and associated costs.
- **The need for formal threat hunting methodologies.** HYAS Insight takes a highly formalized approach to threat intelligence, focusing on the three areas its clients have identified as their most critical: verdicts on adversary infrastructure, like indicators of compromise (IOCs); related infrastructure that better characterizes a threat; and threat actor information that further characterizes the people and organizations behind malicious activity. This makes it possible for threat hunters to readily make sense of threat and adversary patterns and respond effectively to those that are most relevant to them.

The concept of "pivot crawling" is central to HYAS Insight's ability to quickly provide threat hunters with actionable intelligence. Pivot crawling is a proprietary HYAS innovation that assembles data, static rules, and data science methods (both generative AI and machine learning algorithms) to make contextual sense of a vast array of threat intelligence. Interestingly—and somewhat paradoxically—pivot crawling not only assists with formal threat hunting methodologies, but also makes it possible for security organizations to rapidly develop *informal*, ad hoc threat hunts when circumstances demand them. Pivot crawling enables threat hunters to contextualize and prioritize threats that are most relevant to a specific user's requirements.

Here's a real-world example: HYAS Insight was recently able to prevent an attack targeting one of its banking clients' partner ecosystems, using highly refined, client-specific information—including geosourcing data—to identify the threat as coming from a known Russia-based group using infrastructure located in the UK. Not only was the attack stopped dead in its tracks, but HYAS Insight was able to provide forward-looking insight into ways the group might adapt its techniques in the future. See Figure 2.



☐	Malware Family	Detonation Count	Top 5 Tags		Top 5 C2 ASNs				
☐	urelas	2779	trojan 100%		AS9318 87%	AS7684 39%	AS4766 10%	AS10036 7%	AS3786 <1%
☐	risepro	2059	stealer 100%	botnet 2%	AS216319 98%	AS24940 <1%	AS9009 <1%	AS21100 <1%	AS215789 <1%
☐	sality	1567	backdoor 100%		AS8968 100%				
☐	amadey	956	trojan 100%	botnet 16%	AS51381 85%	AS216319 6%	AS212165 4%	AS216309 1%	AS57678 1%

☐	Date	IP	SHA1	Tags	ASN Filtered
☐	2024-03-05	31.41.244.200	e72387fc68070a3db91d041e6bf3c4ddd9a151ef	trojan	AS57678
☐	2024-03-05	31.41.244.200	467af534d6be03a79d7229fee1badf4475f00628	trojan	AS57678
☐	2024-03-03	31.41.244.200	e72387fc68070a3db91d041e6bf3c4ddd9a151ef	trojan	AS57678

Figure 2. Recent Malware Infrastructure Showing High-Level Patterns and Ability to Drill Down into the Tactical Intelligence

The bottom line: HYAS insight makes it possible for security organizations to make the most of their available threat hunting resources, completing more threat hunts and closing more cases. The vast array of threat intelligence HYAS Insight makes available—and, crucially, the way it makes sense of that intelligence—enables threat hunters and other security practitioners to better know their adversaries, understand their evolving tools and techniques, and both efficiently and cost-effectively protect their attack surface and increase organizational resiliency.

To learn more about HYAS' threat hunting capabilities, visit **www.hyas.com**.

SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos **represents the ninth edition of SANS Institute's survey of security professionals engaged in or impacted by this proactive approach to identifying and remediating previously unknown or undetected security threats. The sponsors of this year's survey all offer advanced threat hunting capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting product briefings on their relevant product and service offerings. Note that SANS Product Briefings do not represent a SANS endorsement of a sponsor or its products, but rather an overview of its offerings and their capabilities.**