ANOMALI

GUIDE

Anomali ThreatStream vs. ThreatConnect Threat Intelligence Platform

Anomali ThreatStream vs ThreatConnect Threat Intelligence Platform

5 Ways to Compare and Evaluate

As cyber threats grow in volume and sophistication, organizations need far more than just a repository of threat intelligence feeds — they need a true threat intelligence platform (TIP). TIPs operationalize threat intelligence by enriching it, adding context, ranking it by severity and confidence, and prioritizing analyst work queues. They are dynamic, intelligent solutions that integrate with the larger security ecosystem and workflows.

Both the Threat Connect Threat Intelligence Platform and Anomali ThreatStream operate in this space, each with different approaches and levels of support for intelligent automation and information sharing. Read on to discover how these platforms measure up in the five areas that matter most to your security strategy.

1. Superior Intelligence, Enhanced with Context

The ThreatConnect Threat Intelligence Platform offers automated open source intel (OSINT) collection from 60+ sources with generative AI (GenAI) and natural language processing (NLP) analysis. The platform provides data-transformation capabilities through separately licensed modules to aggregate, standardize, and enrich threat data, ensuring all data is cleaned, deduplicated, and organized for analysis. Additionally, ThreatConnect uses machine learning (ML) and NLP to prioritize and contextualize threats, enabling analysts to focus on the most critical risks.

In contrast, Anomali ThreatStream delivers a comprehensive solution with curated access to 200+ diverse threat intelligence sources. Handpicked by Anomali's dedicated Advanced Threat Research (ATR) team, they include proprietary feeds sourced by Anomali Threat Labs, OSINT feeds, specialized premium feeds (expandable through the Anomali App Store), and feeds from information sharing and analysis centers (ISACs).

While the quantity, quality, and diversity of threat intelligence data sources is important, the ability to transform that data into actionable intelligence is also critical. ThreatStream leverages Macula, Anomali's proprietary ML engine, to enrich threat data, adding context that informs decision-making. ThreatStream does this by:

- Filtering, deduping, and scoring data based on relevance, credibility, and potential impact
- Analyzing, predicting, and classifying cyber threats
- Automating threat scoring

As a result, ThreatStream delivers an enhanced layer of automated cyber defense benefits including:

- Reducing false positives to remove dangerous and time-consuming distractions
- Eliminating "alert fatigue" that can needlessly overtax your cyber defenses
- Making the most efficient use of your limited security analyst resources

Macula operates continuously in the background, processing and analyzing potential threats to classify risks in real time. ThreatStream's intelligent, intentional defense comes from combining this deep contextual analysis curated access to the world's largest threat intelligence repository, based on over a decade of threat research.

The upshot: Anomali ThreatStream provides truly actionable intelligence that significantly reduces time spent on distractions, such as false positives and low-priority alerts.

2. Advanced AI for Adaptive Threat Analysis

Agility is essential in today's rapidly shifting cybersecurity landscape. To adapt to evolving threats, security teams need solutions that provide immediate, sophisticated analysis — a level of responsiveness that only advanced ML and AI can provide.

ThreatConnect's proprietary Collective Analytics Layer (CAL) enhances automation and intelligence gathering through ML and AI for confidence scoring, indicator enrichment, and risk anticipation. However, CAL is offered only as a paid add-on to ThreatConnect's core features.

In contrast, ThreatStream users benefit from Macula's AI/ML integrated scoring and prioritization at no additional cost. This built-in capability enables teams to assess threats more quickly and effectively, without the need for additional integrations.

ThreatStream users can further enhance their security operations with Anomali's GenAI Copilot, which delivers deeper insights, analysis, and automation. Copilot's advanced AI-driven analysis streamlines intelligence prioritization and simplifies stakeholder reporting.

The bottom line: Macula and Copilot provide built-in threat scoring, prioritization, and reporting with AI and ML, although ThreatConnect users must add CAL to obtain similar insights.

3. Streamlined Automation and Integration

TIP workflow automation is critical because it transforms overwhelming volumes of threat data into actionable intelligence while eliminating time-consuming manual processes. By automating routine tasks, analysts can stay focused on what they do best — strategic analysis.

ThreatConnect offers security orchestration and response (SOAR) capabilities through automated playbooks. However, playbooks are designed for specific security scenarios. As these scenarios evolve, playbooks must continuously be revised to match the new conditions. This can delay implementation and reduce overall defensive posture and operational efficiency.

Additionally, high customization requirements often demand dedicated technical expertise — and incur its associated costs.

