SOC Services

Complementing technology with cybersecurity expertise

ThreatMark's Security Operations Center (SOC) team is comprised of cybersecurity professionals who complement our technological solutions in detecting, preventing & mitigating online fraud.

The main role of ThreatMark's SOC team is to vigilantly discover and mitigate threats that endanger our client's security & the financial industry in general.

Keeping up with the latest trends and scammers' modus operandi is an ongoing effort that requires constant attention and an advanced approach.

ThreatMark's SOC team relies on two distinct sources for their work: 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 ThreatMark Anti Fraud Suite (AFS) deployments. Off-page elements include various proprietary methods in scanning and probing the internet for new threats & malicious activities.

By combining these elements, our SOC team casts a wide probing net that can detect, promptly alert, and mitigate cyber threats very fast.

For our clients and interested parties ThreatMark SOC team helps with:

- Early threat Detection & Mitigation
- Malware Detection & Analysis
- Consultancy & Education

You can reach out to our SOC team and discuss your cybersecurity challenges at **soc@threatmark.com**

Early Threat Detection & Mitigation Service Overview

Early Threat Detection focuses on discovering scams even before they can make any damage. Our research indicates that phishing is the key starting point to the most damaging scams in the banking industry.

Accordingly, we've built advanced phishing detection methods within our software. ThreatMark AFS uses a combination of on-page (e.g., our sensors and ID detectors) and off-page (e.g., honey-email, Twitter, internet scraping) factors to identify threats and fraudulent activities.

Once an active phishing site is detected, our SOC team analyzes it, categorizes and applies the new knowledge to ThreatMark's shared Threat Intelligence where the pattern of attack is embedded into the system for future prevention.

At the same time, the phishing attack is instantly processed for immediate mitigation.

Phishing Mitigation
Our SOC team leverages relationships with domain registrars and hosting providers to quickly mitigate and remove all discovered phishing sites as soon as possible.

Malware Detection & Analysis

ThreatMark SOC team also keeps an eye on the malware trends and threats in online banking. Here the team scope is on both desktop and mobile as two distinct but interconnected, channels.

Recently, due to the increased digitalization-accelerated by the pandemic and 'only remote' communication, there has been an increase of mobile banking users throughout the world

Accordingly, our SOC team noted increased existence and threats from mobile apps identified as financial malware.

Regardless of the channel ThreatMark's SOC team continuously works on detecting, analyzing and classifying new pieces of code detected on end users' devices.

True to our technology and industry vertical— a slightly bigger focus is put on the malware that can inflict greater damage to the protected banking applications or inflict serious financial harm. For malware analysis, the team combines automatic checks with necessary manual analysis and detailed investigation.

All findings are categorized and included in the shared Threat Intelligence – which helps all ThreatMark clients stay safe from the investigated and categorized malware. As with phishing, the malware's modus operandi is recorded as well – which makes it easier for our solution, and the SOC team, to detect future threats and prevent fraud even before it can cause any damage.

Consultancy & Education

ThreatMark SOC team can be a valuable partner in making businesses, and their teams, aware of the current cyber threats, fraudsters' activities and relevant prevention methods.

For our clients and interested parties, the team can advise or organizes workshops on the latest cyber threats and prevention methods.

Our SOC team helped Sberbank CZ finetune their anti-fraud landscape by organizing series of workshops and seminars on the topic. Training consisted of examples and best practices when it comes to the identification and mitigation of new malware types for both internet and mobile banking channels.

Read the full case study with Sberbank here: **https://www.threatmark.com/Sberbank**

You can reach out to our SOC team and discuss your cybersecurity challenges at **soc@threatmark.com**