INDUSTRIALIZING DATA FOR MODERN CYBER OPERATIONS

Real-time, hyperscale analytics for cyber defense and cyber threat intelligence

Modern cyber operations are constrained less by collection and more by the ability to process, correlate, and operationalize massive volumes of heterogeneous security data in near real time. Organizations ingest billions of events daily across network flow and DNS telemetry, endpoint and identity logs, cloud and SaaS audit events, breach datasets, and external threat intelligence.

Schemas drift. Formats change. Historical retention remains critical for attribution, threat hunting, and compliance. Without industrial-scale processing, detection fidelity declines, investigations slow, and threat intelligence cannot be operationalized effectively.

Designated Awardable in the
DoW CDAO Tradewinds Marketplace

List of Federal Contracts Available on Request

One Platform Beneath the SOC

Ocient provides the industrial-scale data transformation and correlation layer beneath existing SIEM, SOC, and CTI systems — strengthening mission platforms rather than replacing them.

- Hyperscale correlation across multi-source security and intelligence data
- Long-horizon hunting and large-scale indicator matching without sampling
- Unified ETL, analytics, and ML execution in a single environment
- Near real-time analysis across trillions of records with secure, sovereign, and air-gapped options

High-Impact Cyber Use Cases

Cyber Threat Intelligence at Scale
Match millions of IPs, domains, and artifacts against historical telemetry. Run TTP hypotheses across months or years of retained data. Correlate infrastructure to uncover patterns.

IOC Lifecycle Validation
Identify when indicators first appeared, what behavior they drove, and how they evolved — reducing false positives and improving confidence in decisions.

Breach & OSINT Industrialization
Ingest chaotic mixed-format datasets, normalize inconsistent schemas, extract entities at scale, and produce structured, mission-ready intelligence assets.

AI as a Force Multiplier
Apply behavioral modeling, classification, schema inference and entity resolution directly against large-scale datasets – without exporting data to fragmented environments.

The Outcome

Organizations leveraging Ocient for cyber operations achieve faster time to answer for complex investigations, improved detection accuracy through broader baselines, and scalable, repeatable exploitation of breach and OSINT datasets. By reducing fragmented infrastructure and sustaining performance under surge conditions, Ocient maintains investigative tempo and strengthens confidence in cyber threat intelligence and response decisions.

TURN SCALE INTO OPERATIONAL ADVANTAGE WITH OCIENT

ONSS@ocient.com ocient.com