Recorded Future®

TBI Bank Outpaces Cyber Threats and Boosts Security Team Efficiency by 15% with Recorded Future

TBI Bank uses Recorded Future to centralize real-time threat intelligence, prioritize team resources, and reduce risk across its mobile banking platform.

tbi bank

Use Cases: Dark web investigation; Threat hunting (advanced detection & validation); Advanced threat research & reporting

Goal: Improve visibility into the most pressing cyber threats and enable better prioritization.

Challenge: Protect TBI's banking infrastructure and customers from emerging cyber threats.

Solution: The Recorded Future Intelligence Cloud:

- Threat Intelligence
- Darktrace integration

Outcomes:

- 15% efficiency boost across their security team
- Increased team capacity
- Reduced risk of financial and reputational harm
- Increased customer trust

At TBI Bank, a progressive consumer bank operating across three European countries, there's a strong emphasis on mobile banking. Their mission is to "provide the best service for customers in an easy way, and directly in their pockets," and securing their mobile apps and safeguarding against mobile-specific threats is a key priority. However, the responsibilities of Chief Information Security Officer (CISO) Dobrin Dobrev extend far beyond mobile security. It's on his shoulders to protect the bank's users while securing its entire infrastructure.

"Cyber risks are increasing exponentially," he said. "Threat actors are always trying to stay a step ahead of all the solutions and protections that institutions put in place."

Dobrev's goals are clear: stay ahead of the most relevant threats and focus on early detection and prevention.

An Urgent Need for Real-Time Threat Intelligence

Given the complex and evolving threat landscape, financial institutions must have up-to-date, real-time threat intelligence, but doing the necessary detective work was tough on TBI Bank's security team. Their analysts lacked a centralized source of truth for threat intelligence. Instead, they had to manually scan online forums, social media platforms, and various websites for information—a time-consuming process that sometimes left them questioning the timeliness and accuracy of their findings.

> **"Partnering with Recorded Future was a great decision for our team and an important milestone in our cybersecurity strategy."**
>
> *Dobrin Dobrev*
> *Chief Information Security Officer (CISO), TBI Bank*

"We were manually scrubbing the dark web and identifying malicious IP addresses, and it was really time-consuming work," Dobrev recalled. "It could take days to gather the necessary information and we weren't entirely sure how current it was. Threat actors are constantly evolving and making different aliases, so it could be really difficult to keep up."

TBI Bank needed a way to:

- obtain and centralize the most current threat intelligence
- prioritize the most significant risks for further investigation
- automate aspects of their threat response

Doing so would allow them to react faster and keep both the business and its customers secure.

TBI Bank evaluated several vendors and ultimately chose Recorded Future. "We identified that Recorded Feature provides the most valuable real-time information relevant to our region and financial sector," said Dobrev.

Gaining a Complete View of the Most Pressing Threats

TBI Bank depends on Recorded Future to gain a clearer and more comprehensive view of their global exposures. With Recorded Future, all the information they need is consolidated in one platform, saving analysts from having to manually identify threats and vulnerabilities.

Recorded Future aggregates data from a wide range of sources, including the dark web, hacker forums, and open sources, to deliver real-time threat indicators. These indicators include malicious IP addresses, domains, and other indicators of compromise. It also notifies TBI Bank of emerging threats that are relevant to them, such as new malware strains or phishing campaigns actively targeting the financial industry.

"We've seen a big improvement in the quality of information we're getting," said Dobrev.

Prioritizing the Right Areas to Investigate

The Recorded Future team proved helpful throughout the process—from the initial proof of concept to ongoing support. Leaning on their assistance and expertise, TBI Bank learned how the platform can help them prioritize threats and focus on the most critical and relevant ones. Recorded Future provides detailed context, including information on individual threat actors, their usual methods, and past behavior.

Recorded Future also assigns risk scores based on factors such as the threat actor's reputation and the number of sightings. This comprehensive approach helps Dobrev and his team determine which threats to investigate first, allowing them to allocate resources effectively and reduce overall risk.

Staying Ahead of Bad Actors

So much of cybersecurity is keeping an eye on trends, which was hard to do without complete visibility. Recorded Future provides the visibility the TBI team needs to stay on top of trends and become more proactive about security.

"With Recorded Future, we can track different threat actors, tactics, techniques, and procedures, all in one place. We follow specific groups and receive notifications when new information arises. If we didn't have this information, we'd identify it at a later stage, when the issue might have already become a more serious incident," Dobrev said.

Constant monitoring and rapid response are critical to the bank's success and security because they minimize exposure and prevent incidents from escalating, Dobrev continued. "Everything can start with something as small as a phishing email. If you don't catch it early, it can lead to full access to the environment. That's why early-stage monitoring is so crucial."

The Darktrace Integration Spurs Automation

One of Recorded Future's biggest benefits has been its integrations with TBI Bank's existing tools, including Darktrace. This integration allows TBI Bank to automate its response to known threats. If Darktrace detects a connection to a malicious IP address identified by Recorded Future, it automatically blocks that connection, with no manual intervention from TBI Bank's engineers.

"Recorded Future identifies suspicious activities, and we can immediately block the compromised machine or IP address through automation," Dobrev explained. "This is really the biggest impact for us, that we can launch a direct response in our environment, block it in the early stage, and minimize our exposure."

Through Recorded Future's integration with Darktrace, TBI Bank has full visibility into its entire threat landscape, improving their overall cyber posture.

Increasing Efficiency by 15%

With threat intelligence centralized and automated incident response in place, his analysts and engineers save significant time. Dobrev estimates the team's efficiency has increased by 15%.

This efficiency boost means they can reallocate resources to other critical projects without expanding the team. They're more proactive about threat hunting and vulnerability management, reducing the likelihood of incidents.

TBI Bank measures success not just in efficiency gains but also in the reduced risk of breaches and the associated cost avoidance. By improving threat detection and response times with Recorded Future, TBI Bank cuts the risk of successful cyber attacks, reducing the potential cost impact and increasing customer trust. Dobrev insists it can do the same for any other CISOs looking to become more efficient and enhance their security procedures.

"Partnering with Recorded Future was a great decision for our team and an important milestone in our cybersecurity strategy," Dobrev said.