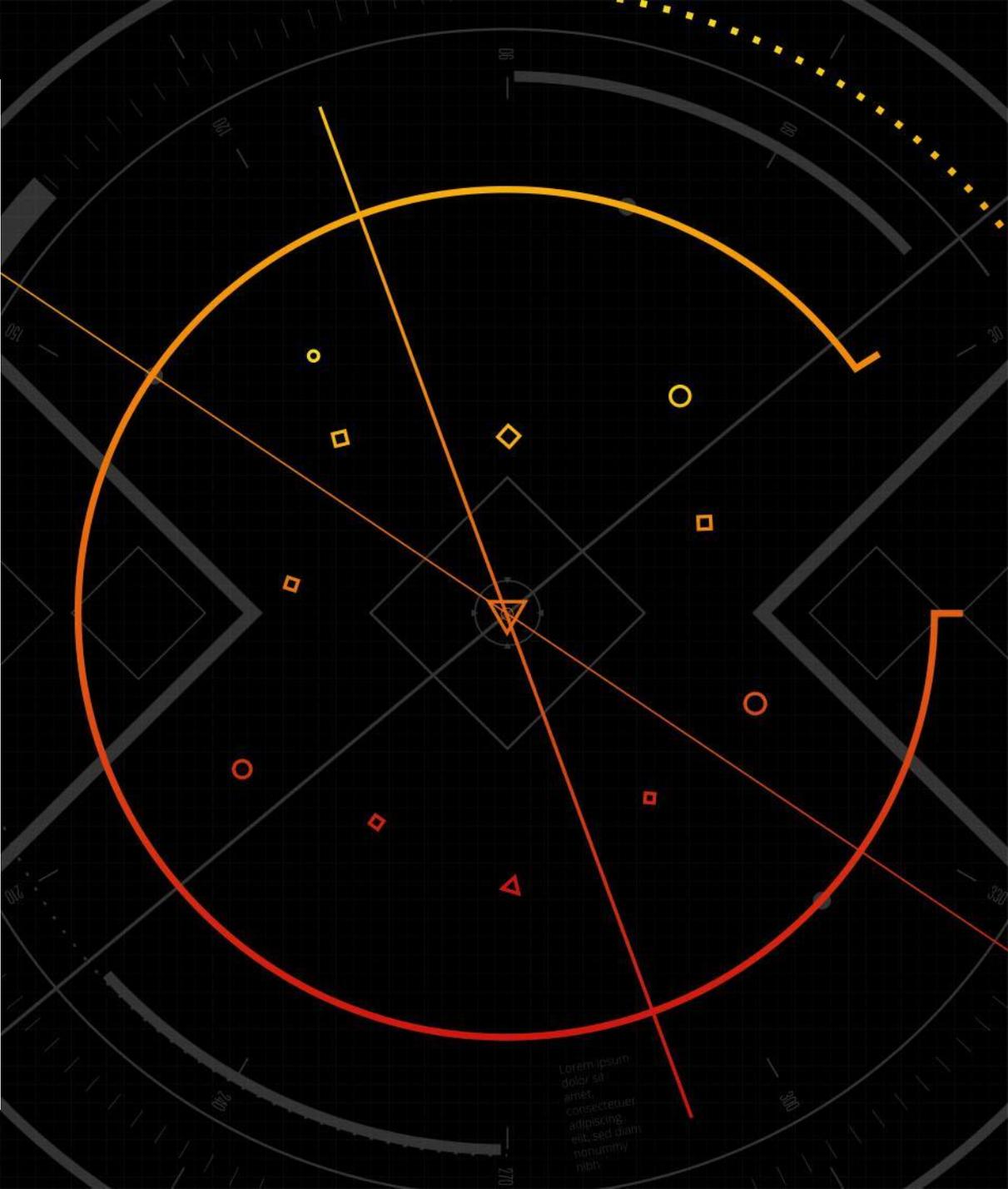# HYAS Insight Overview
