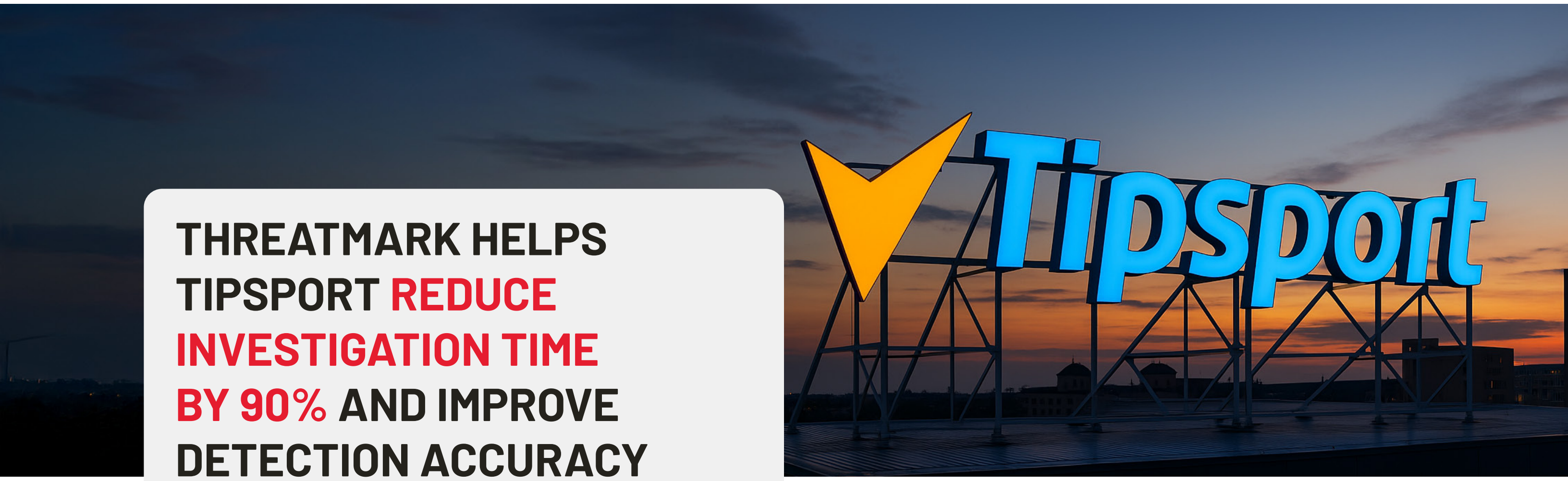

THREATMARK HELPS TIPSPORT REDUCE INVESTIGATION TIME BY 90% AND IMPROVE DETECTION ACCURACY

Tipsport, a leader in the Central European gaming market, serving over a million active users internationally, partnered with ThreatMark to stay ahead of evolving fraud threats and ensure a secure, seamless user experience. By implementing ThreatMark's Behavioral Intelligence Platform, Tipsport reduced investigation time by 90% and significantly improved the detection rate.

KEY CHALLENGES

Account takeover, bonus abuse, account sharing, BOT activity

THE GAME HAS CHANGED

Founded in 1991, Tipsport has grown from a traditional retail bookmaker into a technology-driven company offering a broad portfolio of sports betting, live betting, and online gaming services. As its digital footprint expanded, so did the sophistication of fraud threats.

Tipsport faced increasingly complex fraud vectors, including account sharing, bonus abuse, and automated bot attacks. These threats were often part of coordinated fraud rings using social engineering and scripted automation to evade traditional controls. The situation was further complicated by users frequently sharing accounts, often for fraudulent purposes.

Managing hundreds of detections daily across multiple applications revealed the need for a more structured approach and deeper understanding of fraud patterns. Investigations consumed significant internal resources, often delaying responses to emerging threats. At the same time, dedicated bots for automated betting placed wagers, allowing dishonest bettors to scale their fraudulent operations programmatically and scrape betting data for unfair advantage.

HOW DID TIPSPORT OVERCOME THESE CHALLENGES?

Tipsport implemented the ThreatMark Platform in mid-2024 across its international digital properties including Tipsport, Chance, Maxa, and Pluso. The rollout was swift and smooth, thanks to ThreatMark's streamlined implementation process and strong collaboration between teams.

"Despite its complexity and robustness, the implementation of the ThreatMark Platform was remarkably swift. It began delivering actionable intelligence almost immediately after the project kick-off, clearly demonstrating its value early on," says Petr Hustava, Information Security Manager at Tipsport.

The ThreatMark Platform provided a unified view of customer activity across applications and channels, enabling deep behavioral profiling and forensic context.

DRAMATIC IMPACT FOR TIPSPORT

The ThreatMark Platform quickly delivered beyond initial expectations, reducing investigation times, automating detection, and surfacing high-risk activity earlier in the fraud lifecycle.

Tipsport's anti-fraud team reduced fraud investigation time for complex fraud cases by 90%, from 5 hours to 30 minutes. The Mean Time to Detect (MTTD) dropped by nearly 98%, from 16 hours to 20 minutes. This efficiency boost allowed the team to shift from reactive investigation to proactive detection.

Detection accuracy improved across all major fraud vectors. Tipsport significantly increased its True Positive Rate (TPR) for ATO and bonus abuse scenarios while cutting the False Positive Rate (FPR) from 30% to 5%. Detection of sophisticated bots, used for scraping and automated betting, also improved, giving Tipsport a stronger ability to block programmatic abuse.

The ThreatMark Platform also enabled improved mapping of customer behavior across digital apps, platforms, and user journeys. By collecting consistent behavioral signals across Tipsport's ecosystem, the ThreatMark Platform helped accurately distinguish between legitimate and fraudulent activity without disrupting the user experience.

These improvements also translated into faster case resolution and better analyst confidence. With higher-quality alerts and fewer false positives, Tipsport's fraud team can spend less time on dead ends and more time taking decisive action. The result is not only increased efficiency, but also stronger protections for customers and the business.

WHAT'S AHEAD FOR TIPSPORT?

Operational efficiency improved across the board. The ThreatMark Platform helped identify connections between suspicious accounts, streamline team workflows, and unify behavioral data from across the Tipsport Group's six brands. As a result, Tipsport now saves an estimated 950 man-hours annually. Combined with the enhanced detection rate, it positions ThreatMark as a solution with a highly favorable Return on Investment (ROI).

"With the ThreatMark Platform, we have achieved a 10× faster investigation of complex incidents and drastically reduced detection time of sophisticated fraud from 16 hours to just 20 minutes," says Marek Havlín, Security Engineering Team Leader at Tipsport.

The collaboration also fosters an agile response model between Tipsport and ThreatMark. As new fraud patterns emerge, ThreatMark rapidly adapts detection logic and provides updates tailored to Tipsport's evolving risk landscape. This flexibility allows Tipsport to stay ahead of new threats without overhauling internal processes.

> *"The return on investment is unquestionably strong. We consider ThreatMark a strategic partner in our fight against fraud."*
>
> **MAREK HAVLIN**
> Security Engineering Team Leader
> at Tipsport

KEY RESULTS

90%
90% reduction of average incident investigation time

5%
5% false positive rate since implementing ThreatMark

x10
10× faster investigation of complex incidents

1K
Nearly 1,000 hours of manual incident review saved annually

LEARN MORE ABOUT THE THREATMARK PLATFORM