Краткий обзор разработок RSA

Система RSA® Transaction Monitoring

Мир Интернет-мошенничества непрерывно меняется. Новейшие угрозы, такие как атака «человек посередине» (man-in-the-middle или MITM) и трояны «человек в браузере» (man-in-the-browser Trojans), быстро развиваются и становятся все более широко распространёнными. Финансовые учреждения по всему миру обязаны реагировать на такие угрозы путем создания мощных, эшелонированных систем обороны. Помимо точной идентификации пользователей, пытающихся войти в систему, важно обеспечить аутентификацию выполняемых ими действий для повышения уровня безопасности online-операций, уменьшения числа мошеннических транзакций и снижения риска от вновь возникающих угроз.

RSA® Transaction Monitoring

Система RSA® Transaction Monitoring предоставляет финансовым учреждениям комплексный набор средств для обнаружения фактов Интернет-мошенничества и эффективной борьбы с ним. Система RSA Transaction Monitoring отслеживает поведение пользователей в сети, обнаруживает подозрительные транзакции, позволяет финансовым учреждениям контролировать сомнительные действия в режиме реального времени и принимать соответствующие меры для уменьшения и устранения убытков от мошенничества.
Рассматриваемое решение позволяет финансовым учреждениям:

- отслеживать, обнаруживать и изучать факты мошенничества;
- добавить к применяемой системе аутентификации клиентов еще один уровень безопасности;
- защищаться от возникающих угроз, таких как атака «человек посередине» и трояны «человек в браузере»;
- идентифицировать попытки мошенничества без изменения привычных для клиентов систем и процедур;
- внедрить систему, которая повысит эффективность работы корпоративной группы анализа угроз мошенничества;
- осуществлять быструю интеграцию системы безопасности - в виде развернутого локально программного обеспечения или модели «программное обеспечение как услуга» (SaaS) – с применяемой системой дистанционного обслуживания клиентов;

RSA Transaction Monitoring представляет собой надежное решение, позволяющее добиться превосходных результатов. Результаты, полученные при мониторинге банковских online-операций в одном из ведущих европейских финансовых учреждений:

- снижение числа мошенничеств на 96%;
- процент выявленных подозрительных транзакций по отношению к числу всех транзакций 0,2% – 0,4%;
- коэффициент ложных срабатываний 1:880;
- значительное сокращение убытков от мошенничеств и последующих попыток нарушения защиты.

Кто пользуется системой RSA Transaction Monitoring?

В настоящее время система RSA Transaction Monitoring используется ведущими финансовыми учреждениями по всему миру, она доказала свою чрезвычайно высокую эффективность при выявлении online-мошенничеств. Transaction Monitoring используется многими ведущими организациями, среди которых:

- международные коммерческие банки - для отслеживания попыток входа в банковскую систему дистанционного обслуживания, прохождения безналичных денежных переводов и других действий;
- эмитенты кредитных и дебетовых карт - для предотвращения мошенничества в сфере электронной коммерции;
- прочие поставщики финансовых услуг, например, брокерские фирмы - для мониторинга online-транзакций.

За кулисами: Мониторинг, Обнаружение, Расследование

Ядром системы RSA Transaction Monitoring является мощный самообучающийся RSA® Risk Engine, который постоянно контролирует различные действия пользователей и обнаруживает мошенничество или попытку мошенничества в режиме реального времени. Возможности Risk Engine еще более расширяются за счет получения данных из международной межкорпоративной базы данных схем и профилей мошенничества RSA® eFraudNetwork™. Помимо прочего, система RSA Transaction Monitoring содержит современные средства управления и дополнительные утилиты, среди которых:

- Приложение Policy Manager позволяет финансовым учреждениям легко настраивать установленные по умолчанию RSA системные политики, а также добавлять новые правила для учета своих специфических целей. Перед реальным использованием работа каждого правила может быть смоделирована, что позволяет финансовым учреждениям точно настроить политики для получения оптимальных результатов и контролировать процент транзакций, подлежащих дополнительной проверке.

