ANOMALI

One-pager

INTELLIGENT UNIFICATION LAYER

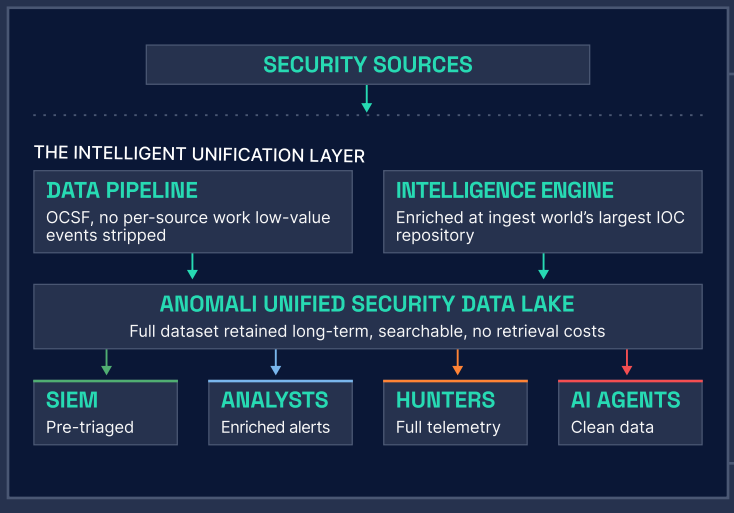
BEYOND DETECTING. START ACTING.

The operational and predictive data foundation that gives your SOC — and your AI agents — decision-ready data from the moment it lands.

Today's security teams run more than a decade's worth of detection tools — SIEMs, EDR, cloud, identity — each generating telemetry in its own format. That fragmentation was manageable when attackers moved in days; it isn't now, when AI-assisted attacks compress the time from initial access to exfiltration to minutes, and analysts sort through alert volumes where only a fraction are real threats.

Adding AI on top doesn't fix it: an agent handed raw, fragmented data makes the same mistakes a human would, only faster. The real blocker isn't a shortage of intelligence or tools — it's that the data those tools depend on was never unified, normalized, or enriched at the point it was created.

The Intelligent Unification Layer (IUL) is a unified data layer between the security tools you already own and the decisions your analysts and AI agents make. It ingests telemetry across the environment, translates it into one common schema, removes noise before it becomes an alert, and fuses vetted threat intelligence into every event as it lands.



A NEW APPROACH: OPERATIONALIZE INTELLIGENCE

That is operational intelligence: context that has already done its job by the time any analyst or agent sees the event.

- **Normalization at ingest** — every event translated to one common schema on arrival, so detection logic works the same across all sources.
- **Deduplication before the SOC** — duplicate events, beaconing, and known-good noise filtered out before they reach an analyst or agent.
- **Enrichment as infrastructure** — actor attribution, MITRE ATT&CK mapping, and confidence scoring fused into every event automatically.
- **Consistent, long-term retention** — data retained cost-effectively, so historical telemetry stays searchable when new threats surface.
- **Predictive correlation** — patterns in the retained data flag likely next-stage activity before it's directly observed.

HOW IT WORKS

The IUL is a unified, normalized, enriched, fully retained dataset every downstream system relies on: a Data Pipeline that translates every source to OCSF with no per-source engineering; a Unified Security Data Lake that retains the full dataset long-term and searchable without cold-storage retrieval costs; and an Intelligence Engine that enriches each event at ingest from one of the world's largest threat intelligence repositories.

START NARROW, PROVE IT FAST

You don't need a feed aggregator and a log warehouse that talk to each other by hand — you need an operationally intelligent data layer from day one. Start with one high-value use case, such as privilege escalation on a single identity source: ship the pre-built detections and see intelligence-enriched alert reduction inside 48 hours.

We're not asking you to replace your SIEM — we make it smarter. The bigger story earns itself, level by level, on your terms.

FITS YOUR ENVIRONMENT, HOWEVER YOU'RE SET UP

Because every source is normalized to a common schema (OCSF) the moment it's ingested, the IUL is genuinely neutral to what you run. Deploy it in front of a legacy SIEM, alongside or on top of an existing data platform, or standing on its own.

Threat actors already operate at machine speed, and boards already expect a credible path to AI-assisted defense. Every quarter on fragmented data widens the gap.

WHAT ORGANIZATIONS HAVE EXPERIENCED

Teams adopting the IUL report sharply lower alert volumes, faster investigations as pre-enrichment removes manual context-gathering, and simpler detection engineering. One organization replaced its legacy SIEM outright — major incident reduction, higher visibility, lower cost, and search times from days to seconds. Another consolidated 30+ cloud and on-premises sources in under four months.

FINANCIAL INSTITUTION

Replaced its legacy SIEM outright

90% fewer critical incidents

8x greater visibility

67% lower cost

U.S. STATE GOVERNMENT

Rapid multi-source onboarding

30+ data sources unified

<4mo to fully onboard

150+ OCSF detections deployed

Command Center: a single, continuously updated view of targeted organizations, trending malware, and top vulnerabilities.

Detections: rule and IOC matches trended by severity and mapped automatically to MITRE ATT&CK tactics.

SEE ANOMALI IN ACTION

REQUEST A DEMO

© Copyright 2026 Anomali Incorporated®. All rights reserved. ThreatStream® is a registered trademark of Anomali Inc.
Anomali Match™ ("Match"), Anomali Lens™ ("Lens"), and Anomali Copilot are trademarks of Anomali Inc.