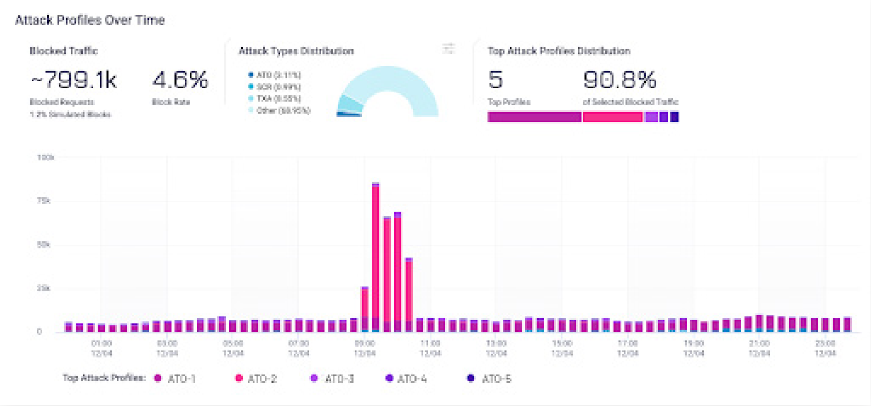
HUMAN

Threat Tracker

Isolate attack paths, characteristics, and actions of distinct attacker profiles, and track changing behavior over time

Threat Tracker isolates your automated traffic into distinct bot profiles, so you can uncover in granular detail what each attacker is doing on your specific application. Anomaly detection and signature mapping are not enough to understand your threat narrative. Part of HUMAN Sightline Cyberfraud Defense, Threat Tracker goes far beyond these traditional approaches, offering never-before-seen insights into individual bots' behavior over time.



Attack Profiles Over Time

Blocked Traffic

~799.1k
Blocked Requests
1.2% Simulated Blocks

4.6%
Block Rate

Attack Types Distribution

- ATO (3.11%)
- SCR (0.99%)
- TXA (0.55%)
- Other (95.35%)

Top Attack Profiles Distribution

5
Top Profiles

90.8%
of Selected Blocked Traffic

Benefits

FOCUS AND ACCELERATE INVESTIGATIONS

Turn hours of exploratory analysis into a quick, focused examination of contextualized data. Threat Tracker surfaces distinct bot activities, attack paths, and changing behaviors — like bots targeting specific products or visiting select pages. Security teams can uncover hidden patterns and zero in on key attacks, revolutionizing their investigative capabilities.

TRANSFORM ATTACK DATA INTO A BOARD-READY THREAT NARRATIVE

Easily tell your bot attack story to key stakeholders and showcase your team's impact. Threat Tracker allows teams to present business-level visualizations of bot behavior and show the effect of their actions over time. This empowers security teams to lead with data-backed authority, bridging the gap between deep technical analysis and business actions.

OPTIMIZE YOUR SECURITY STRATEGY FOR YOUR UNIQUE THREATS

Make strategic decisions based on the specific threats you face. With Threat Tracker, security teams can gain unprecedented clarity on each attacker's actions and intent, define threat priorities. This real-time adaptability enables security teams to proactively identify new threat patterns, respond faster and stay agile against evolving risks.

How It Works

Threat Tracker is powered by HUMAN's secondary detection engine, which uses layered AI models to compare all current and past traffic on a specific application. It identifies distinct bot profiles based on unique characteristics and attacker actions, going far beyond anomaly detection or signature mapping.

ANALYZE

Purpose built AI algorithms analyze automated traffic data in aggregate after an initial bot-or-not decision is made.

ISOLATE

AI models isolate and segment the automated traffic into distinct bot profiles based on its characteristics and actions.

REPORT

Distinct bot profiles are surfaced in the HUMAN console, with details on their behavior, capabilities and characteristics.

Key Capabilities

Deep Threat Insights
Provides details on attackers' target routes, characteristics, and capabilities, as well as the specific indicators of automated activity, to improve understanding of what exactly happened during an attack.

Adaptive Learning and Detection
Purpose-built AI models spot nuanced bot behavior shifts as they happen and automatically optimize mitigation workflows based on evolving bot characteristics.

Bot Indicators and Capabilities
Understand why certain traffic was flagged as a bot and see the specific actions it was taking to evade detection.

Pattern Analysis
Automatically correlate disparate bot activity to pinpoint bots' strategies, understand the scale of attacks, and identify threat patterns — without sifting through the raw activity data.

Continuous Tracking Over Time
Tracks bot profiles, including potential AI agents, to ensure a continuous line of sight and continuous protection even as attackers adapt and change tactics.

Bot vs. Human Traffic Visualizations
Compares characteristics of bot traffic to human traffic (e.g., IPs, ASNs, regions) to help teams visualize the data.

The Human Advantage

Detection without Blindspots

We verify over 20 trillion interactions weekly across 3 billion devices, connecting global dots to reveal threats others miss across the customer journey.

Intelligence at the Core

Satori isn't just threat intel, it's a team on the front lines. From uncovering global fraud rings to surfacing new attack patterns, every HUMAN decision is powered by real-time insights.

Precision that Performs

>2,500+ signals per interaction. 400+ adaptive models. Decisions in milliseconds. HUMAN turns massive telemetry into high-fidelity decisions you can trust.