ANOMALI

One-pager

ANOMALI THREATSTREAM NEXT-GEN PRIORITY INTELLIGENCE REQUIREMENTS (PIRs) OVERVIEW

PIRs ARE CHALLENGING TO MANAGE

Priority Intelligence Requirements (PIRs) are focused threat intelligence questions that help organizations prioritize what matters most in the threat landscape. Defined around specific industries, geographies, or risk areas, PIRs guide teams in monitoring the threats most relevant to their business.

Creating and managing PIRs is often a manual, time-consuming process. CTI teams repeatedly perform the same research tasks—searching feeds, reviewing threat models, and enriching IOCs—without automation or a record of prior findings. This lack of continuity leads to duplicated effort, missed signals, and increased analyst fatigue. In many cases, PIRs are tracked in spreadsheets, making them difficult to maintain, scale, and update consistently.

OPERATIONALIZE PIRs WITH THREATSTREAM NEXT-GEN

ThreatStream Next-Gen enables teams to operationalize PIRs by transforming them into continuously running intelligence workflows. Instead of manual, one-off research, PIRs automatically track defined business risks and deliver relevant results on a scheduled cadence.

With built-in automation and AI-driven analysis, CTI analysts can continuously monitor the threat landscape while eliminating duplicate findings and repetitive effort—ensuring they focus only on the intelligence that matters most.

PIRs use defined threat data, such as observables and threat models, and apply AI-driven analysis to generate actionable outputs, including new threat models, tagged IOCs, workflow tickets, and alerts.

Once configured, PIRs run continuously on a scheduled cadence, automatically analyzing results and producing updated intelligence on a daily, weekly, or monthly basis.

By continuously analyzing its own outputs across every run, ThreatStream Next-Gen PIRs surface only net-new intelligence, eliminating duplicate findings and preventing analysts from reprocessing the same data. This reduces noise, ensures consistent coverage, and keeps teams focused on emerging risks that matter most.

AI-driven analysis accelerates time-to-insight by generating clear, actionable conclusions before triggering downstream actions. With flexible outputs and seamless workflow integration, PIRs fit directly into existing SOC and CTI operations.

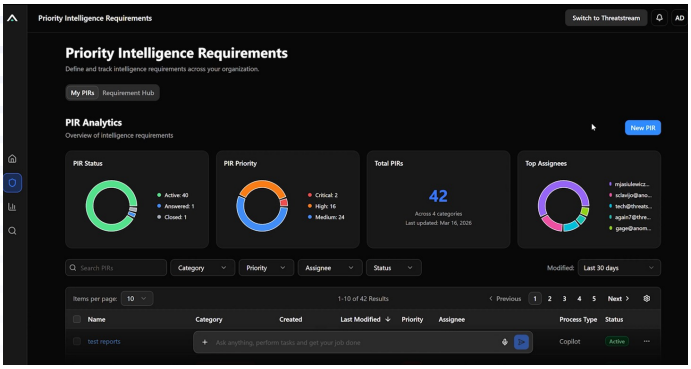
ThreatStream Next-Gen makes it easy to publish and share PIR results across the organization, helping teams communicate relevant threat intelligence to key stakeholders.

With full accessibility through the Anomali Model Context Protocol (MCP) API, PIRs enable agentic CTI workflows where AI systems can programmatically read, update, and act on intelligence.

The result is a continuously running intelligence engine that reduces manual effort, improves clarity, and transforms raw threat data into consistent operational action.

THREATSTREAM NEXT-GEN PIRs DRIVE INTELLIGENCE OUTCOMES

- Eliminate repetitive manual research cycles: Automate recurring intelligence collection aligned to organizational priorities, transforming raw threat data into structured, actionable responses.
- Run PIRs on your schedule: Execute automatically on a configurable cadence (e.g., hourly), with a “Run Now” option for immediate or ad hoc analysis.
- Synthesize structured threat data: Use defined inputs — including observables and threat models — for each PIR run.
- Apply AI-driven analysis: Extract keywords, recommend tags, and generate structured conclusions before triggering downstream actions.
- Surface only net-new intelligence: Analyze results across runs to eliminate duplication, reduce noise, and highlight meaningful changes.
- Publish to multiple destinations: Deliver results to threat models (with tagging), tagged IOCs, Jira, ServiceNow, Slack, and ThreatStream alerts through a unified workflow.
- Enable API-driven automation: Access PIR data and outputs via the Model Context Protocol (MCP) API to support orchestration and agentic CTI workflows.



WHY LEADING ENTERPRISES RELY ON THREATSTREAM NEXT-GEN

Hundreds of Fortune 1000 organizations trust ThreatStream Next-Gen to operationalize threat intelligence because it delivers real-world results.

- Accelerates detection and response by seamlessly distributing intelligence across the security ecosystem
- Unifies intelligence and telemetry for instant context and precise prioritization
- Reduces tool sprawl with a single, integrated intelligence platform
- Empowers analysts with flexible search — from advanced queries to natural language
- Enables collective defense through secure intelligence sharing

SEE ANOMALI IN ACTION

Request a Demo