ANOMALI

BRIEF

Q4 25 What's New in Anomali ThreatStream

Actionable Threat Intelligence, Powered by AI and Real-Time Relevant Telemetry

Q4 25 What's New in Anomali ThreatStream

Actionable Threat Intelligence, Powered by AI and Real-Time Relevant Telemetry

Anomali ThreatStream is an AI-powered threat intelligence platform (TIP) built to unify external threat intelligence with internal relevant telemetry. It automates the process of correlating IoCs, TTPs, and campaigns to your environment, turning data into actionable decisions.

Backed by the industry's largest curated threat intelligence repository, ThreatStream uses agentic AI, automation, and machine learning (ML) to help analysts detect, investigate, and respond faster, all while reducing noise and operational overhead.

What's New

Capability	What It Does	Why it Matters
AI-Generated Threat Profiles	Automatically merges threat actor identities across multiple feeds, frameworks, and vendors into single unified profile (e.g. APT28 = Fancy Bear = Strontium)	Removes manual aliasing, speeds attribution, and delivers a single source of truth
Model Context Protocol (MCP) Server Integration	Securely connects ThreatStream intelligence into AI assistants like Claude and ChatGPT	Get verified Anomali intelligence without leaving your workspace
Agentic Chat	Understands natural-language questions and delivers context-aware, actionable answers directly in workflows	Reduces noise, accelerates investigations, and delivers context-rich, actionable answers
Knowledge Graphs	Maps relationships between actors, malware, infrastructure, campaigns, etc.	Turns fragmented data into connected intelligence for faster pattern recognition

Capability	What It Does	Why it Matters
Intelligence Digest	Turnkey dashboards combining threat intelligence and internal telemetry for real-time visibility	Gives analysts and CISOs strategic, actionable insights, aligning tactical detections with broader decisions
Dynamic Attack Flow	Embeds evolving attack models directly into investigations	Provides collaborative visual context for clear analysis and faster response
Anomali Cyber Watch	Weekly analyst-curated feed of global threat bulletins integrated within ThreatStream	Keeps analysts continuously updated on recent events for deeper, faster investigations

Core Benefits

ThreatStream turns intelligence into action, providing consistent visibility, context, and operational efficiency across every workflow.

- **Faster, Smarter Detection:** Correlates the world's largest threat depository with internal telemetry to surface the most critical threats.
- **AI-Powered Automation:** Agentic AI and NLP accelerate enrichment, scoring, and investigation workflows.
- **Seamless Integration:** Connects easily with SIEM, SOAR, EDR, and XDR tools to operationalize intelligence across your ecosystem.
- **Context-Rich Insights:** Combines curated threat data with relevant telemetry to deliver confidence in every decision.
- **Collaborative Defense:** Secure sharing via ISACs and Trusted Circles enables collective detection and response across peers and partners.

Get Started

ThreatStream is the intelligence brain for modern security. ThreatStream unifies curated global intelligence with real-time telemetry and AI reasoning. It delivers visibility, context, and speed at scale to empower your team to detect, investigate, and respond with precision.

To learn more about Anomali ThreatStream, contact your account manager or request a demo.

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