The Anomali Intelligence Augmentation Service (IAS) is a service that amplifies an organization’s own Cyber Threat Intelligence (CTI) programs, no matter their level of maturity. IAS provides crucial ATI and insight into areas where organizations can lack visibility, experience, or simply the time required to understand complex and emerging threats.

With IAS, organizations can:

- Understand the specific threats, impacts, and adversaries facing their organization and targeted industry
- Leverage recognized security experts to investigate specific security concerns and scenarios
- Maximize the effectiveness of their internal security resources by extending their efforts with focused expertise
- Expand the organization’s field of view/scope/access to intelligence streams/wider understanding of the threat landscape
- Better communicate risks and threats to executives and stakeholders
- Augment your team with leveraging top tier industry experts

**IAS OFFERINGS**

IAS offerings are designed with one goal in mind — providing you with the exact threat intelligence that best augments your unique security efforts and needs.

Powered by Anomali Threat Research (ATR), IAS enables strategic use of outside security experts and research that can provide the precise information necessary to protect your organization. The ATR team is composed of seasoned analysts and researchers each with over 80+ years combined of experience in enterprise incident response, computer forensics, malware analysis, and other defensive operations. Furthermore, the ATR team has access to a large number of intelligence sources that can provide extensive visibility.

IAS works in conjunction with the ThreatStream platform, giving customers the means to submit requests directly. While unique for each organization, IAS offerings include:
1. INVESTIGATION
IAS offers investigations to answer specific customer-defined questions. Investigations provide insight into who, what, when, where and why as soon as possible. Examples include:

- **Domain Intelligence**: When you have a suspicious domain that keeps appearing in your network logs and need to know what it is and how it is interacting with your systems.

- **File Analysis**: A strange file has appeared on your system, you know you can't open it but you want to know what is it and if it is potentially malicious.

- **Compromised Credentials**: Compromised accounts is one of the most common ways attackers access systems, and IAS investigation will tell you if your organization has potentially compromised accounts.

- **Actor Profiles**: Understanding threat actors and how they work is imperative to security, IAS can provide full actor profiling including TTPs, historical overview, and IOCs.

- **OSINT**: Many organizations do not realize the volumes of intelligence they release publicly on themselves, this intel can be turned against them. IAS offers OSINT investigations to help customers understand what intelligence they are broadcasting.

2. ANALYSIS
Analysis projects are more intensive than investigations, they tend to have a broader scope and delve deeper. Analysis is best suited for when an organization needs a full understanding of a subject. Due to their scope, analysis projects are time-consuming and costly and many organizations do not have the resources to commit to one, outsourcing this job to IAS removes these obstacles.

- **Regional Analysis**: Can you provide analysis and insight into threats facing the Asian financial sector?
• **Timelines:** I need to understand how Advanced Persistent Threat (APT) activity across the past two years impacts my organization.

• **Industry Trends and Threats:** What does the current Healthcare industry threat landscape look like? How have evolving standards impacted security efforts?

• **Malware Reversal:** Can you reverse engineer this malware to help us best understand how to defeat it?

<table>
<thead>
<tr>
<th>MD5</th>
<th>Associated Campaign</th>
<th>Compile date</th>
<th>First VT submission</th>
<th>Last VT submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>90372a5e387e42c63b37d88845adbde6a</td>
<td>grp03</td>
<td>[Fri Jul 24 08:25:13 2015 UTC]</td>
<td>2015-11-28 02:17:58 UTC (2 months, 3 weeks ago)</td>
<td>2015-11-29 05:54:55 UTC (2 months, 2 weeks ago)</td>
</tr>
<tr>
<td>f6ac3beef63d9f2e3c0fd6769635c30b</td>
<td>grp10</td>
<td>[Fri Jul 24 08:25:50 2015 UTC]</td>
<td>2015-11-06 13:11:20 UTC (3 months, 1 week ago)</td>
<td>2015-11-20 20:18:18 UTC (2 months, 4 weeks ago)</td>
</tr>
<tr>
<td>591e820591e105000e9396bd50e6776</td>
<td>grp05</td>
<td>[Fri Jul 24 08:25:13 2015 UTC]</td>
<td>2016-01-16 09:20:34 UTC (1 month ago)</td>
<td>2016-01-16 09:20:34 UTC (1 month ago)</td>
</tr>
</tbody>
</table>

**Malware Analysis metadata**

### 3. EXECUTIVE SUMMARIES

High-level overviews designed to brief executives and other stakeholders on specific threats faced by your industry or organization. Examples include:

- **Industry trends and threats:** What threats pose the greatest potential impact for my specific industry?
- **Organizational threats:** What specific threats does my organization face? Are we a target?

### 4. REGULAR REPORTING

Similar to Executive reports, but delivered on a Monthly or Quarterly basis. Focused on threats faced by your specific organization or industry.

### HOW TO ACQUIRE IAS

IAS is available via the ThreatStream platform, Anomali’s comprehensive Threat Detection, Investigation, and Response hub. Once a request has been submitted via ThreatStream, the ATR will respond with an estimated cost and delivery time via a Scope of Work (SOW) that outlines the project scope and expectations.

If more information is needed, the scope and expectations need to be adjusted, or the request requires clarification, the analyst can be contacted directly through ThreatStream or via research@anomali.com.

### CONTACT US

For more information about pricing, availability, or to schedule a consultation, please contact: research@anomali.com

### ABOUT ANOMALI

Anomali arms security teams with highly optimized threat intelligence powered by machine learning. Organizations rely on the Anomali Threat Platform to detect threats, understand their adversaries, and respond effectively.

**Corporate Office:** 808 Winslow Street, Redwood City, CA 94063