Kaspersky Fraud Prevention

Automated Fraud Analytics

Реализация стратегии безопасности связана не только с передовыми технологиями. Речь также идет о данных, которые поступают в ходе анализа пользовательской сессии, а также о способности использовать их наряду с технологиями.

Именно для этого существует Automated Fraud Analytics: бизнес должен знать о возможной мошеннической активности, когда она еще не началась, обладать данными, которые имеют решающее значение для принятия точных, своевременных решений и для выявления ниаболее сложных случаев мошенничества.

Практическая применимость

Угрозы

- Мошенничество развивается - растущие проблемы с клиентами
- Более высокий уровень фрода - штрафы со стороны регулятора
- Угроза пропустить стадию подготовки атаки
- Растущая сложность атак - привычные и устаревшие решения не справляются

Функциональные возможности

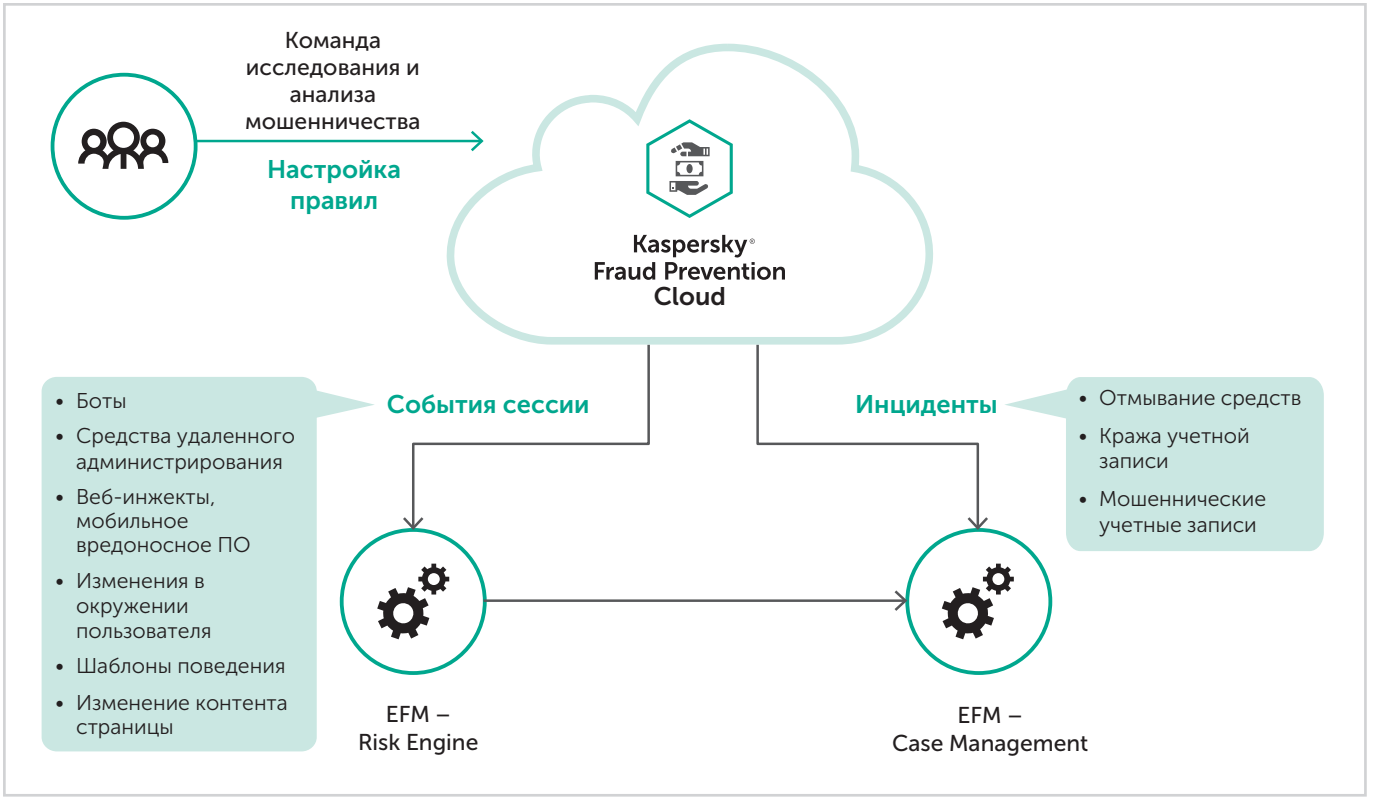
- Построение и сопоставление связей
- Поведенческий анализ на основе глубинного обучения
- Гибкая настройка правил

Кража учетной записи – Что если бы вы были уверены, что ваши цифровые каналы в данный момент используются легитимными юзерами? Что если бы вы знали, как пользователь ведет себя в вашем приложении или на сайте? Это только часть того, что анализирует Kaspersky Fraud Prevention. Мы помогаем вам узнать больше о клиентах, предоставляя ценные данные и знания, чтобы увидеть аномалии и подозрительное поведение до того, как мошенничество было совершено, в то время как сами клиенты не теряют доступ к своей учетной записи.

Мошеннические учетные записи – для защиты бизнеса от такого рода атак применяются поведенческий анализ и биометрия, а также анализ устройства и окружения для построения моделей легитимного и мошеннического поведения. Такой подход позволяет выявить отклонения в пользовательском поведении, и распознать как реального пользователя, пытающегося воспользоваться услугой, так и мошенника, намеревающегося нанести вред бизнесу.

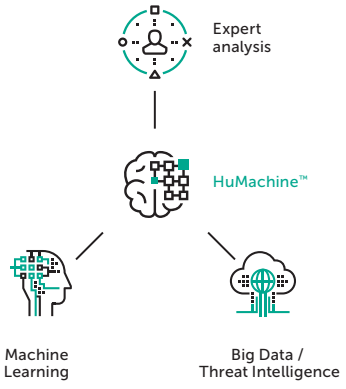
Отмывание денежных средств – построение связей между пользователями и устройствами, а также использование уникальных идентификаторов позволяет выявлять группы учетных записей, доступ к которым осуществляется с одного и того же устройства. Поведенческий анализ повышает эффективность обнаружения, отличая легитимных пользователей от мошенников. Благодаря глобальной репутации устройств Automated Fraud Analytics раскрывает связи между мошенническими аккаунтами и предотвращает сложные преступные схемы, реализуемые в разных организациях.

Аналитика мошенничества – на протяжении всей сессии, с самого ее начала, события, происходящие с пользователем, устройством, а также биометрические и поведенческие показатели тщательно анализируются. Объединение технологий и экспертизы аналитиков позволяет более точно настраивать решение под запросы бизнеса, а также тщательно прорабатывать обнаруженные случаи мошенничества.



Преимущества использования

- Обнаружение подозрительной активности до того, как мошенничество нанесло вред бизнесу
- Больше сценарев мошенничетсва раскрывается, выше уровень точности
- Выявление мошеннических сетей при помощи глобальной репутации и идентификаторов устройств
- Раскрытие сценариев отмывания средств в различных организациях
- Формирование подробных инцидентов, дополняющих внутренние системы мониторинга
- Расширенные возможности расследования инцидентов с помощью интуитивно понятного графического интерфейса



Всё об интернет-безопасности:
www.securelist.com

www.kaspersky.ru
#truecybersecurity
kfp@kaspersky.com