ThreatStream delivers robust automation and orchestration capabilities, which create workflows based on curated threat intelligence across your entire security infrastructure. Anomali delivers immediate value through:

- Built-in integration capabilities that ensure broad compatibility with existing security controls — including firewalls, SIEMs, proxies, DNS, messaging systems, and endpoint protection platforms — reducing incident response times by up to 30%
- Automated filtering, prioritization, and distribution of threat intelligence by relevance and criticality, enabling analysts to work more efficiently
- Flexible deployment options supporting on-premises, air-gapped, or cloud environments

The takeaway: ThreatConnect's integrated SOAR capabilities are slick, but are "fighting the last war" and may increase analysts' workload and costs while also reducing cyber defense effectiveness. ThreatStream enriches security events with relevant threat data, providing context and the automation that helps analysts quickly understand and respond to potential threats in real time.

4. Secure Intelligence Sharing and Collaboration

ThreatConnect offers community-driven intelligence sharing through public communities and manual cross-instance sharing. This open approach relies heavily on user-contributed intelligence and may introduce risks around data quality and verification, leaving organizations vulnerable to potential misinformation or malicious contributions.

Anomali ThreatStream takes a more sophisticated and secure approach to collaborative intelligence with controlled information flow. ThreatStream allows organizations like ISACs to control intelligence distribution in a more granular fashion. Whether establishing two-way sharing among industry peers or implementing one-way flows from parent organizations to downstream partners, every sharing relationship is explicitly defined and secured.

- **Automated ML-driven enrichment**. Rather than depending solely on community contributions, ThreatStream uses ML to automatically build, enrich, and validate threat intelligence. This automated approach includes advanced scoring and prioritization mechanisms that reduce the risk of errors or malicious activity.
- **"Trusted Circles"** framework. Instead of open communities, ThreatStream enables organizations to create defined, secure networks for intelligence sharing. These Trusted Circles can be configured to support:
  - » Industry-specific collaboration among vetted peers
  - » Geographic or vertical-specific intelligence sharing
  - » Parent organization distribution to downstream partners
  - » ISAC integration for critical infrastructure protection

The bottom line: ThreatStream prioritizes quality and security through ML-validated data and carefully controlled sharing networks.

5. Advanced Threat Modeling and Analysis

Threat modeling is a structured approach to identifying, evaluating, and addressing security risks. It helps organizations understand how attackers might compromise their systems, allowing them to prioritize security measures and allocate resources effectively.

While ThreatConnect offers traditional threat modeling through its Diamond Model of Intrusion Analysis and basic threat assessment tools, modern security teams need more sophisticated, dynamic approaches that integrate real-time intelligence and automated analysis.

Anomali ThreatStream delivers comprehensive threat modeling capabilities that combine advanced automation and rich contextual analysis:

- **Dynamic intelligence integration:** ThreatStream aggregates and continuously updates threat intelligence from multiple sources, including OSINT, commercial, and premium feeds. This real-time integration ensures threat models stay current with emerging attack trends and evolving adversary tactics.
- **Sophisticated threat analysis:** ThreatStream provides detailed insights across the entire threat landscape, delivering comprehensive and enriched analysis of actors, attack patterns, campaigns, infrastructure, malware signatures, tools, and vulnerabilities. This broad coverage enables more effective threat modeling and response.
- **Comprehensive model integration:** ThreatStream's threat models seamlessly integrate with the broader Anomali Security and IT Operations Platform or other existing security stacks, enabling automatic updates and ensuring threat models remain current with the latest intelligence.

The result: ThreatStream customers benefit from dynamic, data-driven threat models that evolve with the threat landscape and deliver actionable insights for strengthening security infrastructure.

Feature	Anomali	ThreatConnect
Speed	Anomali's use of GenAI offers real-time visibility into potential vulnerabilities, behavioral anomalies, and active attacks with response times of seconds.	ThreatConnect offers near real-time visibility into threats, with response times measured in minutes.
Visibility	Anomali offers the industry's largest curated repository of threat intelligence data, providing superior global threat visibility.	ThreatConnect's repository is based on OSINT, uncurated open market and commercial feeds.
Summarization	Use of integrated AI-Powered Copilot can generate multi-level summaries of threat data in seconds across the industry's broadest range of threat intelligence sources.	ThreatConnect relies on summarization through its Collective Analytics Layer (CAL), which is limited to 60 OSINT feeds and requires additional spend.
Scalability	Highly scalable, querying petabytes of data and returning results in seconds.	Lower scalability, query response measured in minutes.

The Clear Choice for Modern Security Operations

Anomali ThreatStream delivers a complete, scalable threat intelligence solution that enhances outcomes across the board. With premium intelligence feeds, superior AI capabilities, automation, secure collaboration features, and sophisticated threat modeling, it empowers organizations to stay ahead of evolving threats.

ThreatStream seamlessly integrates with Anomali's industry-leading AI-Powered Security and IT Operations Platform, which unifies ETL, SIEM, next-gen SIEM, XDR, UEBA, SOAR, and TIP capabilities into a single AI-driven solution. This comprehensive integration delivers best-in-class security at a fraction of the cost of competing solutions.

See how Anomali can transform your security operations. Request a demo today to experience the Anomali difference firsthand.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI