TIDAL CYBER®

THREAT-INFORMED DEFENSE

A NEW WAY TO OPERATIONALIZE ENTERPRISE CYBERSECURITY

For decades, cybersecurity efforts have primarily focused on identifying and patching vulnerabilities—flaws in the software we rely on that adversaries exploit to launch attacks.

While addressing critical vulnerabilities is essential, the relentless pace at which new ones emerge makes it nearly impossible for even the most well-resourced organizations to keep every system fully patched.

IN FACT ...

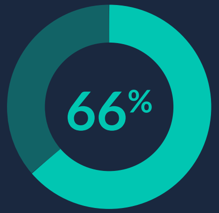
36% say that their cybersecurity team is in constant firefighting mode, spending most of their time addressing high priority or emergency issues, creating a self-perpetuating cycle where nothing ever improves, leading to employee burnout and high attrition rates. (TechTarget / ESG)

62% of security leaders are indicating challenges in aligning resources to respond effectively to priority threats. (Accenture)

78% of organizations reported being breached at least once in the past year, up from **63%** two years prior. In fact, **22%** of organizations reported being breached **6-10 times** in the past year, up from **9%** the previous year. (Ponemon)

2x

Threat volumes are expected to almost double over the next year, with **nearly 80%** of observed threat groups operating and **over 40%** of observed malware had never been seen previously. (McKinsey)



The time spent by Cyber Threat Intelligence Analysts manually collecting data and researching threats, leaving only 33% for actionable response, while a complete threat analysis would require 166%+ more time than currently available. (Genius Drive)

With threat volumes accelerating and breaches continuing unabated, one thing is clear: a **vulnerability-centric** approach to cybersecurity is no longer enough.

To stay ahead of evolving threats, you need a more comprehensive and proactive defense strategy.

RETHINKING CYBERSECURITY: BEYOND VULNERABILITIES TO ADVERSARY BEHAVIOR

Over the past decade, a growing community of cybersecurity practitioners has shifted its focus beyond just exploitable vulnerabilities. Instead, they analyze how cyber adversaries operate, studying the full spectrum of tactics, techniques, and procedures (TTPs) that attackers use to achieve their objectives.

A driving force behind this shift is MITRE and its freely available ATT&CK® knowledge base—a comprehensive encyclopedia of adversary TTPs mapped to known threat actors based on open-source intelligence. Unlike traditional vulnerability management frameworks, ATT&CK highlights how adversaries operate after gaining access, providing defenders with critical insights into real-world attack behaviors.

A common misconception is that cybersecurity revolves solely around patching vulnerabilities. However, most publicly reported TTPs in ATT&CK remain effective even in fully patched environments. This can be difficult to accept, but the reason is straightforward: once an attacker gains initial access—whether through phishing, a compromised website, or another entry point—they become unauthorized users of your systems.

At this stage, adversaries employ “living off the land” techniques, leveraging built-in tools, legitimate credentials, and existing system connections to blend in with normal operations. While employees might use remote administration tools for troubleshooting or cloud storage for collaboration, attackers exploit the same resources to move laterally, exfiltrate data, or establish persistence—all without relying on software vulnerabilities.

A significant majority of business leaders (**86%**) and cybersecurity leaders (**93%**) believe a catastrophic cyber event is likely to occur within the next two years. (World Economic Forum’s Global Cybersecurity Outlook)

$9.36 million the average data breach cost for US organizations, the highest regional cost per breach.(Ponemon)

The key takeaway: Skilled adversaries weaponize what they find within your environment. As a result, organizations must move beyond a vulnerability-centric mindset and adopt behavior-driven defense strategies to reduce risks and better defend against cybersecurity attacks.

WHAT IS "THREAT-INFORMED DEFENSE"?

Threat-Informed Defense is the systematic application of adversary tradecraft knowledge to assess, organize, and enhance security defenses. In simpler terms, it means using known adversary Tactics, Techniques, and Procedures (TTPs) as a lens to evaluate and strengthen your cybersecurity posture.

