ANOMALI

GUIDE

Five Challenges to Operationalizing Threat Intelligence and How to Overcome Them

Five Challenges to Operationalizing Threat Intelligence and How to Overcome Them

An ever-changing landscape of threat actors, malware, tools, and motivations requires technology that is equally, if not more, adaptable than adversaries. While defenders are distracted by patching the walls, bad actors are busy probing for the next weakness and plotting their next attacks.

One of the most powerful tools in our cyber arsenal is effective threat intelligence. It can illuminate potential threats, help us understand relevant attack methods, and inform our preventative actions. However, operationalizing threat intelligence — distilling actionable insights from the deluge of both raw and contextualized data — is a nuanced and sophisticated science.

This guide explores five key challenges in operationalizing threat intelligence and offers potent strategies for addressing them.

One of the most powerful tools in our cyber arsenal is effective threat intelligence. It can illuminate potential threats, help us understand relevant attack methods, and inform our preventative actions.

What is a Threat Intelligence Platform?

A threat intelligence platform (TIP) aggregates, correlates, and analyzes threat data from multiple intelligence providers to provide actionable security insights. TIPs act as a central repository for numerous intelligence types from a variety of open source intelligence (OSINT) and premium sources. However, intuitive TIPs will empower analysts to quickly conduct data and trend analyses so they can hit the ground running. They perform pre-processing, such as deduplication and enrichment, to provide a consolidated and contextualized view of the threat landscape. This helps security analysts make informed decisions and respond more effectively to potential threats.

Do You Need a Threat Intelligence Platform?

Today's growing volume of threat intelligence data often requires manual processing, which is precluded due to limited tool capabilities, budgetary planning, and skills of cyber employees. Organizations often subscribe to multiple intelligence feeds. Unfortunately, this often results in duplication. To address this issue and make the data actionable, a TIP curates, removes duplicates, processes, and prioritizes it. Organizations can streamline their threat detection and response efforts and further elevate their security posture by integrating this TIP-curated data into a security information and event management (SIEM) system and mapping threats to internal telemetry.

The goal of all of these activities boils down to answering one simple question: "Is there a threat, and if so, how worried should I be?"

Challenge 1: Transforming Raw Data into Actionable Intelligence

Threat intelligence often includes observables and indicators of compromise (IoCs) — such as IP addresses, domain names, file hashes, and URLs — that may be reported multiple times across different sources. This redundancy can tilt the signal-to-noise ratio, leading to inefficiency and confusion. Security teams must sift through multiple (often dense) versions of the same data, frequently presented with differing levels of severity or confidence.

A robust TIP, like Anomali ThreatStream, addresses this challenge by consolidating threat data from multiple sources into a single format. It analyzes the collected data to remove duplicates and inconsistencies, providing a unified view of single observables reported by the same source. It organizes threat intel reports into appropriate threat models (actor, malware, campaign, among others). This empowers the digestion of complex topics by organizing observables by iTypes (indicator types) and intelligence reports by threat models and associations (to link relevant data together).

Perhaps most importantly, Anomali ThreatStream helps with attribution. This early identification of potential actors through recognition of their attack patterns and motivations enables the security team to see beyond the IoC level of a threat. This provides a significant advantage in the effort to disrupt a likely attack and minimize its potential impact.

Challenge 2: Ensuring Contextual Relevance

Another critical challenge is ensuring the contextual relevance of threat intelligence. Not all threats are relevant to every organization, and raw threat data can be misleading or irrelevant without context. Contextualizing threat intelligence involves understanding the specific risk a threat poses to an organization based on its industry, geography, security stack, and existing vulnerabilities.

Threat scoring and confidence levels are essential components of contextual relevance. Threat scoring assigns a numerical value to the risk posed by a threat, helping prioritize response efforts. Confidence levels indicate the reliability of the threat intelligence based on the source's historical accuracy and credibility. By integrating these factors, ThreatStream can provide security teams with a prioritized list of threats most relevant to their specific environments. This enables organizations to focus their resources on the most significant threats and optimize their responses.

Challenge 3: Access to Real-time Information

The dynamic nature of cyber threats requires real-time access to the latest threat intelligence. However, many traditional threat feeds don't provide this information in an easily digestible format, hindering a rapid response to evolving threats. An example is the Cybersecurity and Infrastructure Security Agency (CISA) bulletins, which provide timely updates on new vulnerabilities and threats. While they contain a tremendous amount of useful information, CISA reports are long, dense, and very technical.

