Strike48: The Fastest Path to a Modern SIEM Architecture

Traditional SIEMs were designed for a world where storage was expensive. The economics forced teams to sample data, shorten retention, and accept blind spots. Migrating to a new model meant moving in costly and time-consuming phases in order to keep real-time alerting and investigation capabilities live.

Strike48's Prospector Studio gives security and IT teams a rapid migration path to a modern alternative. Strike48 delivers an agentic SOC on day one, while enabling a low-cost, flexible architecture that supports gradual SIEM migration, hybrid operations, and immediate cost reduction.

Three structural limitations your team works around every day

You're paying SIEM pricing for everything

Legacy SIEMs don't distinguish between hot operational data and long-term retention.

Investigations stop at the edge of your SIEM

When agents and analysts can only see what's inside the SIEM, investigations are bound by what you could afford to ingest.

Modernizing means a dangerous transition period

Migrating SIEMs is expensive and time- consuming, leaving many stuck in archaic platforms.

The architecture: One agentic layer uniting your existing stack

Prospector Studio supports a bifurcated backend that separates real-time security operations from long-term investigation and retention.

Leverage your existing SIEM infrastructure for streaming hot data. Utilize a low-cost S3 layer for long-term retention, high-volume telemetry, and the broad visibility data that legacy SIEMs force you to drop.

Prospector Studio sits above both as the agentic control plane. Autonomous agents search across the SIEM and S3 simultaneously, run multi-step investigations, and produce findings without analysts manually pivoting between systems.

What security operations looks like with a modern agentic layer

Full coverage without full SIEM pricing

By tiering logs between your SIEM and S3, you stop paying hot-storage rates for data that doesn't need it.

Investigations that span your entire data

Autonomous agents query across your SIEM and S3 simultaneously. Incident reconstructions are no longer bound by what you could afford to keep in hot storage.

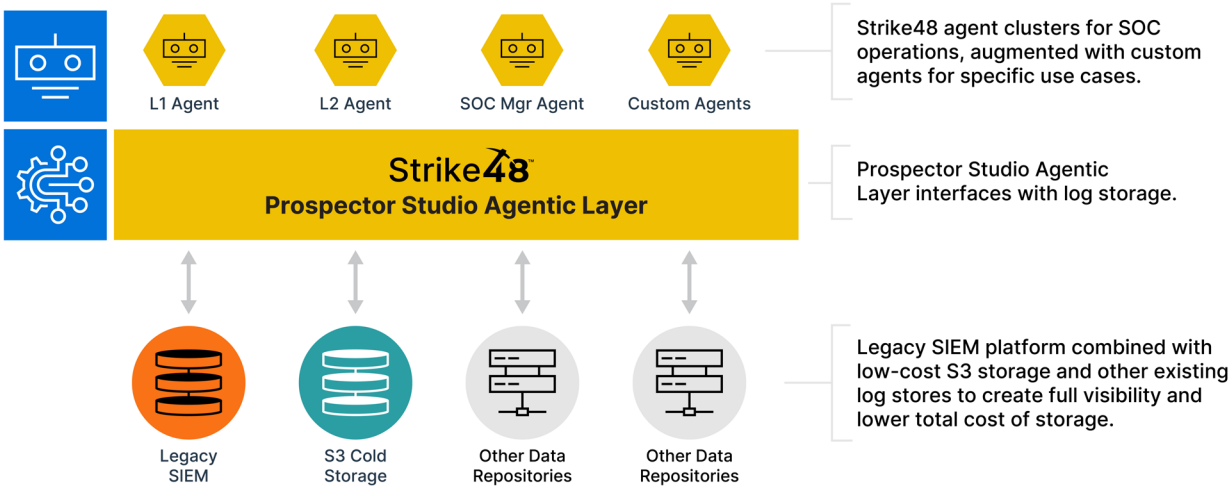
True agentic operations

Autonomous agents run Tier 1 triage and Tier 2 investigations end-to-end. Analysts get enriched, contextualized findings across every log source you have, all conducted at machine speed.

A safer path to SIEM modernization

Connect to both legacy and new systems in parallel via MCP, so your SOC never goes dark. Historical data stays searchable in place — no re-ingestion required, no coverage gap.

The Strike48 agentic layer



How teams move to a modern log architecture with Strike48

1 Connect

Prospector Studio connects to your existing SIEM via MCP and to your S3 buckets directly. Nothing changes in your SOC. You gain immediate visibility into both layers from a single agentic interface.

2 Tier Logs

Move high-volume, low-urgency data out of hot SIEM storage and into S3. Your SIEM handles real-time detections and active incidents. S3 handles retention, telemetry, and broad investigation data.

3 Optimize

For many teams, the dual architecture becomes the permanent operating model: lower cost, broader coverage, full agentic investigation. Optionally, migrate off your legacy SIEM entirely for full optimization.

The bottom line: Strike48 is the fastest path to an agentic SOC

Strike48 Prospector Studio is uniquely powerful for organizations migrating off legacy SIEMs because it was designed for the transition period—not just the destination.

- Modernize without downtime
- Reduce SIEM costs immediately
- Preserve historical investigations
- Search data in place
- Adopt an agentic SOC without ripping out what already works
- Expand visibility by shifting retention to S3

See Prospector Studio running in your SIEM environment

Full log visibility, Agentic Analysts, 24×7 eyes on glass.