Рисунок 1. Мониторинг, Обнаружение, Расследование – RSA Transaction Monitoring представляет собой мощную комплексную систему, позволяющую существенно уменьшить число мошеннических операций.

– Высокоэффективное проблемно-ориентированное приложение Case Management для изучения подозрительных транзакций. Полученное подтверждение о том, что данная транзакция является попыткой мошенничества или, напротив, идентифицирована как легитимная, автоматически учитывается Risk Engine. Это обеспечивает точную подстройку системы и улучшает характеристики ее работы в будущем.

Мониторинг: Вход в систему и последующие действия пользователя

Система RSA Transaction Monitoring может быть интегрирована в различные точки online-приложений для отслеживания указанных ниже действий:

– Вход в систему. Слежение за процедурой входа в систему позволяет Risk Engine создать профиль, характеризующий каждого активного пользователя. RSA Transaction Monitoring часто надстраивается над существующей процедурой строгой аутентификации при входе в систему.
– Безналичный денежный перевод. Система RSA Transaction Monitoring способна определить потенциально мошеннические денежные переводы сразу при их выполнении. Это позволяет финансовому учреждению идентифицировать дискредитированные счета своих клиентов и используемые мошенниками счета получателей, что существенно снижает риск мошеннических действий. Кроме того, RSA Transaction Monitoring следит за выполнением таких действий, как добавление новых бенефициариев, запрос дополнительных кредитов, запрос новых чеков, просмотр чеков и электронные платежи.
– Изменения профиля. Система RSA Transaction Monitoring может быть настроена таким образом, чтобы дополнительно проверять действия, для которых характерна высокая степень риска. К таким действиям относятся изменение паролей пользователей, адресов электронной почты или физических почтовых адресов, контрольных вопросов, телефонных номеров или PIN-кодов банковских карт.

«Верификация транзакций обеспечивает защиту от мошеннических действий, выполняемых в результате атак по схеме MITM (Man-in-the-middle - «человек посередине») или троянов или вследствие использования похищенных идентификационных данных пользователя, когда злоумышленник сумел пройти процедуру начальной идентификации при входе в систему.»

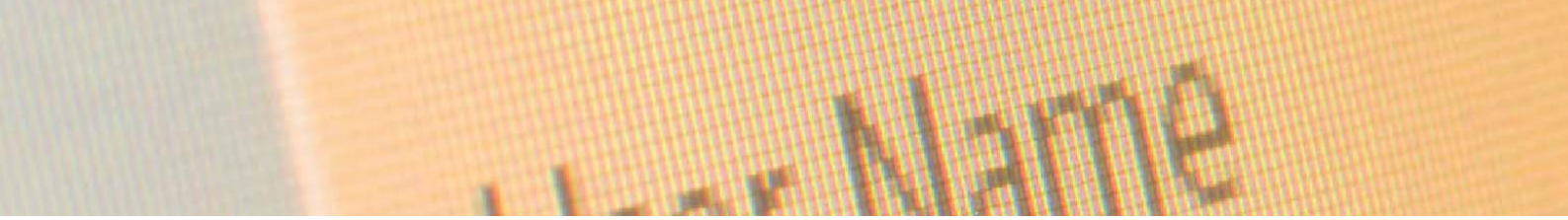
- Авива Лайтэн (Avivah Litan) “*Верификация транзакций дополняет процедуры выявления мошенничества и строгой аутентификации” 10/12/06*

– Неудачный вход в систему. Несколько неудачных попыток входа в систему предупреждают Risk Engine о возможном действии с высокой степенью риска.

Кроме перечисленных выше, система RSA Transaction Monitoring позволяет отслеживать специфические для данного финансового учреждения действия пользователей вне зависимости от того, являются они новыми для системы или расширяют текущий список контролируемых действий.

Обнаружение: RSA® Risk Engine

RSA® Risk Engine, ядро системы RSA Transaction Monitoring, в режиме реального времени оценивает любую online-активность пользователей, отслеживая свыше ста индикаторов для надежного обнаружения факта мошенничества. Risk Engine разработан специально для решения задач, возникающих в быстро меняющейся online-среде, и способен предоставлять результаты непосредственно с момента ввода его в эксплуатацию.



Каждому действию присваивается уникальный балл риска в диапазоне от 0 до 1000 на основании байесовской модели (Bayesian model), которая используется для автоматической оценки вероятности риска по каждому индикатору. Окончательный балл риска состоит из комбинации балла, зависящего от относительно недавнего поведения пользователя (short-term influenced), балла, связанного с данными, накопленными за большой период времени (long-term influenced), а также балла риска, назначаемого вручную и используемого для борьбы с вновь возникающими угрозами.

Борьба с возникающими угрозами

Атаки типа «человек посередине» и трояны «человек в браузере» представляют собой относительно новые методы, которые используются мошенниками для попыток доступа к информационным системам финансовых учреждений. Система RSA Transaction Monitoring, благодаря наличию RSA Risk Engine, полностью подготовлена к борьбе с указанными угрозами, а также угрозами, которые могут появиться в будущем. Используя различные факторы, как, например, предопределенные и связанные с профилем пользователя индикаторы риска, методики анализа с распознаванием профиля атак, кластеризация и “раскраска”, самообучающаяся система Case Management, база данных RSA eFraudNetwork, “учетные записи - ловушки” – Risk Engine обеспечивает на длительное время защиту финансовых учреждений и их клиентов от постоянно возникающих угроз.

Система Risk Engine настраивалась и отлаживалась на массиве данных, содержащем свыше 20 миллиардов клиентских транзакций. Для защиты от вновь возникающих угроз байесовская аналитическая модель Risk Engine способна быстро обнаружить формирующиеся схемы мошенничества, основываясь на анализе лишь небольшой части определенных транзакций. По сравнению с нейронными сетями, где цикл самообучения может занимать от одного до трех месяцев, Risk Engine работает во много раз быстрее. Вероятности в байесовской сети пересчитываются ежедневно, поэтому модель риска всегда является актуальной.

Индикаторы риска

Система RSA Transaction Monitoring проверяет как заранее заданные, так и зависящие от профиля пользователя индикаторы риска.

Они используются для уведомления Risk Engine о специфичных для конкретного действия параметрах, которые несут информацию о степени риска. Список предопределенных индикаторов регулярно обновляется с учетом громадного объема информации, полученной системой Risk Engine, и результатов изучения схем мошенничества.

Примеры некоторых предопределенных индикаторов:

- eFraudNetwork помогает сопоставить IP-адреса и конкретные устройства (пользовательские компьютеры), которые ранее были помечены как несущие высокую степень риска
- Модель поведения пользователя
- Сумма транзакции
- IP-адреса и их география, ранее отмеченные как высокорискованные
- Недавние изменения профиля
- Физическая скорость перемещения терминала пользователя
- Получатели незаконных платежей
- Недавнее открытие счета

Индикаторы, зависящие от профиля, используются для выявления аномалий, относящихся к конкретному профилю. Среди них:

- Идентификационный номер устройства (device ID) и особенности его работы
- Поставщик услуг в сети Интернет, страна и тип соединения
- Аномально высокие скорости перемещения терминала пользователя
- Отклонения от обычного временного режима работы пользователя
- Тип канала
- Сумма транзакции
- Среднее/общее количество операций
- Предыдущие алгоритмы поведенческих действий

Risk Engine не ограничивается только профилированием пользователей; система анализирует также другие параметры:

- Ресурсы, участвующие в транзакции - например, прокси-серверы, другие устройства;
- Комбинация учетной записи пользователя и используемого им ресурса, например, браузера;
- Группы учетных записей пользователя, например: все учетные записи, которым соответствуют одинаковые атрибуты профиля. Использование групп учетных записей пользователей – это один из многих путей, которые позволяют системе Risk Engine определять риск даже в тех случаях, когда по отдельному пользователю существует лишь малое количество собранной информации.

