TIDAL CYBER

# Case Study:

## ACCELERATED THREAT INTELLIGENCE MATURITY BY 2 YEARS

| INDUSTRY | ANNUAL REVENUE | EMPLOYEES | LOCATIONS |
|---|---|---|---|
| Insurance | $750 billion | 55,000 | Global |

### CHALLENGES

- Fragmented and Overwhelming Threat Intelligence
- Lack of Context and Prioritization for Threats
- Inefficient Workflows and Resource Constraints

### TIDAL CYBER SOLUTION

- Threat Research, Profiling, and Prioritization

### OUTCOME

**2 YEARS** of Threat Intelligence Maturity Gained

**65%** Multi-Week Investigations Reduced

**3x** Time Savings Leading to 3x Productivity Boost

### THE CHALLENGE

A global insurance leader faced a major gap in its ability to operationalize threat intelligence.

A recently hired junior threat analyst was tasked with establishing a threat-informed defense program based on MITRE ATT&CK®. Despite best efforts, the analyst struggled due to:

- **Fragmented Threat Intelligence:** Intelligence sources were disjointed, making it difficult to prioritize threats effectively.
- **Unmanageable Threat Volumes:** The organization lacked a systematic way to analyze and categorize emerging threats at scale.
- **Lack of Threat Context:** The analyst received only indicators of compromise (IOCs) without deeper insight into adversary behaviors.
- **No Clear Prioritization:** Threats were addressed reactively rather than proactively, delaying response times and increasing exposure to critical risks.

And no wonder, as typical analysts spend **66%** of their time 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.

With threat volumes anticipated to **double** over the next year, and over **40%** of observed malware having never been previously seen, the insurer needed a modern, structured approach to threat intelligence—one that could enable security teams to anticipate, prioritize, and proactively defend against adversaries rather than chasing the latest attack.[1]

1. McKinsey https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

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

## THE SOLUTION

Tidal Cyber provided a centralized, structured approach to threat research, profiling, and prioritization, transforming and elevating the insurer's security operations.

This resulted in the insurance firm being able to:

- **Take Minutes vs. Weeks for Threat Assessments:** The analyst could now evaluate threats in real time instead of conducting weeks-long investigations.
- **Obtain Tidal Cyber-Curated Threat Intel:** By leveraging curated, enriched threat intelligence, the insurer gained a comprehensive view of adversary behaviors—going beyond IOCs to understand the full scope of threats.
- **Automate Prioritization:** Tidal Cyber enabled the organization to prioritize threats based on behavior and contextual relevance, ensuring that security teams focused on the most pressing risks.
- **Structure Threat Research:** The insurer gained a single source of truth, mapping threats directly to MITRE ATT&CK with enriched metadata, saving analysts time and effort.
- **Elevate Confidence in Risk Assessments:** The organization implemented a tailored Tidal Cyber confidence score, allowing for rapid evaluation of each new threat and ensuring security controls were aligned with evolving risks.

**Every day, the team leveraged Tidal Cyber to help the insurance firm with:**

- **Consolidated Threat Intelligence:** Tidal Cyber helped the insurance firm aggregate intelligence from open-source, third-party, and internal sources into a unified platform.
- **Real-Time Threat Prioritization:** Threats were automatically ranked by Tidal Cyber based on relevance to the organization's attack surface and known adversary behaviors.
- **Rapid Defense Validation:** With quantified risk metrics, the insurance firms' security teams leveraged Tidal Cyber to better assess exposure to emerging threats and proactively reinforce defenses before attacks materialized.
- **Actionable Insights for Defense Teams:** CTI analysts leveraged Tidal Cyber insights to proactively guide detection engineers, ensuring security operations focused on defending against high-priority threats rather than reacting to every new attack.

## THE OUTCOME

Thanks to Tidal Cyber, the insurance leader achieved in months what would have taken years using traditional threat intelligence methods.

Benefits included:

- **2 Years of Threat Intelligence Maturity Gained:** The insurer's CTI program accelerated its development timeline by two years, significantly increasing cyber resilience.
- **Multi-Week Investigations Reduced to Minutes:** The analyst could quickly assess threats and prioritize responses with confidence, freeing time for more strategic defense improvements.
- **Consistent Threat Profiling:** Instead of constantly pivoting to the threat du jour, security teams now focus on a structured, long-term approach to threat-informed defense.
- **Proactive Security Posture:** The insurance organization improved overall cyber defense readiness, allowing teams to reinforce protections against threats before they materialized.

With Tidal Cyber threat intelligence, the analyst can handle three times the **workload** compared to before, a force multiplier needed to achieve maturity and improve security posture.

With cyber threats increasing and adversaries growing more sophisticated, large enterprises like this insurance firm can no longer afford fragmented, inefficient threat intelligence processes.

By adopting Tidal Cyber's structured, intelligence-driven approach, the insurance leader not only transformed its threat intelligence but also demonstrated the CTI team's strategic value—showing that proactive, data-driven threat defense directly improves enterprise security posture and continuous risk management.

With Tidal Cyber, enterprise security teams are no longer playing catch-up. They're staying ahead.

> *We were able to leverage Tidal Cyber to accelerate our early-stage threat program maturity by two years!* – Threat Analyst