OCIANA® provides the operational intelligence layer required to protect critical underwater infrastructure.

We help you detect behaviour early, determine intent, and act before impact. In the CUI domain, awareness without action is just expensive observation.

About OCIANA®

OCIANA® is the maritime operational intelligence layer that turns volumes of maritime data into clear, explainable insight on vessel behaviour. It enables operators to detect threats earlier, determine intent, maintain attribution over time, and act with confidence in complex and ambiguous environments.

To learn more, visit gsts.ca.

CANADA

329 De la Commune St W,
Montreal, QC H2Y 2E2

1 Research Dr, Dartmouth,
NS B2Y 4M9

911 Yates St,
Victoria, BC V8V 4X3

UNITED KINGDOM

Fortis House, Cothey Way,
Ryde PO33 1QT

www.gsts.ca

GSTS®

Protecting Critical Underwater Infrastructure

Before, during, and after an incident

OCIANA® delivers persistent behaviour analysis of maritime activity around subsea critical underwater infrastructure, enabling early detection, real-time awareness, and post-incident investigation.

Reality of CUI Risk

Critical underwater infrastructure (CUI) is exposed, distributed, and inherently difficult to monitor.

Threats move, adapt, and operate below traditional detection thresholds.

- **Grey-zone interference** and deliberate disruption
- **Anchoring, loitering,** and suspicious proximity behaviour
- **AIS manipulation,** spoofing, and dark vessel activity
- **Fragmented visibility** across agencies and operators

Most systems detect events, but very few explain them.
Almost none provide attribution continuity.

OCIANA® Approach

OCIANA® monitors vessel behaviour, not just infrastructure. It surfaces vessels exhibiting defined risk conditions and provides the context needed to determine whether activity is routine, anomalous, or intentional.

- **Persistent behaviour analysis** of maritime activity
- **Detection of grey-zone** and non-compliant vessel behaviour
- **AIS anomaly** and identity manipulation detection
- **Correlation of vessel activity** with subsea events
- **Investigation** and playback
- **Operator-defined** monitoring conditions
- **Secure multi-agency** collaboration

No data overload | No black-box scoring | Operationally relevant insight only

Operational Coverage Across CUI Lifecycle

Plan with awareness

Understand historical vessel behaviour along proposed routes. Identify high-risk zones before deployment.

Monitor what matters

Detect vessels entering sensitive areas and identify abnormal behaviour such as loitering, route deviation, or AIS anomalies.

Correlate incidents in real time

Align vessel activity with subsea events to determine who was present, what they were doing, and whether it was coincidence or intent

Investigate with confidence

Replay vessel movements, identify repeat patterns, and support enforcement or intelligence actions.

Bring Your Infrastructure Data. Keep Your Control.

OCIANA® enables secure ingestion of sensitive CUI overlays:

- Infrastructure data remains isolated to the owning organization
- Access is strictly controlled by user and role
- Supports cable routes, protection zones, and subsea sensor inputs
- Enables direct correlation between vessel behaviour and infrastructure