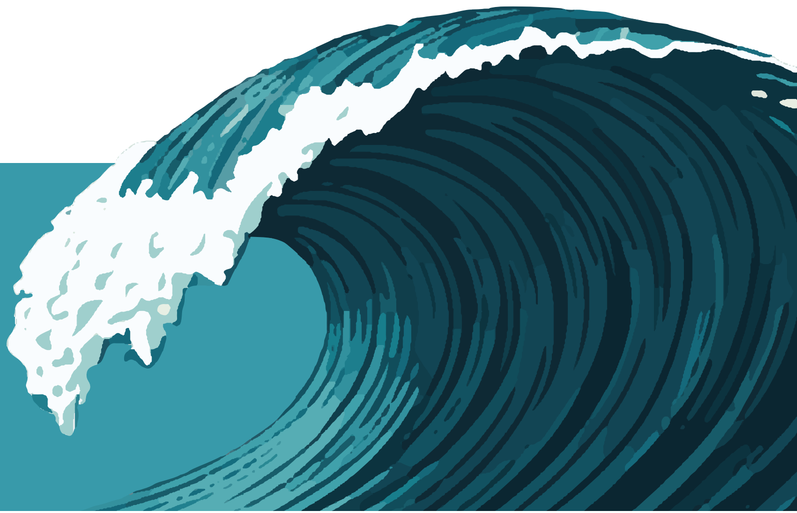
TIDAL CYBER

Case Study:

REDUCING SECURITY RISKS WITHOUT ADDITIONAL SECURITY INFRASTRUCTURE INVESTMENTS



INDUSTRY	ANNUAL REVENUE	EMPLOYEES	LOCATIONS
Manufacturing	$950M	10,000	United States

THE CHALLENGE

A U.S.-based manufacturing company suffered **two security breaches in a single year**, exposing critical vulnerabilities in their cyber defense strategy.

With the average cost of a breach reaching **$4.88M per incident**—not including **brand damage and long-term credibility risks**—taking swift, strategic action was imperative.[1] Despite investing in endpoint detection and response (EDR) solutions, the organization l**acked visibility** into whether these tools effectively mitigated threats.

Security leaders wanted to assess their current **detection coverage**, validate whether their EDR solution was delivering on its promise, and ensure they were not leaving critical gaps in their defenses. Additionally, the company was evaluating potential investments in **upgrading their EDR platform** but needed data-driven insights to justify any further spending.

The key questions were:

- How well did their existing security stack protect against known threats?
- Would upgrading their EDR improve their security posture, or would additional tools be necessary?
- Could they reduce exposure without costly new investments?

The team previously struggled, taking **17 and 33 days** to assess each threat, including evaluating tool efficacy against the identified threat techniques, finding configuration coverage gaps, and developing mitigation strategies.

This would take **136 to 264 person hours**, and between **$11,424 to $22,176** per threat (at an $84/hour fully loaded rate). Across 50 relevant threats based on this Manufacturers profile, each assessment cycle was estimated to consume **3.6 to 7.0** full time security analysts, resources the organization didn't have to dedicate to this task, inflating risks, and a key contributor as to why the organization had experienced recent security breach issues.

[1] Ponemon / IBM - https://www.ibm.com/reports/data-breach

> *We couldn't afford another breach, but lacked the skilled resources and time to identify priority threats, close gaps, and mitigate risks. Tidal Cyber gave us the visibility, prioritized action plan, and efficiency we needed to reduce security exposure and ensure success—with the resources we already had.*
> – CISO

THE SOLUTION

Tidal Cyber for EDR Coverage Analysis

The company integrated their EDR solution with **Tidal Cyber**, allowing them to instantly evaluate their **actual detection coverage** and identify areas for improvement.

Within moments of deployment, Tidal Cyber provided:

- A **comprehensive assessment** of their security stack's ability to detect and respond to relevant threats.
- **Visibility into coverage gaps**, highlighting potential weaknesses in their current setup.
- A **prioritized list** of **42 specific opportunities** to improve detection effectiveness—without requiring additional security investments.

With Tidal Cyber's automated mapping to MITRE ATT&CK, the manufacturing company gained real-time insights into which adversary tactics, techniques, and procedures (TTPs) their EDR could detect and where they had blind spots.

THE OUTCOME

Strengthened Security Without Additional Investment

By leveraging **Tidal Cyber**, the manufacturer quickly identified threat vulnerabilities and techniques that needed to be addressed to close gaps in the existing security posture.

What previously required **17 to 33 days** of manual effort for every identified threat was streamlined with Tidal Cyber automation, reducing time-to-action by **two-thirds**—from **as much as a month** to **less than a week**. The biggest benefit: empowering the team to go beyond merely assessing a subset of priority threats to now getting a continuous, thorough understanding of all the threats the team should be addressing - both key threats today and emerging threats in the future.

Across **50** threats, what would have taken from **3.6 to 7.0** full time security analysts to organize, synthesize and operationalize—resources the company did not have available— was automated with Tidal Cyber, delivering the equivalent of **$380K to $731K** boosted productivity value annually.

Moreover, the team was able to rapidly **reduce security risk exposure** without costly new tool investments. Instead of blindly upgrading their EDR or purchasing additional solutions, the security team optimized their existing security stack, achieving:

Closed Detection Gaps

Strengthened EDR effectiveness by addressing **42** critical coverage opportunities.

Maximized Security ROI

Enhanced defenses without additional investments in new tools.

Reduced Breach Risk

Improved detection and response, minimizing future security incidents.

By adopting a data-driven, automated threat informed defense approach with Tidal Cyber, the manufacturer gained full visibility into their security coverage, allowing their existing team with existing security solutions, to proactively detect, prevent, and mitigate threats before they could escalate into costly breaches.

> *Tidal Cyber gave us instant visibility into what our EDR was actually protecting us against. Instead of spending more, we optimized what we already had—reducing our exposure without needing additional investments.*
> – Security Operations Lead