By shifting perspective and viewing your enterprise through the eyes of an adversary, you gain critical insights into how attackers could exploit your systems—allowing you to prioritize security operations and investments more effectively. This approach helps uncover how a skilled adversary might leverage your existing infrastructure and resources against you, enabling a more strategic defense.

Since Threat-Informed Defense relies on a deep understanding of adversary behavior, the MITRE ATT&CK® knowledge base plays a foundational role, providing a standardized way to describe and track TTPs. However, Threat-Informed Defense extends well beyond ATT&CK, as its true value lies in connecting adversary TTPs with the broader security context of your enterprise. This includes:

- Threat groups actively targeting your industry
- The current state of your defensive capabilities
- Testing-based confidence in your security controls
- Known vulnerabilities that enable high-risk adversary TTPs

Ultimately, Threat Informed Defense is about making meaningful connections between relevant adversary behaviors and the defenses designed to stop—or at least detect—them.

By embedding adversary insights into security strategy, organizations can shift from reactive, vulnerability-driven approaches to proactive, behavior-driven defense.

MINDING THE GAP(S)

Understanding adversary tactics, techniques, and procedures (TTPs) through a Threat-Informed Defense approach enables security teams like yours to gain critical insights into their enterprise's security posture. By using known adversary behaviors as a foundation for analysis, you and your team can more effectively identify meaningful gaps in their defenses—going beyond conventional compliance-driven approaches.

Since adversaries use a relatively small and well-documented set of TTPs, your security teams can map these behaviors against existing security frameworks such as:

- U.S. NIST Cyber Security Framework,
- The Center for Internet Security's 18 Critical Controls
- The U.S. Department of Defense's CMMC,
- Protection, detection, and response capabilities provided by your own cybersecurity tools.

A key advantage of this threat-informed approach is the ability to establish clear benchmarks for evaluating defenses. With a precise understanding of the adversary TTPs most relevant to your organization, your security teams can then systematically assess whether deployed controls can prevent, detect, or respond to these threats.

To maintain security effectiveness over time, continuous testing programs should be implemented that verify whether defenses remain operational and effective: ensuring that adversaries do not exploit unaddressed gaps.

Barely half of all organizations currently have the risk metrics they need to understand, track and prioritize cyber threats (PwC)

24% say that their organization doesn't have the tools and processes to operationalize threat intelligence today, making it difficult to understand priority cyber-adversary tactics, techniques, and procedures (TTPs). (TechTarget / ESG)

47% of attacks were missed in a 12-month period due to a lack of visibility or context from current security tools. (Deloitte)

WASHING YOUR HANDS

While Threat-Informed Defense significantly enhances an organization's cybersecurity posture, it is not a substitute for good cyber hygiene. Organizations must continue to prioritize fundamental security practices, including:

- Asset identification and management
- Secure configuration and change management
- Patching known vulnerabilities

Threat-Informed Defense does not replace these foundational cybersecurity activities—rather, it provides a powerful framework to assess, prioritize, and measure their effectiveness. By applying Threat-Informed Defense systematically, organizations gain greater visibility into the strengths and weaknesses of their defenses and can develop a clear, data-driven roadmap for continuous security improvement.

Organizations still need to identify their assets, manage their configurations, and patch exploitable vulnerabilities in their systems. Threat-informed defense doesn't obviate the need for those foundational activities, but it does provide a critically important means to assess, prioritize, and measure the effectiveness of them.

Threat-Informed Defense, applied systematically within an enterprise, can significantly increase visibility into the effectiveness of the currently deployed defenses and provides a clear roadmap for improving those defenses over time.

TIDAL CYBER AND THREAT-INFORMED DEFENSE

The three co-founders of Tidal Cyber, Frank Duff, Rick Gordon, and Richard Struse, were all working at MITRE, advancing ATT&CK and Threat-Informed Defense when they left to launch Tidal Cyber at the beginning of 2022. They formed the company for one simple reason—a strongly-held belief that defenders need and deserve tools and services that make achieving the benefits of Threat-Informed Defense practical and sustainable and easy to operationalize without adding more complexity to existing defenses.

