

HOW TIDAL CYBER ACCELERATED GROWTH FOR A NEW CYBERSECURITY CATEGORY: THREAT-LED DEFENSE



Industry: Cybersecurity / Threat Intelligence / Threat-Led Defense



Business Model: SaaS Cybersecurity Platform delivering Threat-Led Defense and threat-informed security decision support



www.tidalcyber.com



EXECUTIVE SUMMARY

Tidal Cyber is the category creator and leader in Threat-Led Defense, helping organizations align security controls and investments to real-world adversary behavior. As market demand for threat-informed security increased, Tidal Cyber experienced strong technical validation through proof-of-concept engagements and practitioner adoption.

However, like many innovative cybersecurity platforms early in their lifecycle, the team encountered a common go-to-market challenge. While technical evaluations were successful, too many opportunities stalled before converting to closed deals, often ending in “do nothing” outcomes when business leaders entered the decision process.

To accelerate growth, Tidal Cyber partnered with Genius Drive to evolve from a product- and practitioner-led motion to a **value-led sales and customer success approach**, grounded in credible, quantified business outcomes. This shift helped Tidal Cyber clearly articulate the economic and operational value of Threat-Led Defense, accelerating deal velocity, supporting executive-level decisions, and contributing to **115% annual growth**.

CHALLENGE

Tidal Cyber’s platform resonated strongly with security practitioners during technical evaluations and proofs of concept. However, the team faced several challenges as opportunities progressed:

- Proofs of concept demonstrated technical capability, but **did not consistently convert into executive-approved deals**.
- Too many opportunities stalled or ended in “do nothing” outcomes when buyers struggled to justify the investment in business terms.
- As a new category, **Threat-Led Defense lacked established benchmarks** for articulating and quantifying business value, and a repeatable way to communicate that value to new prospects.

Tidal Cyber recognized that accelerating growth would require moving beyond technical validation to **credible, outcome-focused value positioning** that resonated with CISOs, security leaders, and executives.



ANN CHESBOROUGH,
TIDAL CYBER

As a new category, quantifying the value of Threat-Led Defense hadn't really been done before. Genius Drive helped us clearly define and quantify the value impacts, and backed it up with credible analysis and support that our customers and prospects could trust.

SOLUTION



Capturing and Codifying Realized Customer Value

Genius Drive analyzed realized value from existing Tidal Cyber customers, identifying clear operational, financial, and risk-reduction outcomes enabled by Threat-Led Defense. These insights were captured in customer success stories used directly in prospect, renewal, and expansion conversations.



Developing Credible Value Positioning and Thought Leadership

Building on this analysis, Genius Drive developed a value-focused white paper that articulated typical savings, efficiency gains, and risk reduction. This repositioned Tidal Cyber from a technically differentiated platform to a solution clearly anchored in business impact, especially for executive audiences.



Enabling Quantified, Executive-Ready Value Conversations

Genius Drive delivered a Business Value Framework and supporting value presentation to quantify and communicate value for each prospect. This enabled Tidal Cyber to justify investment beyond technical proof points, accelerate renewals and expansions, and confidently present value in strategic deals.



RICK GORDON,
CO-FOUNDER & CEO
TIDAL CYBER

Getting a handle on our value positioning early in our lifecycle was critical. Genius Drive helped us move beyond technical validation and clearly articulate the business impact of Threat-Led Defense. That clarity played an important role in accelerating our growth and setting us up for continued success.

RESULTS AND BENEFITS

The partnership with Genius Drive delivered both immediate and strategic impact:



Accelerated Tidal Cyber's evolution to **value-led sales and customer success**



Established a credible, defensible framework for quantifying the value of Threat-Led Defense



Reduced stalled opportunities by equipping teams to engage executives with confidence



Strengthened renewal and expansion conversations with quantified outcomes

Most importantly, the value-led approach supported Tidal Cyber's broader growth trajectory:



115% annual growth in 2025, placing Tidal Cyber among the top-performing SaaS companies at its stage



Reinforced Tidal Cyber's position as **one of the fastest-growing cybersecurity companies in the market**



Entered 2026 with strong audit momentum, disciplined scale, and a clearer articulation of measurable customer value

↓ 40%

Reduction in tool overlap usage, saving \$250K-\$500K annually through threat-informed prioritization.

↑ 80%

Increase in control efficiency by identifying underperforming tools aligned to TTPs.

↓ 30%

Fewer tool purchases when security leaders demonstrate they can meet TTP coverage requirements with existing tools.



Increase Security Tool Efficiency

↓40% less tool overlap, resulting in annual cost savings of \$250K-\$500K for mid-sized to large enterprises.



Reduce Cyber-Insurance Premiums

↓15 to 30% annual savings can be realized with CTI optimized coverage and reporting.



Reduce Mean Time to Prioritize Threats

↓60% reduction in time to prioritize detections and mitigations by aligning actions to adversary behavior instead of CVE scores.



Ensure GRC and SecOps Team Alignment

↓65% less time spent aligning GRC and SecOps when using shared threat-informed views of exposure.



Automate Reporting

↓3x reduction in time (a 67% savings) automating reports, including weekly threat intelligence operational reports and quarterly board-level reports.



Accelerate Audit Prep

↑90% faster audit preparation by integrating control framework mapping directly into threat-aligned defensive coverage views, eliminating manual efforts and streamlining evidence collection across teams.



Decrease the Probability of Attack Success

↑2x Improvement in accuracy using threat context (TTP) to inform detection logic.
↑70% Increase in validated control coverage across ATT&CK techniques and sub-techniques
↓50% Fewer coverage blind spots after mapping to adversary procedures (vs. techniques-only).
↑2.5x Improvement in detection fidelity (actual vs. assumed coverage)

Cost Avoidance

Productivity / Process Improvements

Reduced Risk & Improve the Business

Accelerate Time to Value - From months to days