Методика анализа с распознаванием профиля атак

Алгоритм автоматического распознавания профиля атак способен консолидировать различные параметры и рассчитывать балл риска используя принцип байесовской сети. Для оценки риска используется статистическая модель, позволяющая учесть все признаки и вычислить вероятность того, что изучаемое действие является мошенническим или отличается высокой степенью риска.

Рисунок 2: При определении уровней риска система RSA Risk Engine рассматривает многочисленные элементы данных.

Байесовская аналитическая модель способна быстро обнаружить новые схемы атак на основании небольшого числа мошеннических операций. Для online-приложений такая особенность очень важна, поскольку преступные сообщества в Интернете способны быстро адаптироваться к новым инструментам контроля, которые внедряют финансовые учреждения, и поэтому постоянно изменяют цели и методы мошенничества. Параметры байесовской сети ежедневно пересчитываются, что позволяет поддерживать модель риска в актуальном состоянии.

Некоторые из уникальных специализированных средств системы Risk Engine:

- Комбинация кратковременных и долговременных баллов риска (short / long-term influenced scores). Система использует два байесовских блока: один учитывает активность пользователя за период, составляющий несколько недель (кратковременный); второй учитывает данные за период, составляющий несколько месяцев (долговременный). Такой подход позволяет модели «запоминать» долговременные, хорошо известные тенденции и одновременно адаптироваться к новым вариантам мошеннических операций.
- Управление рисками с учетом агентурной информации. Системы автоматического распознавания шаблонов атак способны распознавать новые схемы мошенничества только путем анализа недавних случаев мошенничества. При таком подходе попытка мошенничества может быть пресечена только после того, как система обнаружит тенденцию.

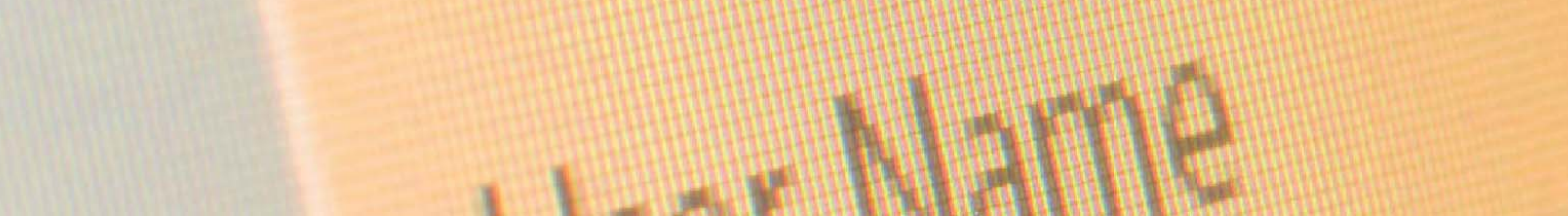
Для улучшения характеристики технологии предотвращения мошенничества и снижения опасности новых угроз RSA, кроме автоматического распознавания шаблонов атак, использует результаты расследований Командного Центра по борьбе с мошенничеством AFCC.

В AFCC (RSA Anti- Fraud Command Center) работают более 80 аналитиков, которые проникают в группы Интернет-мошенников с помощью технологий агентурной разведки, аналогичных методикам, используемым правительственными спецслужбами. Они добывают ценную информацию, которая позволяет команде специалистов RSA, занимающейся вопросами борьбы с мошенничеством, вручную подстраивать параметры системы. Данная технология помогает противодействовать самым последним методам мошенничества, а также атакам на организации других отраслей.

Применение самообучения

Технологии, используемые преступными сообществами для online-мошенничеств, характеризуются высоким уровнем адаптации. Мошенники обладают почти неограниченной мобильностью и потенциально способны в любой момент атаковать любой Интернет-портал, используя proxy-сервер для скрытия своих IP адресов. Принимая во внимание скорость, с которой мошенники изменяют способы своей деятельности, внедрение системы управления рисками, которая обладает возможностями самообучения в режиме реального времени, становится очень важным фактором.

Система RSA Transaction Monitoring выявляет факты потенциального мошенничества и присваивает подозрительным действиям высокие баллы риска. Операции с максимальным баллом регистрируются в системе Case Management, работающей в режиме реального времени. Благодаря этому финансовое учреждение имеет возможность контролировать потенциально опасные операции.



