OcientAIQ for Threat Detection and Response

Full-fidelity network and IT telemetry joined to detect threats the SIEM alone cannot retain.

The Problem

Carrier security teams are defending against threats that move slowly, hide in weak signals, and span more telemetry than the security stack can economically retain. IPFIX and NetFlow, DNS and DHCP, signaling, endpoint telemetry, firewall and proxy records, application logs, and security events all exist — but they rarely remain full-fidelity, joined, and queryable across the full life of an intrusion. The pressure shows up in three places:

Dwell time outlasts retention. Low-and-slow intrusions can span weeks or months, while searchable telemetry only covers the most recent activity.

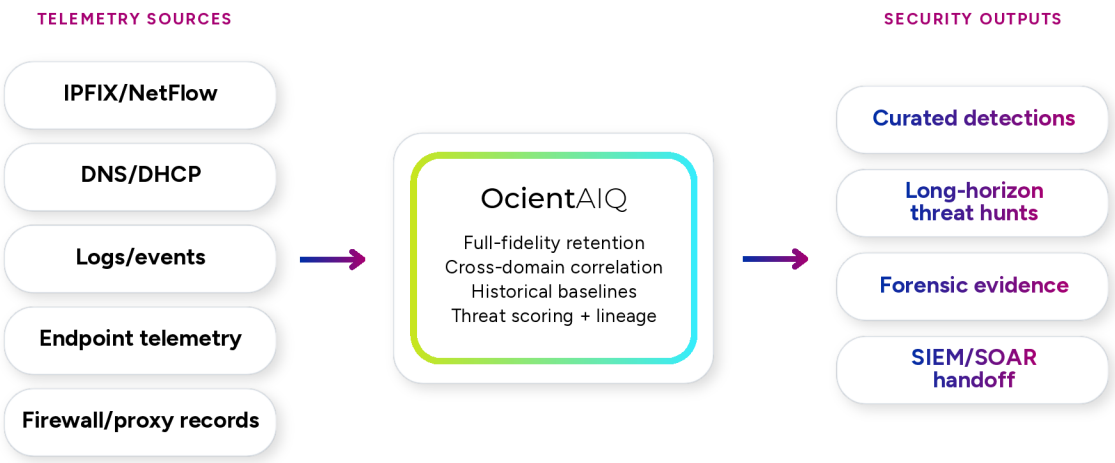
Sampling misses the long tail Reconnaissance, command-and-control, and slow exfiltration often live in the patterns that aggregation erases.

Evidence is split across domains. Flow, DNS, signaling, endpoint, and application events must be joined to prove what happened, but are rarely queryable from one place.

The Solution

OcientAIQ™ gives CSP security teams a full-fidelity analytical foundation beneath the SOC. It retains network and IT telemetry at carrier scale — IPFIX, NetFlow, DNS, DHCP, signaling, IPDR, logs, endpoint telemetry, firewall and proxy records, and other security-relevant events — and keeps that history queryable for long-horizon threat hunting and forensic reconstruction.

The SIEM remains the SOC pane of glass for real-time alerting, triage, dashboards, and playbooks. OcientAIQ sits underneath it as the retention, analytics, and detection layer: correlating the complete historical record, publishing curated detections back to the SIEM, and preserving drill-back access to the source evidence behind every finding. With OcientAIQ, analysts shift from looking at what is still searchable to seeing what actually happened.



How OcientAIQ Strengthens Threat Detection and Response

Long-horizon threat hunting. Hunt across full-fidelity network, DNS, signaling, and log history over months or years — not just the SIEM hot window.

Cross-domain correlation. Join IPFIX, DNS, DHCP, signaling, endpoint, firewall, proxy, and application events to reconstruct activity across domains.

Historical baselining and anomaly detection. Compare current behavior against years of retained telemetry across protocol, port, prefix, direction, geography, subscriber, device, or service context.

Threat-pattern detection. Match malicious infrastructure, obfuscation networks, suspicious beaconing, scanning behavior, and spoofed flows against the full retained corpus.

Forensic evidence and drill-back. Send curated detections to the SIEM with links back to the full-fidelity records and lineage behind each finding.

SIEM hot-tier offload. Publish curated detections, context, and drill-back links into the SOC workflows already in place, while OcientAIQ preserves the full-fidelity evidence behind them.

What Makes OcientAIQ Different

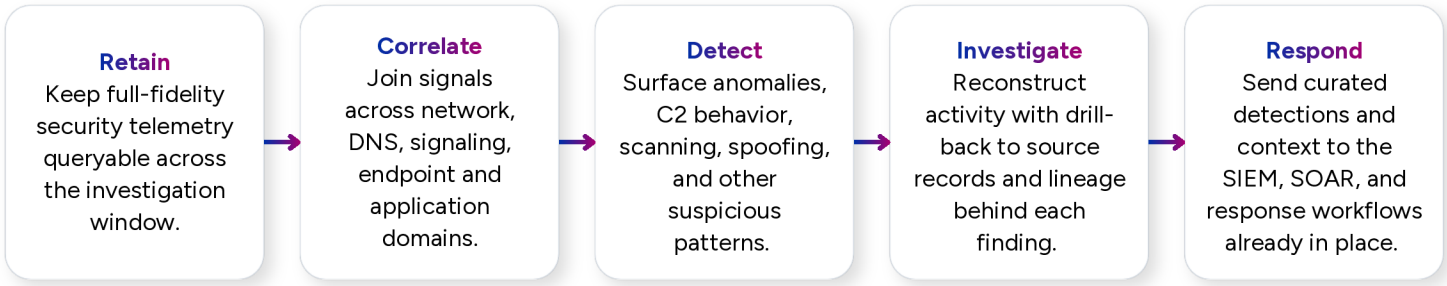
Extends the SOC without disrupting it. OcientAIQ sits beneath the SIEM as the full-fidelity analytics layer, preserving existing workflows while extending the history analytics can hunt.

Built for the cross-domain hunt. Threats rarely stay inside one source. OcientAIQ joins telemetry across domains so analysts can reconstruct activity from first signal to finding.

Full-fidelity, not sampled history. OcientAIQ retains unsampled security telemetry across long horizons, not sampled probes, summarized extracts or short retention windows.

Predictable economics for long-horizon security analytics. Capacity pricing lets teams hunt, investigate and score the retained corpus without turning every query into a new cost event.

Value at Every Stage



Ready to hunt beyond the SIEM hot window?

sales@ocient.com ocient.com