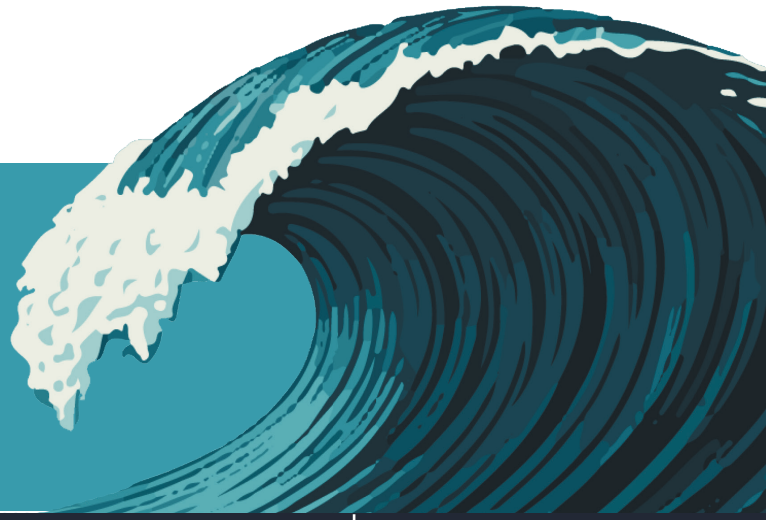
TIDAL CYBER

Case Study:

IMPROVED DETECTION COVERAGE MEASUREMENT EFFICIENCY BY 10X



INDUSTRY	ANNUAL REVENUE	EMPLOYEES	LOCATIONS
U.S.-based Financial Services company	$16 billion	22,000	Throughout U.S.

DETECTION ENGINEERING CHALLENGES

- Lack of Visibility & Prioritization
- Inefficient Detection Development
- Resource Constraints & ROI Concerns

TIDAL CYBER SOLUTION

- Detection Engineering Prioritization

OUTCOME

10x increase in analyst productivity

$500 reclaimed efficiency per TTP

INCREASED **ROI** of the detection engineering team

THE CHALLENGE

A financial services firm struggled to write detections efficiently, raising concerns about the return on investment (ROI) of its detection engineering team.

Without a structured approach to assessing ATT&CK coverage, managing detection overlap with vendors, or prioritizing new detections, the team faced inefficiencies that hampered resource allocation and security coverage.

Compounding the issue, the firm lacked visibility into its detection landscape. Engineers had difficulty evaluating their strengths, identifying gaps, and minimizing redundant efforts. Researching threats was time-consuming, and prioritizing which detections to build next was a constant challenge. Many custom detection rules overlapped with vendor-provided rules, leading to wasted effort without enhancing the firm's overall resilience.

The absence of an organized detection engineering strategy resulted in slower response times, inefficiencies in leveraging vendor solutions, and a suboptimal security posture. The firm needed a way to streamline detection development, eliminate redundancies, and maximize the effectiveness of its security investments.

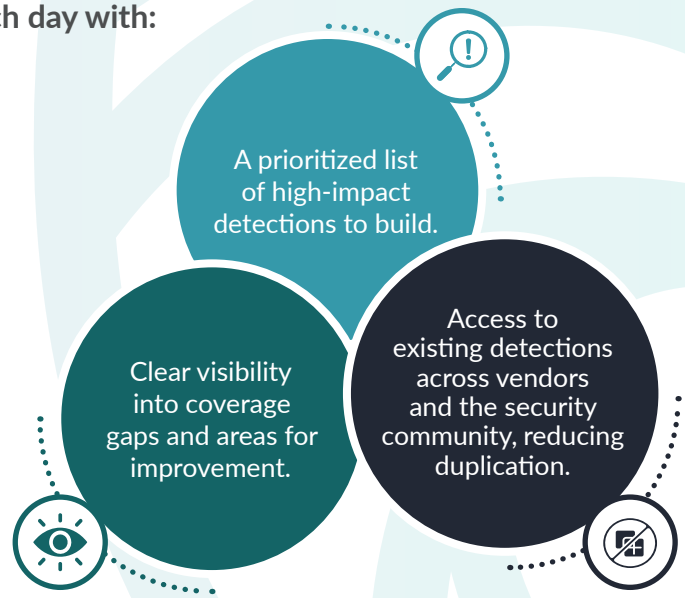
> *Efficiently performing and scaling this analysis is not feasible without Tidal Cyber's platform.*
> – Senior Detection Engineer

tidalcyber.com
@TidalCyber
tryenterprise@tidalcyber.com
company/tidalcyber/

THE SOLUTION

Tidal Cyber provided a centralized system to streamline detection engineering, enabling end-to-end visibility from initial concept to implementation. Its product registry allowed detection engineers to overlay vendor-provided detections with their own, eliminating redundancy and maximizing efficiency. By integrating open-source and community-driven detections, the platform accelerated development and leveraged collective intelligence for stronger security outcomes.

With Tidal Cyber, detection engineers started each day with:



By automating detection prioritization and mapping sector-specific threat profiles against the firm's security stack, Tidal Cyber optimized workflows. Engineers could quickly identify and address coverage gaps, validate detection effectiveness using breach and attack simulation (BAS) tools, and focus on security enhancements that mattered most.

This automation-driven approach reduced redundant work, empowered engineers to make faster, more informed decisions, and ensured the firm maximized the value of its vendor and custom detections.

> *Our junior analysts were empowered to do so much more, freeing our senior team to improve our security posture and reduce risks.*
> – Senior Detection Engineer

THE OUTCOME

To measure the impact of Tidal Cyber's Detection Engineering Prioritization, the financial services firm conducted a side-by-side comparison of its efficiency gains:

A junior analyst using Tidal Cyber assessed the organization's TTP (Tactics, Techniques, and Procedures) coverage in **under 30 minutes**, completing a comprehensive analysis and using the remaining time to refine recommendations.

The junior analyst implemented **11 new detections** and **enhanced two existing capabilities** within the allocated time.

Meanwhile, a senior detection engineer, working manually without Tidal Cyber, spent nearly the **entire six-hour window** just compiling an inventory of existing detections, producing only **one new detection**.

By reducing analysis time per TTP from **six hours** to just **30 minutes**, Tidal Cyber delivered **$500 in savings per TTP**, and further enabled:

- **A 10x increase in detection engineering productivity** – Junior analysts delivered results previously limited to senior-level expertise, acting as a force multiplier that scaled impact without additional headcount. Senior engineers were freed to focus on strategic security initiatives rather than manual detection tasks.
- **Stronger threat coverage and faster response** – Real-time visibility into detection gaps enabled the security team to prioritize and address the most critical threats, significantly reducing risks without increasing costs.
- **Optimized resource utilization and assured ROI** – Eliminated redundant detection efforts, maximized the value of vendor-provided capabilities, and allowed engineers to focus on higher-value security improvements.

By empowering the detection engineering team with automation, real-time prioritization, and visibility, Tidal Cyber helped transform the financial service organization's security approach, making high-impact detection development more scalable, efficient and far-more effective.

tidalcyber.com
@TidalCyber
tryenterprise@tidalcyber.com
company/tidalcyber/