Tidal Cyber's mission is to make it practical and cost-effective for all enterprises to adopt Threat-Informed Defense and quickly enjoy its benefits. We believe that these tools and services should be independent of any specific vendor's security product or capability. That independence helps ensure that our enterprise customers always understand what is best for them, and that our solution provider customers are positioned to deliver success.

TIDAL CYBER COMMUNITY EDITION

Befitting a company founded by three individuals who had worked to democratize access to Threat-Informed Defense, our first release was the Community Edition platform, launched in August of 2022. Still freely available to all, Community Edition provides a comprehensive knowledge base of both adversaries and their TTPs aligned with ATT&CK. In addition to adversary TTPs, the Tidal Cyber Registry, which includes mappings to hundreds of other security tools, goes beyond ATT&CK by making it easy for users to understand how specific security products (commercial and open source) align with adversary TTPs.

With more than 3,000 users worldwide and growing rapidly, Community Edition is an important resource for cybersecurity practitioners looking for the most up-to-date information on adversaries, their TTPs, and the tools that can defend against them.

However, we wanted to also offer something beyond Community Edition to truly help enterprises advance their day-to-day security operation.

<15% of organizations today are highly successful in gaining improved insights for making informed decisions, being fully prepared for future cyber incidents, and making data-driven choices that balance risk and revenue. (PwC)

TIDAL CYBER ENTERPRISE EDITION

As powerful as Community Edition is, most enterprises need more than a knowledge base to effectively implement Threat-Informed Defense. That's why Tidal Cyber developed Enterprise Edition, a Software-as-a-Service (SaaS) platform designed from the ground up to do just that. Launched in April 2023, Enterprise Edition is now used by customers on three continents, including some of the largest and most sophisticated financial institutions, insurers, healthcare, pharmaceutical, manufacturing, and technology companies.

Enterprise Edition gives our customers continually updated visibility into the security coverage provided by their existing security tools against the threats of concern to the organization.

20% Reduction in the risk of a security breach (Genius Drive)

TWO KINDS OF INTELLIGENCE

The Enterprise Edition platform was designed to seamlessly integrate two types of intelligence necessary to determine the effectiveness of an organization's cyber defenses. The first type of intelligence is Cyber Threat Intelligence, or "CTI," which focuses on cyber adversaries and the TTPs that they use. Enterprise Edition customers benefit from the work of Tidal's CTI team, which continually curates new, high-confidence open-source threat intelligence published by government agencies and leading cybersecurity researchers and vendors. Our customers can then add their own threat intel on top of that, including CTI from Threat Intelligence Platforms (TIPs), commercial threat feeds, and other sources.

Of particular interest to those customers with limited or no CTI resources in-house, Tidal identifies the threats of concern to an organization, based on industry sector, geography, and/or technology platforms in use and rapidly keeps that up to date as the threat landscape evolves.

The second type of intelligence provided by Tidal is Cyber Defense Intelligence, or CDI, which focuses on the specific capabilities of security tools and products. Tidal has led the industry in the development of this new type of intelligence, working with security tools and their vendors/creators to catalog the capabilities of tools against specific adversary TTPs as defined in ATT&CK.

This is at the heart of Enterprise Edition's ability to show our customers how their existing defenses align with the threats of concern at the TTP level. The time and effort this saves security teams is enormous, meaning that they can better focus on understanding and improving their security.

53% of respondents cite a lack of necessary expertise as a current disadvantage in achieving a strong cybersecurity posture. (Ponemon)

MAPPING YOUR COVERAGE

Enterprise Edition is continually aligning the threats of concern to an organization to its current defenses and showing our customers how well-defended they are against each adversary TTP. We call this process Coverage Mapping, and it gives Enterprise Edition users a clear understanding of where their defenses are strong and where they are weak. The platform computes a score associated with each adversary TTP of concern and makes it easy for users to understand where to prioritize their efforts to improve their coverage. Color-codes assigned to score ranges allow at-a-glance understanding of strengths and weaknesses in your defenses (see Figure 1).

