SOLUTION BRIEF

Real-time threat intelligence for security data pipelines

Tenzir shifts threat intelligence triage left by applying alphaMountain's real-time verdicts to OCSF-aligned security data in the pipeline, so SOC teams decide what to alert on, what to lake, and what to automate before data reaches the SIEM.

Context before detection

Security teams collect more DNS, endpoint, network, identity, and cloud telemetry every year, but too much of it reaches detection systems without the contextual data needed to separate routine activity from active threats.

Post-ingestion enrichment arrives late and rarely covers everything. SIEM lookups add delay, batch updates miss fast-moving campaigns, and static lists leave analysts and agents operating on stale context.

Enrich in motion

Most teams enrich threat context after telemetry has already reached the SIEM. Tenzir moves that decision point upstream. Pipelines add intelligence while events flow from DNS, endpoint, network, and cloud sources toward SIEMs, EDRs, security data lakes, and automation tools.

With alphaMountain, Tenzir keeps threat intelligence current and brings it into the telemetry path where it can change outcomes. DNS, web, and network events can arrive with threat scores, categories, hostname intelligence, and supporting context already attached. Teams can route high-risk activity to the SIEM and AI SOC, keep full-fidelity OCSF data in a lake, and suppress low-value noise before it becomes analyst work.

Better together: Tenzir and alphaMountain

alphaMountain delivers high-fidelity threat intelligence for the infrastructure attackers use every day: domains, URLs, hostnames, and IP-related activity. Tenzir provides the programmable data layer that applies that intelligence to telemetry before the rest of the detection stack acts on it.

Detect threats earlier

Tenzir enriches events close to the moment users and systems generate DNS and web activity. Instead of waiting for analyst lookups or SIEM-side batch jobs, teams can classify activity with alphaMountain intelligence while the data is still in motion. The practical goal is simple: move decisions from hours-late lookup workflows to minute-level pipeline decisions.

Shift triage left

Early threat context helps distinguish malicious, benign, and low-priority activity before it creates analyst work. Teams can route high-risk

CHALLENGE

SIEM enrichment happens after ingestion, covers only a fraction of telemetry, and leaves analysts doing repetitive lookups when response time matters most.

SOLUTION

Tenzir uses alphaMountain's high-quality enrichment in the pipeline to triage DNS, web, and network telemetry: send high-risk events to the SIEM and AI SOC, keep full-fidelity OCSF data in the lake, and suppress low-value noise.

KEY RESULTS

- **Shift triage left:** Classify DNS, web, and network events in the pipeline before SIEM ingest and alert review.
- **Lower SIEM load:** Target 30–70% less hot-path volume by routing low-risk telemetry to the lake instead of the SIEM.
- **Minutes, not hours:** Replace batch enrichment and manual lookups with live verdicts while data is still moving.
- **Fewer analyst lookups:** Move enrichment into the pipeline so analysts and agents start with verdicts, categories, and context instead of querying threat intel by hand.
- **OCSF + AI SOC-ready:** Keep full-fidelity OCSF data in the lake while enriched events feed SIEM and AI SOC workflows.

events to detections and AI SOC workflows, keep full-fidelity OCSF telemetry available in the data lake, and suppress or deprioritize low-risk noise with more confidence. For a proof of value, this makes impact measurable: the percentage of telemetry kept out of SIEM hot paths, the improvement in alert quality, and the reduction in manual lookup time.

Keep intelligence fresh

Threat intelligence changes quickly. Tenzir avoids one-off CSV imports and manual refresh cycles by keeping alphaMountain feeds and live lookups connected to the data flow. Short-lived indicators can age out, recycled infrastructure creates fewer false positives, and OCSF-aligned detections stay aligned with current intelligence.

Equip agents

Agents need events that are already classified, contextualized, and ready for action. By attaching threat context before telemetry reaches the SIEM or data lake, Tenzir gives AI SOC workflows better input for decisions and leaves analysts with fewer repetitive enrichment tasks. Analysts and agents start from ranked, enriched events instead of raw logs and manual lookups.

Scale from proof of value to production

Teams can start with one high-value source, such as DNS or web proxy telemetry, and enrich it with alphaMountain intelligence before it reaches the SIEM. A strong proof of value measures three numbers: how much data shifts from SIEM hot paths to the lake, how much faster analysts understand risky events, and how many repetitive lookups disappear. From there, the same OCSF-aligned pattern can expand to more sources, more destinations, and more automated workflows without redesigning the architecture.

Summary

Threat intelligence is most valuable when it reaches telemetry before detection and investigation decisions happen. Tenzir and alphaMountain bring that context into the data pipeline: DNS, web, and network events become OCSF-aligned, pre-classified, and ready for SIEMs, security data lakes, detection tools, and AI SOC workflows. Security teams get earlier classification, fewer false positives, less manual enrichment, and a practical path from a focused proof of value to production-scale coverage.