

WHAT HIGH-FIDELITY DATA MEANS FOR THE AGENTIC SOC

Agents don't fail on model quality alone. They fail on the data underneath them. This is how to judge whether your security data is good enough for an agent to reason on, and act from.

An AI agent working an alert doesn't run one query and stop. It explores the data, forms a hypothesis, tests it, and iterates. Every step reads from your security data, which means the quality of the agent's decision is capped by the quality of the data beneath it. A human analyst can paper over a gap with instinct or a quick call to another team. An agent inherits the gap as a flaw in its reasoning, then repeats that flaw across every case it touches.

High-fidelity data is security data an agent can safely reason on and act from. Four properties make it measurable.

1. COMPLETENESS

Every relevant signal is present and kept long enough to matter. Nothing sampled away, nothing aged out early.

Example. Reconstructing a slow intrusion can take a year or more of history. If retention limits dropped everything past 90 days, the agent reasons over a partial timeline and never sees the first foothold.

Agent impact. An agent reads missing data as evidence that nothing happened, then closes the case.

2. CONSISTENCY

Every source speaks one schema. A field means the same thing everywhere, and duplicate records are resolved before analysis.

Example. Endpoint, firewall, and identity logs each name the same user a different way. A person reconciles it by eye. An agent joins on the wrong field and ties together two events that were never related.

Agent impact. Inconsistent data produces correlations that are confident and wrong. OCSF normalization is what closes the gap.

3. ENRICHMENT

Raw signal arrives carrying context: threat intelligence, asset criticality, identity, and prior incident history.

Example. A connection to an unfamiliar address means nothing on its own. Fused with threat intelligence and the role of the asset involved, it resolves into either background noise or a priority-one event.

Agent impact. Raw signal tells you what happened. Context tells you what it means. Without it, an agent can only describe. With it, an agent can decide.

4. PROVENANCE

Every data point carries its origin, its timestamp, and its handling history, so any conclusion traces back to source.

Example. An agent recommends isolating a host. Before you approve, you need to see the exact records that drove the call and where each one came from.

Agent impact. Provenance makes a decision explainable, reversible, and defensible to an auditor. Without it, autonomy is a risk you can't sign off on.

THE FOUNDATION OF THE AGENTIC SOC

An agentic SOC starts with high-fidelity data. Anomali centralizes security telemetry, normalizes it to OCSF, removes duplicates, and enriches it with intelligence, so agents reason on a foundation built for the job.

This data fabric sits between the security tools you already own and the decisions your people and your agents make. It ingests everything, normalizes it into one schema, strips out the noise before it ever becomes an alert, and fuses vetted intelligence into every event as it lands.

[Find out how](#) Anomali helps you power a SOC that can see everything, know what matters, and act with confidence.



FINANCIAL INSTITUTION

One financial institution replaced its legacy SIEM outright and saw:

90%

fewer critical incidents

8x

greater visibility

67%

lower cost

SEE ANOMALI IN ACTION

[Request a Demo](#)