THE INVESTMENT ASSOCIATION

ANOMALI®

IA-TITAN

Powered by Anomali

COLLABORATION IN THE FIGHT AGAINST CYBERCRIME IN FINANCIAL SERVICES

According to the Financial Conduct Authority (FCA), the UK's Financial Services sector is seeing an exponential rise in data breaches year on year. The latest signs are that the sector is under sustained and relentless attack from multiple adversaries, using an ever-increasing array of new techniques, tactics and procedures.

The financial and reputational repercussions of these attacks, along with increased action by regulators to hold UK companies to account with significant financial penalties, is putting pressure on the sector to take a more proactive, intelligence-led approach towards cyber security.

The Investment Association (IA) is helping its membership in the fight against cybercrime by forming IA-TITAN, the IA's Threat Intelligence Alert Network, a threat intelligence sharing community created specifically for IA members utilizing Anomali's cyber threat intelligence platform.

IA-TITAN, powered by Anomali, will enable members to centralize a range of data and intelligence from law enforcement, government agencies and other relevant authorities. Intelligence on cyber hazards and risks will be specifically relevant to the asset management industry in the UK.

IA-TITAN PLATFORM

The Anomali ThreatStream platform powering the IA-TITAN community is purpose-built to facilitate the collection and management of threat intelligence from multiple sources and at scale, enabling these processes to be automated and thus mitigating time-intensive manual tasks.

The platform enables the secure and meaningful sharing of relevant threat intelligence, from Indicators of Compromise to more strategic intelligence about threat actors, campaigns, TTPs (tactics, techniques and procedures), and vulnerabilities. This allows community members to take a proactive approach by gaining insight into their adversaries.

Participating members can gain additional benefits by upgrading to Anomali's enterprise-grade solutions to further 'operationalize' the threat intelligence, uniting all the tools in their security infrastructure, speeding the detection of threats and enabling proactive defense measures.

ThreatStream Features At-A-Glance	ThreatStream Access with IA-TITAN Membership	ThreatStream Enterprise Access
Threat Intel Collection		
Trusted Circles threat intelligence sharing	•	•
Anomali open source threat intelligence feeds	•	•
Anomali premium threat intelligence feeds		•
Intelligence marktplace access — Anomali APP Store		•
Free feeds from Anomali APP Store		•
Threat Intelligence Feeds SDK		•
Threat Intelligence Enrichment SDK		•
TAXII Server/Client		•
Threat Intel Management		
User accounts — Unlimited		•
Dashboard for searching, viewing, alerting	•	•
Feeds normalization, de-deduplication, false-positive removal	•	•
Threat models — MITRE ATT&CK, Diamond, Kill Chain	•	•
Investigations workbench	•	•
View full Threat Bulletins and intelligence details pages	•	•
Anomali Enrichments — GeoIP/Open Ports/WhoIs History		•
Freemium Sandbox		•
Anomali Lens Freemium		•
Threat Intel Integration		
Integrations Tier0 (API)		•
Integrations Tier1 (SIEM)		•
Integrations Tier2 (EndPoint, Firewall, SOAR, etc.)		•
Integrations SDK		•
Platform and Support		
Technical Support — Standard 24x5 support		•
Dedicated Customer Success Manager		•
Anomali University	•	•
Deployment platform — SaaS	•	•
Deployment platform — On-Prem or Airgap		•

ADDITIONAL ANOMALI SOLUTIONS FOR UPGRADE

ANOMALI MATCH

Anomali Match is purpose-built to automate and speed time to detection in your environment. Anomali Match correlates years of metadata against active threat intelligence to expose previously unknown threats to your organization.

- Threat Intel and Log Matching Scalability
  - Analyze millions of Indicators of Compromise (IOCs) against billions of events every day
  - Multi-year event history matching/lookback
- Threat Intel Integration
  - Native integration with ThreatStream
  - Turnkey integration with leading SIEMs (Splunk, QRadar, Arcsight)
  - Universal Link for log source ingestion (EDR, FW, IPS, Scanner, etc.)
- Anomali Lens Freemium
- Domain Generation Algorithm (DGA) Detection
- Deployment
  - Server installer for on-prem hardware deployments
  - Available for cloud deployments

LENS+

Lens+ enables threat and security analysts to make faster and more accurate decisions. Len provides instant access to strategic and tactical intelligence from any mobile or browser page. Analysts at all levels are empowered with real-time scores and context that accelerate decision making. Executives can easily access threat intel on their devices to stay informed about the latest threats to their business.

Lens+ supports the MITRE ATT&CK framework, allowing analysts to take a model-based approach to threat analysis by identifying the tactics, techniques, and procedures (TTPs) identified in scanned pages.

- Natural Language Processing (NLP) for any web-based content
- Threat Actor Identification
- Malware Family Identification
- CVE Identification
- Malicious IP Address and URL Identification
- Auto-scan
- MITRE ATT&CK TTP Recognition
- MITRE ATT&CK Model Investigation
- Anomali Match Freemium

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

ANOMALI®