TIDAL CYBER

A New Era In Threat-Led Defense Begins Here.

# Flexible Threat Intelligence Integration

## Centralizing Threats & Adversary Behavior

Seamlessly integrate any threat intelligence source and maps it to MITRE ATT&CK® for immediate operational impact with the Tidal Cyber Threat-Led Defense Platform.

MITRE | ATT&CK®

**TIDAL CYBER CONTENT CURATION**
(AI+Human+ATT&CK)

**THIRD-PARTY TI PROVIDERS**
(Expanded TI Volume)

**CUSTOM THREAT INTEL**
(Internal, DFIR)

**THREAT INTELLIGENCE NORMALIZATION**

- Align to MITRE ATT&CK Techniques ***and*** Procedures
- Correlate Across Internal and External Sources
- AI-Assisted Extraction & Enrichment

**DATA ANALYSIS & CORRELATION**

- Behavioral Patterns
- Anomalies (New Techniques)
- Mapping to Known TTPs

**THREAT INTELLIGENCE AGGREGATION & PRIORITIZATION**

- Threat Actor Profiles
- Attack Chains & Campaign Content
- Tool/Tech-Specific Threat Modeling
- Prioritized Threats Targeting Deployed Controls

**THREAT PROFILE CREATION**

- Continuous Update Automation
- Curated & Custom Profiling
- Apply Granular Threat Weightings
- Immediate Context on Relevant Threats

**OPERATIONALIZATION**

- Detection Engineering
- Incident Response
- Reporting
- Threat Hunting
- Control Validation
- Threat Modeling (Purple/Red)
- Reporting & Risk Comms
- Exposure Mapping

**COVERAGE MAPPING**

- Pair with Defensive Capabilities
- Calculate/Boost Confidence Score
- Actionable, Tailored Recommendations

**FEEDBACK LOOP**

- Adjust Detections Based on New Attacker TTPs
- Refine Tooling Based on Control Validation
- Continuous Refinement of Threat Models & Controls

Security teams can add their own techniques with some limitations.

# Threat Intelligence Partners

Ingesting threat intelligence from global TI partners enhances the value of Tidal Cyber's Threat-Led Defense Platform by enriching your view of adversary behavior with diverse, complementary insights aligned to your environment.

Recorded Future

ThreatConnect.

servicenow

LOLBAS

Mandiant

INTEL471

CROWDSTRIKE

Trellix

Vertex

## Our Partners Are Force Multipliers

### Enrich Intel, Harden Controls, Close Feedback Loops, and Demonstrate Risk Reduction

Tidal Cyber is the first true Threat-Led Defense platform built to flip the traditional defensive model by putting real adversary behavior at the center of your defense strategy. Threat-led defense moves beyond assumptions, CVE-counting, and checkbox compliance. By mapping techniques, sub-techniques, and procedures to ATT&CK, we reveal exactly where you're exposed and how attackers actually execute TTPs.

It's a level of precision you've never had before, empowering your security team to proactively reduce risk and optimize high-impact security investments.

Threat-Led Defense is Tidal Cyber's unique implementation of Threat-Informed Defense, enhanced with procedure-level granularity to make CTI more relevant and actionable.

**Shift to a proactive, continuous Threat-Led Defense *first.***

**Learn More About Tidal Cyber Threat-Led Defense at**
**contact@tidalcyber.com**



TIDAL CYBER