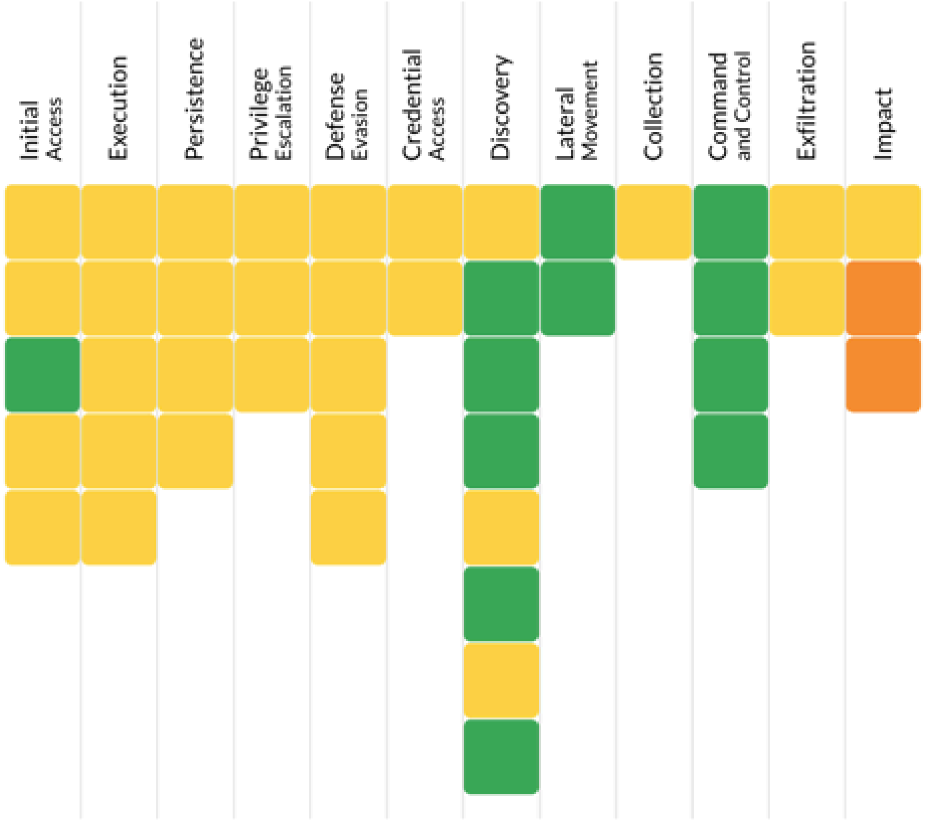


Figure 1: High-level view of a simple coverage map

>50% Over ½ of organizations currently lack confidence that their cyber budget is:

- Allocated towards the most significant risks to the organization
- Focused on remediation, risk mitigation, and/or response techniques that will provide the best return on cyber spending
- Includes monitoring the effectiveness of our cyber program against cybersecurity spending. (PwC)

Another notable aspect of Enterprise Edition is its ability to monitor for changes in both the threat and defensive environment and automatically recalculate all impacted coverage maps. This ensures that security teams always have the most up-to-date view of their security coverage without requiring team members to manually update the system.

In addition to showing users where their defenses aren't up to the task, Enterprise Edition automatically makes specific recommendations for how organizations can improve their coverage, starting with the tools they already own. This helps ensure that our customers are getting all the value possible from existing security tooling – maximizing their return on investment (ROI) from those products and very quickly improving their coverage.

30% say that their organization has recently added new network/ cloud-based hosts, applications, and users, making it difficult for the cybersecurity team to keep up with the scale of the infrastructure and assure coverage. As well, 30% say there are one or several "blind spots" on their networks. (TechTarget / ESG)

KEY BENEFITS

Some of the key benefits to customers using Tidal Cyber Enterprise Edition include:

Identify and close important security gaps

The faster your organization can identify and close the key gaps in their defenses, the less likely adversaries will find and exploit those gaps. This, however, isn't a one-time exercise as the threat environment is evolving on a constant basis and cyber defenses change as organizations change.

Unfortunately, **26%** say that threat detection and response is anchored by manual processes that hinder their ability to keep up. (TechTarget / ESG)

Tidal Cyber's ability to track these changes and update your coverage maps in real time helps ensure that your prioritizing what really matters and leveraging resources where they are needed most, so that your enterprise stays more secure over time.

Make security teams more efficient and effective

Security teams are often under-staffed and under-resourced, making it difficult to keep pace with an ever-changing threat and defensive environment. In fact, **62%** of security leaders are indicate challenges in aligning resources to respond effectively to priority threats. (Accenture)

Tidal Cyber's Enterprise Edition automates many of the tasks required to maintain accurate visibility into your security coverage, saving you and your team valuable time and allowing them to do more with the team they have today.

In addition, many security tools increase the burden on already stretched security teams. Tidal's approach ensures that your team has the visibility and insights they need without a lot of extra effort, making the entire security operation more effective with reduced investment.

65% Boost in Cybersecurity Threat Intelligence (CTI) and Security Operations Center (SOC) Manager capabilities and productivity. (Genius Drive)

Get the most out of existing tools

Today's organizations devote substantial resources to acquire and maintain what is often a large set of security tools. In fact, the typical organization has over **76** security tools, a **19%** increase over the past two years (Deloitte)

Understanding how each tool uniquely addresses threats of concern is a full-time job. Understanding how each tool should be optimally configured across the enterprise to maximize impact against key threats compounds that burden to unsustainable levels of effort.

Tidal's Registry and Enterprise Edition enhance cybersecurity by mapping to and integrating with key security tools, ensuring organizations maximize their defensive capabilities. This integration streamlines workflows and prioritization, reducing time wasted on low-value tasks while providing data-driven insights that improve threat coverage and minimize security gaps. With clear coverage maps and prioritized action plans, security teams can accelerate mitigation efforts and strengthen overall resilience against cyber threats.

5% to 10% Reduction in redundancies with security tool investments (Genius Drive)

Save money

It's no secret that security budgets are under significant pressure in the current environment. And no wonder why with a hefty **13.2%** of the total IT budget currently being spent on security, up from just **8.6%** in 2020. (National CIO Review)

It's been highly recommended, especially with security consolidation driving costs up vs. down, that teams start with assessing what protections they already have and how they are used – to get the most of what's already in place.

Tidal's unique insights into the value that each security tool provides across the enterprise is key to identifying potential opportunities for tool rationalization and resulting cost savings without exposing your organization to undue risk.

45% Optimization in Security Architect and Engineer efficiency and effectiveness. (Genius Drive)

Improve communication to stakeholders

One under-appreciated aspect of the role of security teams and security leadership is how much communication with other stakeholders is required. And with **49%** of CEOs viewing cyber risk as the number one threat to their business growth in the next 12 months the ability to accurately communicate posture and risks is essential. (PwC)

Enterprise Edition uniquely captures the evolution of both the threat landscape as well as the changes made to the defensive environment in response to those threats, making it easy to communicate the value your security teams are delivering.

For organizations that create separate coverage maps to cover different parts of their environment or track different threats, our Coverage Map Rollup feature provides a single confidence score. With this, you can assign the weight to each coverage map based on the relative impact of a compromise to the environment that coverage map represents.

What used to be a once-a-year herculean lift to assess threat risks, report on issues and document compliance, can now be a continuous reporting process, with elevated results, complete traceability and improved transparency.

Data-driven reporting and global coverage scores resonate particularly well with your executive and board stakeholders and allow your security and compliance teams to spend their precious time improving security instead of creating ever-more PowerPoints to explain what you are doing.