Результаты исследования немедленно возвращаются в систему Risk Engine и модель рисков обновляется соответствующим образом.

Система Risk Engine работает в обоих направлениях с целью снижения коэффициента ложных срабатываний до минимума. Аналогично тому, как на учет ставятся операции, связанные с подтверждёнными мошенническими схемами, регулируется и порядок работы с подозрительными схемами, которым присвоен высокий балл риска, но которые возникли в результате законного поведения пользователя. Например, если обнаружен новый proxy-сервер, на котором выполняются очень необычные операции, система Risk Engine присвоит таким операциям высокий балл риска; однако если расследование покажет, что такие операции являются законными, то доказательства законности вернутся в Risk Engine, и система сможет выполнить самонастройку для работы с такими операциями в будущем.

Возможности быстрого самообучения позволяют системе развиваться и адаптироваться для оперативного реагирования на любые изменения технологий, используемых мошенниками. В случае внедрения системы аутентификации, работающей по принципу оценки рисков (например, системы RSA® Adaptive Authentication для явной аутентификации), результаты попыток аутентификации (удачные или неудачные) также передаются в систему Risk Engine, которая благодаря этому получает сведения о попытках доступа к защищаемым ресурсам.

Эффект от подключения к сети RSA® eFraudNetwork

Ключевым элементом системы Transaction Monitoring является база данных RSA® eFraudNetwork: межкорпоративная сеть, предназначенная для распространения и совместного использования информации о деятельности мошенников. Среди членов данной сети - десятки международных финансовых организаций, а также некоторые из ведущих мировых поставщиков услуг в сети Интернет. Сообщество eFraudNetwork распространяет сведения о мошенничествах среди многочисленных организаций в режиме реального времени: если атакам мошенников подвергся один из членов сообщества, все остальные немедленно получают об этом уведомления и защищаются от таких атак.

Система RSA Transaction Monitoring помогает работающим в сети RSA транснациональным компаниям - поставщикам финансовых услуг выявлять профили и схемы атак, отслеживать поведение мошенников более чем в 65 странах. Различные системы RSA, предназначенные для борьбы с мошенничествами, в настоящий момент применяют свыше 50 крупных банков, организаций-эмитентов кредитных и дебетовых карт, брокерских фирм и тысячи более мелких финансовых учреждений.

«eFraudNetwork представляет собой уникальную и важную технологию, обеспечивающую конкурентное преимущество компании«Alliance & Leicester». Борьба с online-мошенничествами является нашей повседневной задачей, и eFraudNetwork позволяет защищать наших клиентов круглосуточно в режиме реального времени.»

-«Alliance & Leicester»

Все эти организации обслуживают сотни миллионов клиентов по всему миру. Кроме того, база данных eFraudNetwork подключена к ресурсам основных поставщиков услуг в сети Интернет, например, AOL, Netscape, Earthlink и Microsoft. Клиенты RSA немедленно становятся членами сообщества eFraudNetwork и пользуются всеми преимуществами доступа к его общеотраслевым ресурсам.

eFraudNetwork доступна во всех возможных вариантах развертывания системы RSA Transaction Monitoring. При внедрении системы в центре обработки данных финансового учреждения (on-premise) локальная копия базы данных eFraudNetwork обновляется каждые несколько минут, обеспечивая заказчиков актуальными сведениями.

Преимущества учетных записей-ловушек

Учетные записи-ловушки способны предоставить финансовым учреждениям ценные сведения относительно схем мошенничества. Такие сведения помогут предотвратить мошеннические операции и защититься от атак в будущем.