ThreatStream's real-time data ingestion bridges the gap with quick and usable summaries that are easily integrated with security workflows. This ensures up-to-the-minute situational awareness, helping reduce the window of exposure and enhancing defensive capabilities.

Improve your security posture with threat intelligence feeds. Specialized feeds ensure comprehensive intelligence coverage across various industries, verticals, and niche areas, including fraudulent activity, geopolitical threats, adversary monitoring, brand monitoring, phishing, social media threats, and more.

All Anomali ThreatStream customers automatically receive curated Anomali Threat Research (ATR) and open-source (OSINT) feeds. Premium specialized feeds curated from Anomali's partners provide in-depth coverage for specific industries, niche topics, and Information Sharing and Analysis Centers (ISACs).

Challenge 4: Disseminating Threat Intelligence

Effective dissemination of threat intelligence is crucial for timely and appropriate responses. Different types of threat intelligence require different dissemination methods. For example, while a human analyst might need to review a detailed threat report or bulletin, machine-readable threat data, such as IP addresses associated with malicious activity, should be fed directly into automated systems (such as firewalls) for immediate blocking.

Integrators within ThreatStream facilitate the distribution of relevant threat intelligence across various security controls and platforms. By automating the dissemination of threat data to appropriate tools — such as Anomali Security Analytics (a next-generation SIEM) for monitoring, firewalls for blocking, or endpoint security solutions for alerting — ThreatStream ensures that the right intelligence reaches the right place at the right time. This streamlined approach minimizes manual intervention, accelerates response times, and reduces the likelihood of error.

Challenge 5: Collaboration and Sharing

Cyber threats are evolving in complexity, often striking multiple organizations across sectors. Enhanced defensive capabilities stem from collaboration and intelligence sharing among trusted entities. For example, when one financial institution sounds the alarm after an attack, the entire community benefits.

Despite the advantages of information sharing, establishing secure and effective collaboration channels remains a challenge. Anomali powers the threat intelligence sharing of many of the world's leading Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and other threat intel sharing communities.

ThreatStream's Trusted Circles feature facilitates secure and efficient threat intelligence sharing among predefined groups, such as industry-specific consortia, government bodies, and partner organizations. These circles enable participants to immediately share relevant threat data while maintaining control over what is shared and with whom. This collaborative approach improves individual organizations' security while contributing to the broader cybersecurity ecosystem.

