ANOMALI

ANOMALI INTELLIGENCE CHANNELS

OUT OF THE BOX INTELLIGENCE FOR SECURITY TEAMS

Security teams are under pressure to do more with less. Unfortunately, most organizations struggle with effectively implementing threat intelligence, not benefiting from the value their threat intelligence team, processes, and tools provide.

Anomali can help. We've made it easier for security teams to experience the power of threat intelligence to detect and respond to advanced threats with Anomali Intelligence Channels.

Intelligence Channels provides tailored intelligence curated by The Anomali Threat Research team, with integrated dashboards and insights that provide an immediate overview of relevant threats in each area.

This continuous, focused intelligence enables security teams to respond faster and more confidently to targeted threats in their environment.

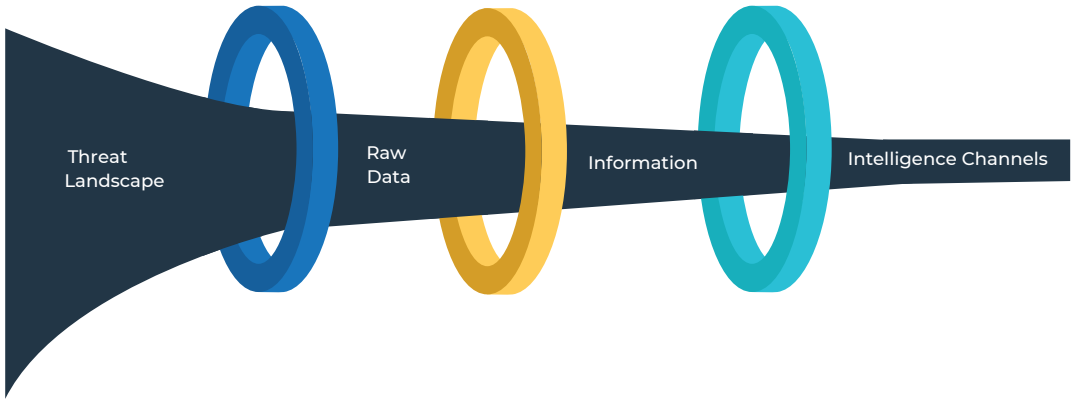
Intelligence Channels streamline the collection and use of relevant intelligence by analyzing adversary information and operationalizing threat data to continuously monitor for threats, prioritize defenses, and respond accordingly.

KEY BENEFITS

- Ready to go intelligence for Security Teams
- Customized feeds that surface relevant threats
- Focused intelligence to fill in the gaps
- Streamline processes to align resources
- Quickly understand targeted threats and their impact

Intelligence Channels include focused intelligence for:

- Threat Actor Monitoring and TTPs
- Brand and Domain Monitoring
- Phishing and Fraudulent Activity
- Infrastructure
- Malware Intelligence
- Region or Sector Specific Threats
- Social Media
- Mobile Threat Defense
- Vulnerabilities and Exploits



Anomali Intelligence Channels

THREAT ACTOR MONITORING AND TTPS
Adversaries that pose the greatest threat to public or private enterprises, based on sophistication and volume of activity.

BRAND AND DOMAIN MONITORING
Targeted threats, including website spoofing, targeted phishing, and email scams.

PHISHING AND FRAUDULENT ACTIVITY
Financial fraud, bogus applications, identity theft or misuse, and phishing scams.

INFRASTRUCTURE
Threats or malicious activity against cyber infrastructure, including hardware, software, supply chain components, and public and private cloud architectures.

MALWARE INTELLIGENCE
Known or suspected threats from malicious software.

REGION OR SECTOR SPECIFIC THREATS
Threats assessed to have a significant impact on a global scale, including political, social, criminal, governmental, economic, or environmental events. Examples include conflict/war, cyber attacks, economic sanctions, significant changes in financial markets, and natural disasters.

SOCIAL MEDIA
Social media threats against brand impersonation risks, social engineering, etc. as well as OSINT indicators shared on social media

MOBILE THREAT DEFENSE
Threats targeting mobile devices, including device, network, application.

VULNERABILITIES AND EXPLOITS
Threats targeting configurations and known vulnerabilities.

KEY USE CASES

INCREASE VISIBILITY
View complete collection coverage for specific areas of focus.

FOCUS INVESTIGATIONS
Attribute relevant intelligence for specific investigations aligned to strategic areas.

STRENGTHEN INTEL
Fill in gaps with existing intel programs.

BUILD A FOUNDATION
Quickly inject specific categories of intelligence into threat operations.

info@anomali.com | www.anomali.com

808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI