ANOMALI
THREATSTREAM

INTELLIGENCE INITIATIVES

Align Organizational Intelligence Goals with Intelligence Initiatives

Organizations are under pressure to improve efficiency, reduce cost, improve time-to-market, and beat the competition. Unfortunately, most organizations continue to work in silos, making it harder to reach those goals. As technology and intelligence gets introduced to add detection and response capabilities, priorities may not align.

Intelligence Initiatives provide a foundational guide for organizations to integrate the CTI (Cyber Threat Intelligence) lifecycle as part of their working process to reach organizational goals.

Intelligence Initiatives enable organizations to better understand and value their team's effort while working towards organizational goals.

Once established, an organizational goal can be mapped to an initiative in ThreatStream. Users can then associate the most appropriate collections or feeds to this initiative tailoring the entities to be reviewed to the time period of the initiative.

Investigations can be attributed to one or more initiatives, as well as relevant Threat Models. When completed a summary report of the initiative is available for the wider organization to review and evaluate that initiative, answering some of these questions:

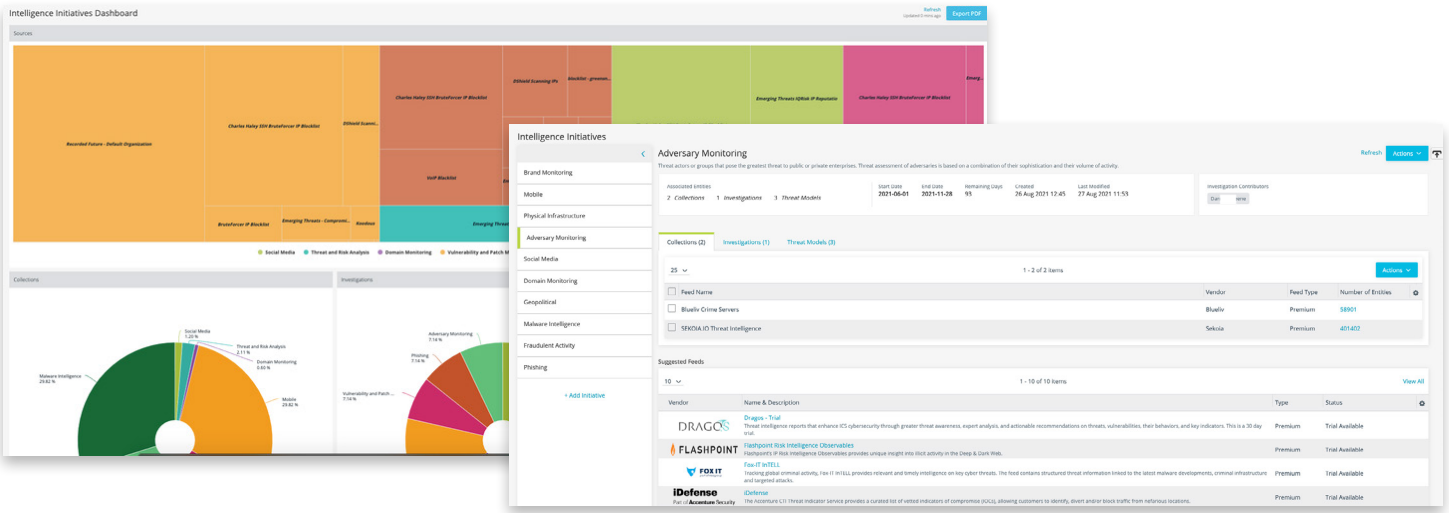
- Is the organization using the right collections and feeds?
- Which investigation work was required to secure the organization as part of this initiative?
- Which team members worked across different initiative investigations? How did our understanding of related threat models evolve?

KEY BENEFITS

- Measure ThreatStream activity and align with organizational goals
- Identify specific feeds to particular initiatives
- Review user contributions of participants for each initiative
- Generate executive-facing reports at end of each initiative to provide key metrics

All available feeds in ThreatStream have been categorized to an Initiative for customers to easily associate a collection of threat intelligence to an organizational goal.

Out-of-the-box dashboards provide quick access to key metrics relating to an Initiative, giving management an immediate overview of ongoing Intelligence Initiatives being worked on by their ThreatStream teams.



OUT OF THE BOX INTELLIGENCE INITIATIVES

Adversary Monitoring
Threat actors or groups that pose the greatest threat to public or private enterprises. Threat assessment of adversaries is based on a combination of their sophistication and their volume of activity.

Brand Monitoring
Threats to a corporate brand based on observations in open and closed sources. Includes compromises of corporate intellectual property, domains, or credentials; threats to corporate personnel, facilities, or operations; attacks on corporate brands or reputations; and rogue applications.

Malware Intelligence
Known or suspected threats from malicious software.

Domain Monitoring
Misuse or compromise of corporate domains. Includes domain names crafted to deceive consumers through variations of legitimate domains or typosquatting, domains that host counterfeit websites that impersonate a legitimate entity, and domains created to support phishing campaigns.

Fraudulent Activity
Activities include financial fraud (credit cards, business email compromise, rewards fraud, etc.), bogus applications, identity theft or misuse, and unauthorized access to information systems of facilities.

Vulnerability and Patch Management
Known vulnerabilities prioritized by risk. Based on intelligence assessments of potential threats against the current configuration.

Phishing
Attempts to fraudulently acquire access or information by means of impersonation through email or messaging. Includes tactics, techniques, procedures, and impacts of such campaigns. Includes attribution when possible.

Mobile
Threats to mobile communications hardware (Apple, Samsung, etc.), operating systems (iOS, Android, etc.), and applications.

Threat and Risk Analysis
Threats to an organization mapped against known defensive tools. Threat assessment is based on the known or suspected intent and capabilities of specific threat actors, groups, or TTPs. Risk assessment is based on potential damage.

Physical Infrastructure
Threats or malicious activity against cyberinfrastructure, including hardware, software, supply chain components, and both public and private cloud architectures.

Social Media
Threats made on social media to corporate brands, personnel, facilities, or reputation. Threats may include malicious comments or explicit threats.

Geopolitical
Threats assessed to be most likely 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.

KEY USE CASES

STREAMLINE INTELLIGENCE
Align Threat Intelligence data and capabilities across entire organization.

SECURE COLLABORATION
Securely collaborate with internal colleagues to speed threat identification and activities.

HOLISTIC VIEWS
View complete collection coverage for specific organizational intelligence initiatives.

RELEVANT INTELLIGENCE
Attribute relevant intelligence for each initiative to help make better decisions.

MEASURE RESULTS
View team progress and analyst contributions toward an organizational intelligence initiative for evaluation.

ABOUT ANOMALI

Anomali provides threat detection and response solutions that enable cyber resilience and elevate a cyber-fused response using integrated threat intelligence. Anomali extends and amplifies threat visibility by curating structured and unstructured global intelligence and security incident data to inform decisive response.

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

ANOMALI