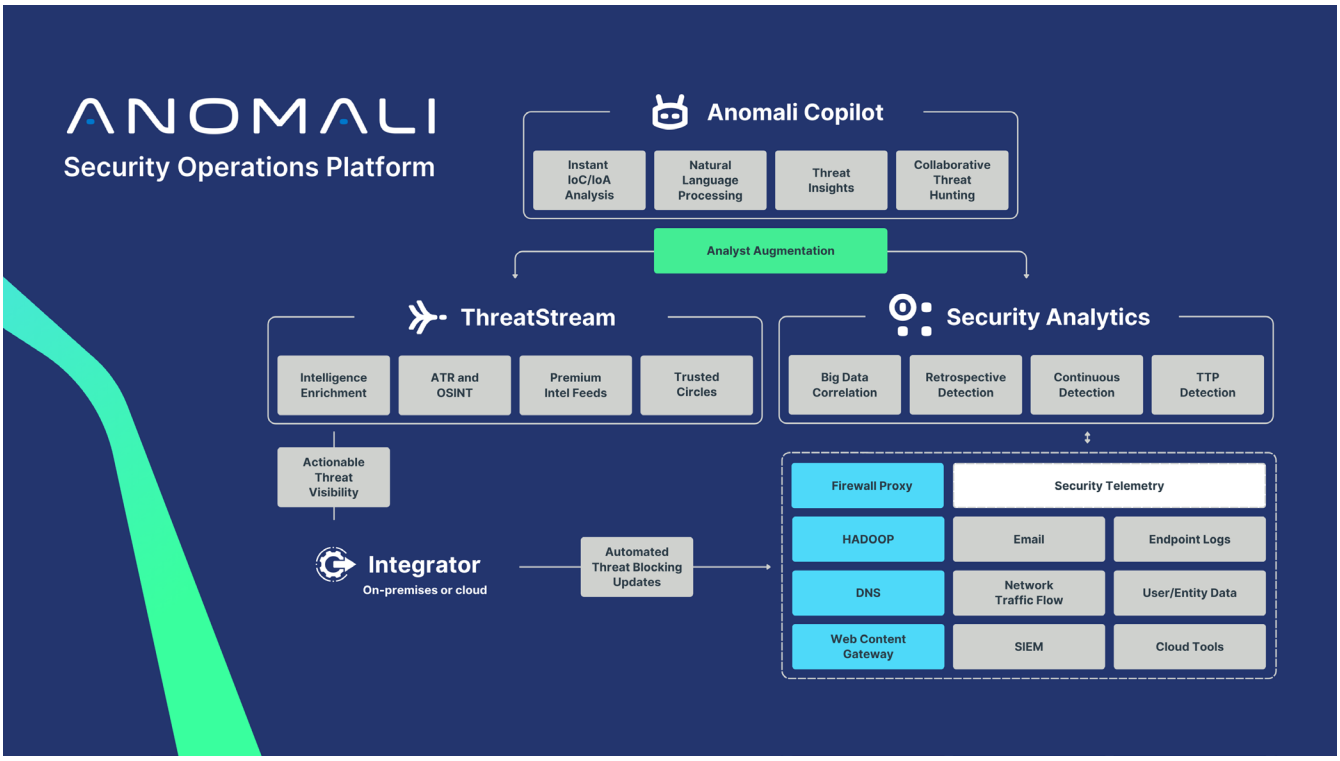
Building for the Future: Advanced Capabilities and Innovations

As cybercriminals refine their tactics, organizations must continuously adapt their defenses to stay ahead of emerging risks. One area of innovation is the integration of advanced correlation capabilities, which can enhance the accuracy and relevance of threat intelligence. Generative AI (GenAI) solutions that leverage machine learning and behavioral analytics, such as Anomali Copilot, can enable organizations to more effectively correlate threat data with their internal telemetry, identifying and remediating the most dangerous threats.

Copilot's advanced correlation capabilities can analyze petabytes of historical data in seconds and identify patterns that suggest potential threats, even if they have not yet manifested in known attack signatures. This proactive approach allows organizations to anticipate and prepare for emerging threats. As ThreatStream/ Copilot continues to develop these capabilities, they will become even more effective and critical tools in the fight against cyber threats.

Using the entire integrated Anomali Security and IT Operations Platform is the best way to get an even more comprehensive understanding of your organization's security posture.

- **ThreatStream** ingests and contextualizes various threat intelligence types into iTypes and threat models, automating intelligence dissemination to numerous tools via Integrator.
- **Copilot** offers machine learning and natural language processing to query and understand the threat intelligence from ThreatStream (or any other integrated source, such as a web browser or Microsoft Office products).
- **Security Analytics** is a next-generation SIEM that empowers fusion intelligence via ThreatStream intelligence and log analysis. It allows analysts to manage their IT infrastructure with relevant threat intelligence, helping them take proactive measures against threats.



Key Takeaways

While essential, operationalizing threat intelligence comes with significant challenges. To truly reap the benefits, organizations must first surmount the hurdles of transforming massive amounts of raw and contextualized data into actionable intelligence, ensuring real-time access, achieving contextual relevance, providing effective dissemination, and fostering collaboration.

At Anomali, we recognize that the work of the threat intelligence team is not done until the SecOps team can truly operationalize the intelligence. In other words, intelligence must go from “actionable” to “actioned.” Anomali makes that possible.

Anomali ThreatStream is a robust TIP with more than 200+ integrations, including OSINT feeds, commercial and premium feeds, and proprietary data. By providing curated access to the world’s largest intelligence repository, Anomali ThreatStream enables organizations to streamline their threat investigation processes, enhance their cybersecurity posture, and stay a step ahead of emerging threats.

Ready to discover how ThreatStream and Copilot can help your organization manage current threats and build a resilient and adaptable security strategy for the future? Schedule a demo and learn how to operationalize your threat intelligence operations with Anomali.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security and IT Operations Platform.

ANOMALI