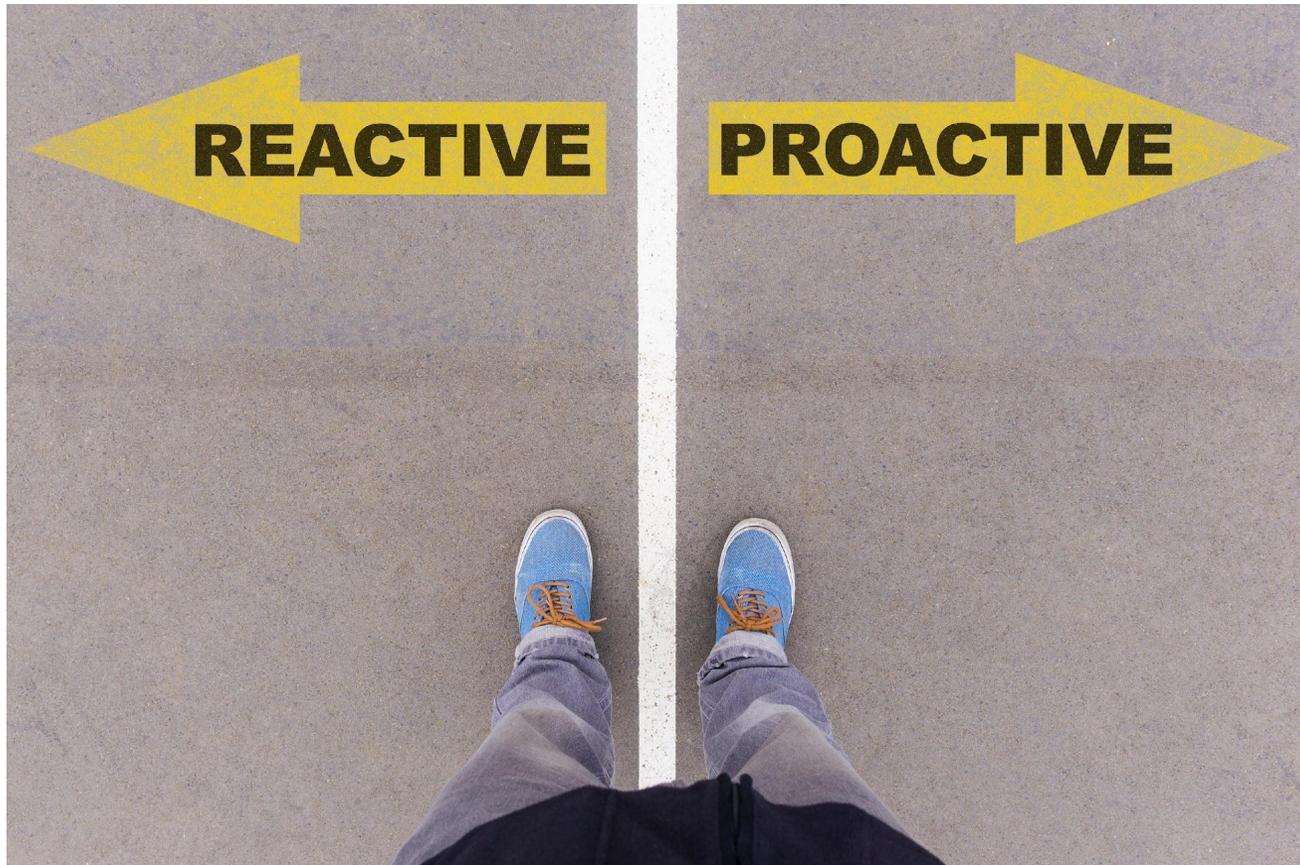
September 1, 2020

