



ThreatMark

ThreatMark

AFS Threats

Компания ThreatMark представляет решение для обнаружения киберугроз, основанное на поведенческом анализе пользователей и машинном обучении

Рост числа онлайн и мобильных пользователей и транзакций ведет к увеличению количества киберугроз. Хакеры постоянно ищут и находят новые способы и методы атак на клиентов банков и выпускают обновленное вирусное ПО. Популярность мобильного банкинга привела к росту атак на мобильные устройства и межканальных атак, которые трудно обнаружить с помощью традиционных средств.

Мы способны распознать атаки нулевого дня с невероятной точностью благодаря многоуровневой защите, комплексному подходу и анализу поведения и биометрии пользователей.

О компании ThreatMark

- Опытная команда специалистов по кибербезопасности, бывших этичных хакеров и экспертов по машинному обучению и искусственному интеллекту
- 20+ миллионов клиентов защищено
- Разработано специально для банков

ThreatMark AFS Threat **защищает**



Банковские трояны



Социальная инженерия



Кража личности



Небезопасные конфигурации



Фишинг



Боты и веб-скрапинг



Атаки на мобильный банкинг



Кросс-канальные атаки



Более высокая скорость обнаружения¹

ThreatMark TDS чувствителен к современным методам онлайн-мошенничества, включая социальную инженерию, фишинг и атаки нулевого дня.



Меньше ложных срабатываний¹

Глубокий поведенческий анализ профиля и целостный подход делают ThreatMark TDS адаптивным и точным при анализе потенциального мошенничества.



Экономия на двухфакторной аутентификации²

ThreatMark TDS способен распознавать пользователей с высокой точностью и дает банкам возможность сэкономить на двухфакторной аутентификации в 90% случаев.

¹ По сравнению с традиционным решением ² Оценка экономии на SMS-авторизации

Многоуровневый подход к обнаружению угроз и мошенничества



Поведенческий анализ пользователей

Активность пользователей мониторится на протяжении всей сессии с момента открытия приложения до выхода из него. Анализируются сотни параметров, включая поведение пользователей, биометрические данные, взаимодействие пользователей с веб и мобильным приложениями, подробности сессий, транзакций и т.д. Знание мельчайших деталей о пользователе позволяет более точно обнаруживать угрозы и сократить количество ложных срабатываний.

Машинное обучение

Для анализа поведения пользователей и сотен технических и финансовых параметров используются самые актуальные разработки в области машинного обучения и искусственного интеллекта. Благодаря этому мы способны обнаружить подозрительную активность в аккаунте пользователя еще на этапе подготовке к атаке, что ранее было невозможно.

Threat Detection Solution

ThreatMark AFS Threats может использоваться в составе комплексного решения ThreatMark Anti-Fraud Suite вместе с защитой мобильного банка, или может быть интегрирован с уже используемыми в банке системами риск-менеджмента и антифрода.



ThreatMark AFS

Комплексное решение для обнаружения угроз и предотвращения мошенничества



AFS Threats

Дополнение к уже используемым решениям для анализа транзакций

Time	Risk	Detection type	Alerts of detection	Session	Persisted session	User	IP
01/24/2019 11:40:00 AM	High	Unusual location	1/1	Q	Q	720728418	194.212.57.229
01/24/2019 11:38:36 AM	High	Unusual location	1/1	Q	Q	448028413	31.36.146.40
01/24/2019 11:30:34 AM	High	Unusual location	1/1	Q	Q	448028413	194.212.187.116
01/24/2019 09:58:52 AM	High	Unusual location	1/1	Q	Q	384028437	194.212.76.37
01/24/2019 09:58:52 AM	High	Suspicious transaction	1/1	Q	Q	720728418	194.212.58.719
01/24/2019 09:58:52 AM	High	Unusual location	1/1	Q	Q	720728418	194.212.58.719
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	414284034	194.212.4.108
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	50120	194.188.176.132
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	501740	194.206.167.28
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	448126	194.88.103.81
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	N/A	28.62.103.768
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	N/A	194.188.103.86
01/24/2019 09:58:51 AM	High	Unusual location	1/1	Q	Q	294207	197.0.86.15
01/24/2019 09:28:38 AM	High	Abnormal access	1/1	Q	Q	470928414	31.36.77.76
01/24/2019 12:16:56 AM	High	Unusual location	1/1	Q	Q	448028413	31.36.192.87
01/23/2019 09:52:18 PM	High	Unusual location	1/1	Q	Q	414284034	31.36.192.87

Внедрение

- Быстро и легко:** внедрение за несколько недель
- Гибко:** внедрение в облаке или в инфраструктуре банка
- Удобно:** все данные перед глазами фрод-аналитиков и службы безопасности
- Комплексно:** дополнительный сервис фрод-аналитики