ANOMALI®

HYAS

KNOW YOUR ADVERSARIES

Investigate and understand adversary infrastructure with Anomali and HYAS

ANOMALI AND HYAS JOINT SOLUTION FEATURES

- The combination of HYAS™ Insight and Anomali ThreatStream improves visibility and productivity for analysts, researchers and investigators while vastly increasing the accuracy of their findings
- Anomali ThreatStream users can automate domain blocking for preemptive protection via Anomali platform integrations with existing security infrastructure
- HYAS Insight supports pivoting for link analysis and visualization in Investigations

IMMEDIATE TIME-TO-VALUE

- Proprietary WHOIS database including dynamic DNS domains
- Ultra-granular IP geolocation data
- Adversary hunting by email, domain, IP, telephone, registrant ID, BSSID, nameserver, and other data points
- Hundreds of millions of malware hashes and their corresponding network traffic

CONTEXTUALIZE, PRIORITIZE AND MITIGATE THREATS

HYAS Insight enrichment for Anomali ThreatStream 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 Anomali-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.

CRITICAL INTELLIGENCE

Unique insights into adversary infrastructure

FLEXIBLE DEPLOYMENTS

Fast, scalable implementation on-premises and in the cloud

IMMEDIATE RESULTS

Fast and scalable, speeding analyst investigations by up to 3X

ACCELERATING INVESTIGATIONS

CHALLENGE

Within the SOC and CSIRT, teams must 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.

SOLUTION

The Anomali ThreatStream Platform connects HYAS Insight intelligence with your existing security solutions, making it faster and easier to turn security insights into action. Billions of indicators are queried and easily tied into collaborative investigations to enhance detection and response to serious threats.

CUSTOMER BENEFIT

Analysts can accelerate investigations by up to 3X with HYAS Insight, optimizing the number of events per analyst hour, speeding productivity, and avoiding burnout.

GAINING VISIBILITY INTO ADVERSARY INFRASTRUCTURE

CHALLENGE

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.

SOLUTION

HYAS Insight data enables analysts using Anomali ThreatStream to see beyond adversary OPSEC to identify domain infrastructure used for C2 or phishing attacks.

CUSTOMER BENEFIT

Cyber adversaries are typically repeat offenders. Using Anomali ThreatStream and HYAS Insight, analysts can identify adversary infrastructure and preemptively block it to avoid future attacks.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®