HYAS

SOLUTION BRIEF

HYAS™ AND THREATCONNECT

Threat Intelligence Playbook

HYAS Insight enables Security Operations (SOC), Incident Response (CSIRT), and Threat Intelligence teams to dramatically speed their investigations by quickly understanding adversary infrastructure.

With HYAS Insight, ThreatConnect Platform users can save dozens of hours per month by enriching investigations with high fidelity domain name information, as part of threat hunting and incident response playbooks. Users can also automate domain blocking for preemptive protection via ThreatConnect Platform integrations with existing security infrastructure.

CHALLENAGES

Accelerating Investigations

Within the SOC and CSIRT, teams struggle to identify adversaries and enumerate their infrastructure. With the deluge of incoming threat indicators, prioritizing events and understanding which are most severe is a challenging task.

Gaining Visibility into Your Adversary

Adversary tradecraft obscures the origin of attacks. Countering today's attacks and avoiding future incursions requires understanding the legacy as well as emerging infrastructure used by adversaries for activities for command and control (C2) or launching phishing attacks.

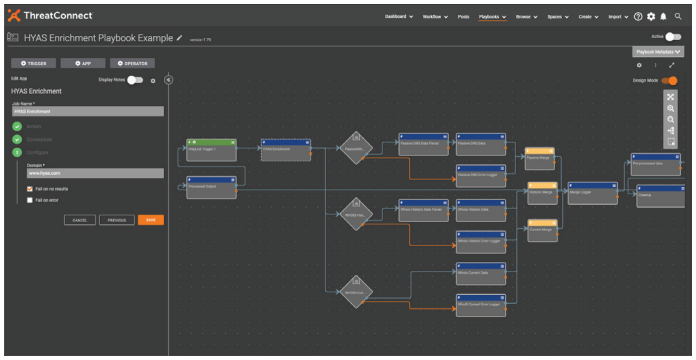
THE SOLUTION

Contextualize, Prioritize and Mitigate Threats

HYAS Insight enrichment for ThreatConnect enables SOC and CSIRT teams to connect specific attack instances and campaigns to billions of historical and current indicators of compromise faster than ever before, bringing invaluable new insights and visibility to your security efforts. The ThreatConnect-HYAS combination enables further automation of proactive cyber threat operations and can inform risk assessments, profile attackers, guide online fraud investigations, and map attacker infrastructure.

KEY FEATURES

- **Proprietary WHOIS database including dynamic DNS domains** - Enables proprietary and detailed insights into campaign infrastructure used by adversaries.
- **Ultra-granular IP geolocation data** - Rather than knowing a country or city where an adversary operates, HYAS Insight achieves accuracy to seven GPS decimal points, to precisely understand the adversary location.
- **Adversary hunting by email, domain, IP, telephone, registrant ID, BSSID, nameserver, and other data points -** HYAS Insight enrichment for ThreatConnect enables analysts to pivot and "spiderweb" to speed investigations.
- **Hundreds of millions of malware hashes and their corresponding network traffic -** Understanding malware network traffic behaviors and detailed malware reporting accelerates investigation closure.



- **Excellent historical domain whois and passive DNS data** - Speeds investigations with thorough understanding of past and present attacker domain infrastructure.
- **Global WiFi SSID mapping including associated network activity** - Zero in on adversaries WiFi infrastructure and cut through obfuscation.

THE HYAS & THREATCONNECT ADVANTAGE

Unique among threat intelligence vendors, HYAS leverages exclusive data sources and non-traditional collection mechanisms to deliver a powerful threat investigation and attribution solution. The combination of HYAS Insight and ThreatConnect improves visibility and productivity for analysts, researchers and investigators while vastly increasing the accuracy of their findings.

HOW TO GET STARTED

If you are already a ThreatConnect customer, this app can be downloaded from the ThreatConnect GitHub. For more information about this app, please contact your ThreatConnect Customer Success representative or email sales@threatconnect.com.

ABOUT THREATCONNECT

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ABOUT HYAS

HYAS enables enterprises to detect and mitigate cyber risks before attacks happen and identify the adversaries behind them. HYAS Insight improves visibility and productivity for analysts, researchers and investigators while vastly increasing the accuracy of their findings. HYAS Insight enables analysts to connect specific attack instances and campaigns to billions of historical and real-time indicators of compromise faster than ever before, bringing invaluable new intelligence and visibility to security efforts. Threat and fraud response teams use HYAS Insight to hunt, find, and identify adversaries, often down to their physical doorsteps.

Learn more about how we can optimize your threat investigations with the HYAS Insight at https://www.hyas.com.