Use

Use Cases for Threat-Informed Defense

Organizations rely on **Tidal Cyber** to streamline operations, maximize the value of existing defenses, and enhance team efficiency—delivering both time and cost savings while strengthening overall security and reducing risks.

- **Threat Research and Profiling:** Managing cyber threat intelligence (CTI) is a challenge for analysts who struggle to identify, prioritize, and map threats within frameworks like MITRE ATT&CK. As adversary tactics evolve, teams risk wasting time on manual research instead of focusing on strategic action.

  Tidal Cyber automates threat intelligence workflows, continuously updating threat data and prioritizing behaviors based on real-time adversary activity and organizational risk. This ensures CTI teams can focus on the most relevant threats and maintain an up-to-date defense strategy.

  By streamlining intelligence collection, Tidal reduces the time you need to identify attack vectors from hours to minutes. The platform maps threat behaviors, provides clear dashboards, and aligns your security teams using MITRE ATT&CK, ensuring more efficient and effective defense strategies.

- **Defensive Stack Optimization:** Security teams like yours struggle to manage tool sprawl, eliminate redundancies, and optimize security investments. Many lack visibility into tool capabilities, leading to inefficiencies and underutilized defenses.

  Tidal Cyber optimizes your defensive stacks by mapping security tools against sector-specific threat profiles, identifying gaps, and providing actionable recommendations to maximize efficiency. The platform helps you eliminate redundancies, improves resource allocation, and ensures alignment with real-world threats.

  By automating tool evaluation, reducing overlap, and enhancing visibility, Tidal Cyber streamlines your operations and ensures your security tools deliver maximum value—helping your organization cut costs while strengthening defenses.

- **SOC Assessment:** SOC managers often struggle with limited visibility, fragmented intelligence, and inefficient risk prioritization, making it difficult to balance immediate threats and long-term adversary trends.

  Tidal Cyber provides a unified, real-time view of threat coverage, allowing your SOC leaders to quickly assess security gaps, optimize defenses, and improve cross-team coordination. The platform dynamically maps threats to existing controls, helping your SOC teams pinpoint weaknesses and eliminate inefficiencies.By automating coverage mapping and enabling data-driven prioritization, Tidal Cyber helps your SOC managers respond swiftly to emerging threats, ensuring a more proactive and effective defense posture.

- **Security Engineering:** Security architects and engineers commonly struggle with threat prioritization, team coordination, and resource optimization. Without a unified, data-driven approach, your security teams face fragmented workflows, inefficient remediation efforts, and misaligned tool configurations, leaving critical risks unaddressed.

- Tidal Cyber enhances your security engineering by streamlining threat prioritization, optimizing tool usage, and improving coordination across teams. The platform maps security gaps, aligns defenses with evolving threats, and delivers actionable insights, ensuring your teams focus on high-priority risks while minimizing wasted effort. Automated remediation guidance, coverage mapping, and false positive filtering further reduce inefficiencies and accelerate your response times.

- By aligning defenses with active threat profiles, enhancing collaboration between CTI, Blue, and Red Teams, and providing real-time visibility into security gaps, Tidal Cyber enables your security engineers to work smarter, maximize efficiency, and continuously strengthen defenses.

- **Threat Hunting Prioritization:** Threat hunters often struggle to prioritize efforts, convey their impact, and ensure hunts yield actionable results. Without structured prioritization, hunts can be inefficient, misaligned, or fail to detect critical threats.

- Tidal Cyber prioritizes hunts using threat profiles and coverage maps, ensuring focus on high-impact threats while providing automated recommendations and structured hunt tracking. This allows your teams to reduce preparation time and increase efficiency.

- By automating hunt recording, integrating risk dashboards, and converting results into detection rules, Tidal Cyber enhances your hunt effectiveness, improves visibility, and strengthens organizational security.

- **Red Team Test Analysis:** Red and Purple Teams often struggle with prioritizing simulated attacks, optimizing testing efficiency, and translating results into actionable improvements. Many rely on intuition rather than data-driven prioritization, leading to resource misallocation and unclear test impact.