www.hyas.com

Existing Security Approaches are Incomplete

Most enterprises have no idea who is trying to attack them -- their security approach is <u>reactive</u>

Only by getting <u>proactive</u> can we make substantial security improvements with real ROI

Problems Being Solved by HYAS Insight

Fraud Investigation

- Cutting through adversary obfuscation and tradecraft
- Accelerating investigations to identify adversaries and reduce fraud losses

Forensics and Incident Response

- Understanding adversary infrastructure to speed investigations, improve analyst productivity
- Identifying attackers to preempt future incursions

Threat Intelligence

- Enriching existing toolsets adversary infrastructure intelligence
- Proactively detecting & disrupting emerging infrastructure before it can be used by adversaries

Threat Hunting

- Gaining visibility midstream by de-obfuscating and correlate adversary infrastructure
- Improving analyst productivity with integration into data visualization and threat intelligence (TIP/SOAR/SIEM) toolsets
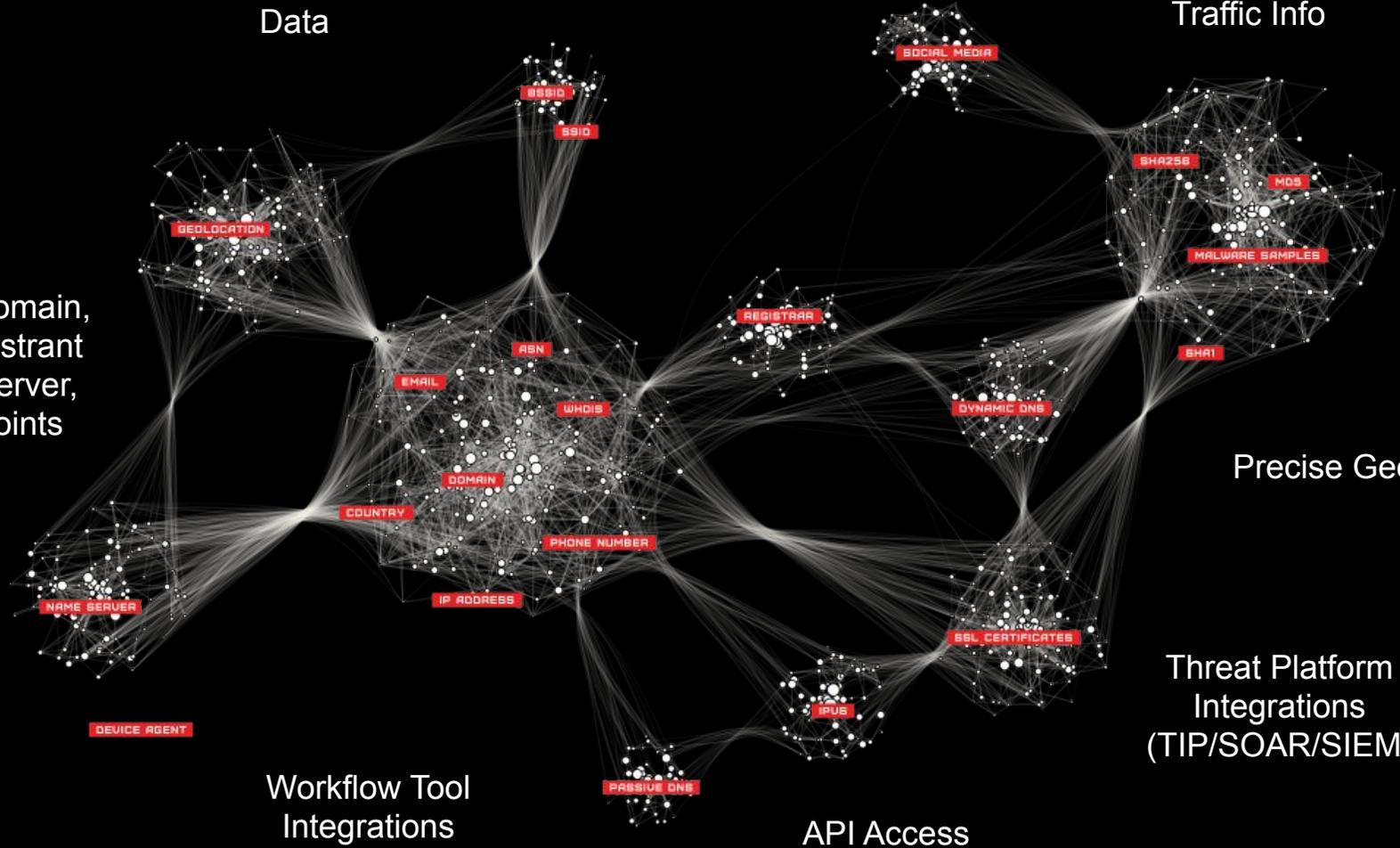
HYAS Insight Overview

HYAS Insight aggregates data from the whole internet, absorbs intelligence to identify attacker infrastructure and threats, and empowers threat investigation and response.

Passive DNS Data

Proprietary & Historical WHOIS Data

Exhaustive Malware Hash Data Including Network Traffic Info

Adversary Email, Domain, IP, Telephone, Registrant ID, BSSID, Nameserver, and Other Data Points

3.3B+
Data Points Processed Every Day

250M+
DNS Queries Analyzed Daily

Geo-IP
with "To the Doorstep" accuracy

Precise Geo-IP

Threat Platform Integrations (TIP/SOAR/SIEM)

Workflow Tool Integrations

API Access

HYAS Insight Differentiators

- Adversary attribution "to the doorstep"
  - Unmatched proprietary and historical WHOIS data provides visibility
  - Precise geolocation to six digits of precision
- Superior understanding of C2 and phishing infrastructure
  - HYAS explodes hundreds of thousands of malware samples per day to understand adversary infrastructure
- Analyst productivity improvement averaging 3x
- Rapid deployment with integrations with existing toolsets and workflows
  - HYAS Insight cloud-native UI
  - Data workflow: Maltego, Polarity, King & Union Avalon
  - TIP/SOAR/SIEM: Anomali, ThreatConnect, and others
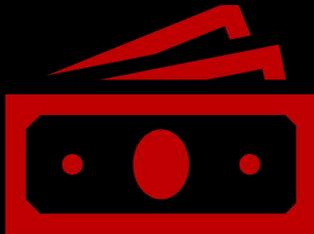 - API for custom integration

HYAS: Solving Business Problems

Improve security

- Do more than just end-point protection
- Block phishing attempts at the egress of your network
- Render malware inert by blocking communication with C2
- Protect roaming devices inside and outside your network

Save Money and Time

- Reduce alert fatigue by reducing what needs to be scanned
- Make faster, more informed business decisions based on domain reputations

Improve Your Business Intelligence and Get Proactive

- Make effective, efficient decisions
- Feed DNS-based data intelligence into all aspects of your security stack
- Let blocked domains help you understand your attackers and get proactive
- Knowing your attackers is critical intelligence you need

About HYAS

- Founded 2015
- Funding: A Round led by M12 (Microsoft Ventures)
- HQ in Victoria BC, Canada
- Customers:
    - 2 of Fortune 5
    - Multiple Fortune 100 enterprises
    - Customers in 4 countries on 3 continents
- Product Portfolio
    - HYAS Insight
    - HYAS Intelligence Services
    - HYAS Protect

THANK YOU

www.hyas.com