ThreatMark SBERBANK

SUCCESS STORY

August 2020

ThreatMark's SOC Team Helps Sberbank Fight Online Fraud and Finetune Its Anti-fraud Landscape

ThreatMark helps the bank with building secured and threat-safe digital banking with a dedicated team of professionals from our Security Operation Center (SOC). Our analysts are working diligently around the clock to analyze, discover and identify new phishing sites & malware threats. They proactively help with specific cases and provide advisory guidance in fine-tuning our client's anti-fraud systems. In this success story, read how ThreatMark SOC team closely works with Sberbank to strengthen the bank's online banking fraud mitigation.

Sberbank in Czech Republic is the local branch of the biggest Russian bank which has 20,000 branches internationally, with over 260 thousand employees internationally. In Russia alone, 70 % of population uses Sberbank in 11 Regional Banks and 14,000 branches. The bank's international network is made up of subsidiaries, branches, and representative offices in 21 countries, including the Czech Republic.

ThreatMark was delighted by the Sberbank initiative to kick-start the cooperation and commitment to go beyond in trusting their customers and protecting their personal & business banking.

From the start of the cooperation in 2017, Sberbank insisted on innovation in solving the key challenges – unauthorized and fraudulent transactions. To tackle the challenge, they implemented ThreatMark's solution offering reliable & strong protection for their international customers, enhanced with consultation services from ThreatMark's Security Operation Center (SOC).

Introducing SOC

SOC is an essential component used by the majority of ThreatMark's customers. It allows each one of them to benefit from the proactive research & shared intelligence on cyber threats & malicious activities.

ThreatMark's SOC team relies on two distinct sources for their work. We call these on-page and off-page elements. On-page elements include anonymized data (such as unknown malicious code samples, phishing attempts, suspicious operations, device identifiers, and user behavioral patterns) which are collected from all deployments. Off-page elements include various proprietary methods in scanning and probing the internet for new threats & malicious activities. The data from both sources are pooled and thoroughly analyzed.

> *"We appreciate that your anti-fraud team let us look under the hood of hackers' work and keep our fraud analysts up to speed against new cyberthreats happening in the digital world."*

Klára Vítková, Senior Fraud Specialist
Sberbank Czech

This analytic work produces *signatures* – descriptions of bad actors modus operandi. After the initial analytic processing, signatures are then pushed to our centralized security knowledge center to ensure that all our client's instances are ready to face this kind of risk. It is important to note that the same process & methods apply for both old and new (never identified before, so called zero-day malware) threats. By combining both on-page and off-page dimensions, ThreatMark casts a wide probing net and is able to detect, promptly alert, and mitigate all cyber threats.

Consultancy & Workshop

Additionally, ThreatMark's SOC team is engaged in consultancy and educational activities for our clients. On the client's request, the team can organize and implement a workshop on the latest cyber threats and prevention methods. For Sberbank, our SOC team organized a 2-day workshop focused on new malware types for both internet and mobile banking channels. Training consisted of real-life examples and best practices when it comes to identification and mitigation of these threats.

The feedback ThreatMark team received from Sberbank attests to the necessity of timely education & raising security awareness activities. To quote Klára Vítková: '*After the three years that Sberbank works with ThreatMark, we appreciate that your anti-fraud team let us look under the hood of hackers' work and keep our fraud analysts up to speed against new cyberthreats happening in the digital world. We consider ThreatMark's team to be full of experts in the field, and Sberbank's team is delighted to have them on board.*'

Conclusion

The proper way to secure any online system resides in both technological and human elements. Just as bad actors use technology to exploit the human side; the solution needs to cover both to adequately work. ThreatMark's complete anti-fraud solution – ThreatMark AFS – covers both dimensions within a broader, trust-first cybersecurity suite. ThreatMark AFS is a modular & feature-rich banking fraud prevention that detects cyber threats, validates user identity through behavioral biometrics and detects payment fraud using machine learning and business rules in real-time. This success story shows how ThreatMark's SOC keeps Sberbank ahead of the threats with its multi-channeled data collection methods. And beyond technology, the SOC team helps mitigate the risks & threats with the human side as well – by empowering Sberbanks's personnel so they can actively educate, engage & protect their users and their most precious assets.

ThreatMark s.r.o.

Hlinky 505/118,
603 00 Brno,
Czech Republic

IČ: 04222091, DIČ: CZ04222091

Contact us at:
info@threatmark.com