



HYAS



# HYAS™ INTELLIGENCE SERVICES

Founded by a team of world-renowned security analysts and entrepreneurs, the HYAS Intelligence Team works with clients to help empower organizations to better understand their adversaries, and how they can pursue or defend against them.

The HYAS Intelligence Team is an important resource for many global 2000 clients, helping them to better understand the nature of the threats their organizations face on a daily basis. From advanced persistent threats facing entire industries to the adversary targeting a specific organization, the team at HYAS acts as an extension of our clients' teams to help provide actionable intelligence and act as a force multiplier for when it really matters.

## HOW WE ENGAGE WITH CLIENTS

At HYAS, we pride ourselves on the collaborative nature of our client engagements. Whether working with teams directly, or with their trusted partners, the HYAS Intelligence Team builds strong working relationships with the clients that trust us to be an extension of their own teams. The strength of these engagements helps to ensure that clients receive the intelligence they need when they need it, and allows HYAS to be proactive in providing advice related to emerging or changing threats.

## LIFECYCLE OF A CLIENT REQUEST

**Initial Client Scoping Discussion and Data Exchange:** The HYAS Intelligence Team sits down to learn more about the event, key client investigative and intelligence priorities, and to discuss available and relevant data. At the end of this discussion, our team will indicate to the client if the case is one that we can provide significant value on. If the client wishes to move forward, arrangements are made for

collecting the appropriate data for the HYAS Intelligence Team to begin the investigation phase of the engagement.

### Investigation Phase:

Our team then goes to work on the investigation, digging deep into the data and circumstances of the investigation to enrich the data and evidence related to the case, and deliver on the intelligence requirements of the client. During this phase the Intelligence Team keeps the client abreast of developments in the investigation, providing updates at agreed upon intervals, or as circumstances warrant.

### Final Client Brief and Investigative Report:

The HYAS Intelligence Team presents their findings to the client team. The brief focuses on empowering the organization to understand:

1. Adversary/Target information related to the event or investigation. (Often identifiable to their legal names, photos, social media accounts, phone numbers, personal email, and locations of interest, etc.);
2. The nature of their tactics, techniques, and procedures (TTPs) used by the adversary;
3. What infrastructure is associated with the actor or group, relevant to the event/investigation, as well as any additional infrastructure;
4. Recommended options for the client, including ongoing monitoring of new actor infrastructure.
5. Recent Investigations

## EXAMPLES OF HOW HYAS HELPS:

- ▶ Network investigations and event attribution
- ▶ Adversary dossier development and monitoring
- ▶ Client liaison with international law enforcement agencies
- ▶ Business Email Compromise investigations
- ▶ APT infrastructure attribution and monitoring
- ▶ Phishing attack attribution and kit analysis
- ▶ Fraud and financial cybercrime investigation
- ▶ Infrastructure provider research and analysis
- ▶ Credential stuffing attack investigations
- ▶ Cybercrime as a service tracking and monitoring
- ▶ Malware analysis and reverse engineering

## RECENT INVESTIGATIONS

### Monitoring APT33 Infrastructure

Risk takes many forms for global corporations, including the geopolitical risks they face from world events. Over the past year, risks from state sponsored or aligned threat actors has increased and changed. At the request of a number of clients in different industry verticals, the HYAS team continues to monitor infrastructure related to APT33, an Iranian threat actor group. By leveraging the team's unique visibility into the infrastructure being staged, HYAS Intelligence Team clients are able to block malicious infrastructure weeks before it is used in campaigns against other global corporations.

### Actor Attribution and Dossier Development

Certain actors and groups that target an organization can take a toll on the company in a host of different ways. Whether it is direct losses from financial cybercrime, the effect that adversary activities have on a company's brand and customers, or the resource drain they cause by constantly defending against them, understanding the individual actor or group is incredibly important to give companies options in how to deal with them. A recent case that the HYAS Intelligence Team assisted with identified an Asian threat actor group that was stealing over \$300,000 USD a day through their activities. Investigating the incident, we identified the actors, their infrastructure, and were able to recover much of the data that they stole. Acting as a resource alongside international law enforcement for the client, indictments – and more importantly – arrests of the actors were affected, permanently removing them as a threat to the organization.

**“WE GO TO THE  
TEAM AT HYAS  
WITH THE HARD  
QUESTIONS.”**

- Fortune 50 Financial Institution



## ABOUT HYAS

HYAS, a First Nations word meaning “great and powerful,” is the world's leading authority on pre-zero-day cybersecurity risk. HYAS provides the industry's first security solution that integrates into existing security frameworks and enables enterprises to detect and mitigate cyber risks before attacks happen and identify the bad actors behind them. Post attack, threat and fraud response teams use HYAS to hunt, find, and identify adversaries, often down to their physical doorsteps. With HYAS, enterprises are able to adopt a more proactive and adaptive security posture and protect against both known and not-yet-launched attacks, identifying the bad actors targeting their organizations and the infrastructure used to launch their attacks.