- Tidal Cyber prioritizes tests using threat profiles and coverage maps, ensuring your teams focus on critical security gaps. The platform provides real-time threat mapping, confidence scoring, and integration with Breach and Attack Simulation (BAS) tools, refining test selection and resource allocation.

  By automating test result analysis, strengthening stakeholder communication, and improving reporting, Tidal Cyber maximizes your efficiency, improves security validation, and enhances your Red/Purple Team effectiveness.

- **Detection Coverage Measurement:** Detection engineers face challenges in tracking detection lifecycles, prioritizing new detections, and managing vendor-provided capabilities. Many rely on intuition instead of a structured, data-driven approach, leading to misaligned priorities and redundant efforts.

  Tidal Cyber streamlines your detection engineering by leveraging coverage maps to prioritize efforts, track vendor contributions, and validate detection effectiveness. The platform integrates threat intelligence with real-world attack simulations, ensuring detections align with evolving threats.

  By automating detection cataloging, improving visibility, and enabling continuous updates, Tidal Cyber helps your engineers focus on high-priority detections, minimize wasted effort, and optimize security investments.

  GRC Control Assessment: GRC teams struggle with manual compliance processes, fragmented reporting, and difficulty mapping security controls to real-world threats. Ensuring compliance while addressing security risks is often time-consuming and inefficient.

  Tidal Cyber automates your GRC processes by aligning compliance frameworks with security controls, allowing teams to map threats to technical implementations, track compliance status, and respond efficiently to audits.

  By automating reporting, streamlining risk assessments, and improving compliance accuracy, Tidal Cyber reduces your audit burdens, strengthens regulatory alignment, and enhances security resilience.

- **Security and Compliance Risk Reduction:** Organizations face challenges in maintaining strong security defenses while keeping pace with evolving compliance requirements. Poor visibility into attack vectors, rising cyber risks, and regulatory pressures increase financial and operational exposure.

  Tidal Cyber reduces your security and compliance risks by mapping security controls to real-world threats, allowing teams to identify coverage gaps, mitigate breach risks, and align security efforts with compliance mandates.

  By automating risk assessments, streamlining compliance efforts, and improving response strategies, Tidal Cyber lowers your potential breach costs, reduces regulatory penalties, and enhances overall security resilience.

TIDAL CYBER®

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

GETTING STARTED WITH ENTERPRISE EDITION

Deploying Tidal Cyber Enterprise Edition is a straightforward and efficient process, designed to integrate seamlessly into your existing security environment. The platform sits above your defensive stack, providing holistic visibility into security tool performance without requiring direct access to your environment.

Because Tidal is agentless and sensor less, there's no need to install software on endpoints or monitor network traffic. This eliminates operational disruptions, speeds up deployment, and ensures privacy by avoiding access to sensitive data such as PII, PHI, or other non-security-related information. Additionally, each customer operates in a completely isolated cloud tenant, streamlining any third-party risk assessments required before deployment.

Whether you have a small security team looking to level up or a large, globally distributed team needing comprehensive visibility, Tidal Cyber Enterprise Edition delivers immediate value from day one. Our dedicated Customer Experience (CX) team supports you not only during onboarding but throughout your entire journey, ensuring you maximize the platform's benefits as your security needs evolve.

THE BOTTOM-LINE

As cyber threats evolve, enterprises need a proactive approach to security that goes beyond traditional vulnerability management. Threat-Informed Defense helps you deliver unprecedented visibility and actionability into your organization's cybersecurity posture.

Tidal Cyber Enterprise Edition makes this approach practical by automating security coverage assessments, integrating adversary insights, and providing real-time visibility into defensive gaps. By mapping existing security tools to known threats, it helps you and your organization strengthen their security posture, improve efficiency, and ensure defenses stay aligned with emerging risks.

Tidal Cyber makes the promise of Threat-Informed Defense a reality