Создание ловушек в банковской online-среде аналогично использованию меченых купюр для поимки обычных воров. Если Командный центр RSA по борьбе с мошенничеством (AFCC) обнаруживает сайт мошенников, то с помощью технологии RSA Randomized Credentials Technology (RCT) (патентная заявка находится на рассмотрении) туда отправляются ложные данные об учетной записи. Механизм RCT отсылает «реальные» учетные записи-ловушки на «фишинг»-сайт так, чтобы ловушки для мошенника выглядели как можно более реалистично. Когда мошенник пытается использовать полученные фиктивные параметры доступа для входа на веб-сайт финансового учреждения, система RSA Risk Engine немедленно обнаруживает такую попытку и идентифицирует мошенника. После этого характеристики отмеченного устройства (например, IP-адрес) передаются в базу данных RSA eFraudNetwork.

Как следствие, любые будущие попытки входа с данного устройства в защищаемую систему даже при использовании подлинной учетной записи могут быть обнаружены и предотвращены. В сочетании с возможностями Risk Engine свыше 90% использованных учетных записей-ловушек предотвращают дальнейшие попытки мошеннических атак.

Кластеризация и «Раскраска»

Система Risk Engine использует два патентованных итерационных процесса, которые называются кластеризация и «раскраска». Кластеризация представляет собой процесс ассоциации и связывания транзакций, которые имеют какие-либо общие элементы (учетная запись пользователя, IP-адрес, устройство, с которого производился вход в систему). Поэтому вместо рассмотрения одной транзакции в единицу времени система может рассмотреть «более масштабную картину».

«Раскраска» представляет собой процесс, в рамках которого транзакция, которая идентифицирована как мошенническая, приводит к выделению («раскраске») всего кластера, к которому принадлежит данная транзакция. Таким образом, каждая транзакция из данного кластера будет рассматриваться как операция с повышенным уровнем риска в зависимости от степени связанности элементов кластера (насколько сильно рассматриваемая операция связана с мошеннической операцией).

Данный процесс повторяется циклически, поэтому при получении информации о новых транзакциях они связываются с предыдущими операциями и становятся частью существующего кластера. Если параметры предыдущей транзакции (например, IP) уже «закрашены», то параметры новой ассоциированной транзакции также будут «закрашены». Это приводит к немедленному снижению риска мошенничества.

Для оптимизации процедур распознавания новых тенденций мошенничества без увеличения числа ложных срабатываний Risk Engine применяет также метод, известный под названием активного отбора образцов. В тех случаях, когда существует какое-либо подозрение о мошеннических операциях, Risk Engine активно выполняет выборку малого объема таких операций для дальнейшего изучения. Когда такие операции идентифицируются в качестве законных или мошеннических, Risk Engine автоматически выполняет самонастройку для повышения точности работы в будущем и при необходимости запускает процесс кластеризации.

Policy Manager

Несмотря на то, что средства присвоения баллов риска системы Risk Engine рассчитаны на обеспечение оптимальной точности путем присвоения максимального числа баллов только самым рискованным операциям, компания RSA признает, что каждое финансовое учреждение имеет свою собственную специализированную базу знаний и политик управления рисками.

Поэтому в рассматриваемую систему входит приложение Policy Manager, позволяющее организациям строить собственную модель управления рисками, которая может быть настроена в режиме реального времени. Применяя данное приложение, финансовые учреждения полностью контролируют свою политику управления рисками. Они также могут использовать приложение Case Management для изучения появляющихся схем мошенничества и точно определять, какие риски будут являться допустимыми, а какие нет. Собственная модель управления рисками может быть основана на встроенном наборе правил, установленном по умолчанию.

Благодаря использованию приложения Policy Manager финансовые учреждения могут преобразовывать свои политики управления рисками в определенные решения или меры на основе учета балла риска и других параметров, например, страны, к которой относится IP, количества операций и профиля пользователя. До ввода в действие каждое правило может быть протестировано с помощью средств моделирования и точно отрегулировано в несколько этапов до получения оптимального результата. Кроме того, после ввода в действие каждое правило может быть настроено на обработку только ограниченного объёма транзакций. Таким образом, степень влияния нового правила лимитируется в процессе работы для дальнейшей оценки его эффективности.

Приложение Policy Manager разработано с учетом удобства использования, позволяет легко осуществлять мониторинг существующих правил и обеспечивает возможность задания и внедрения тысяч новых правил без влияния на эксплуатационные характеристики системы.

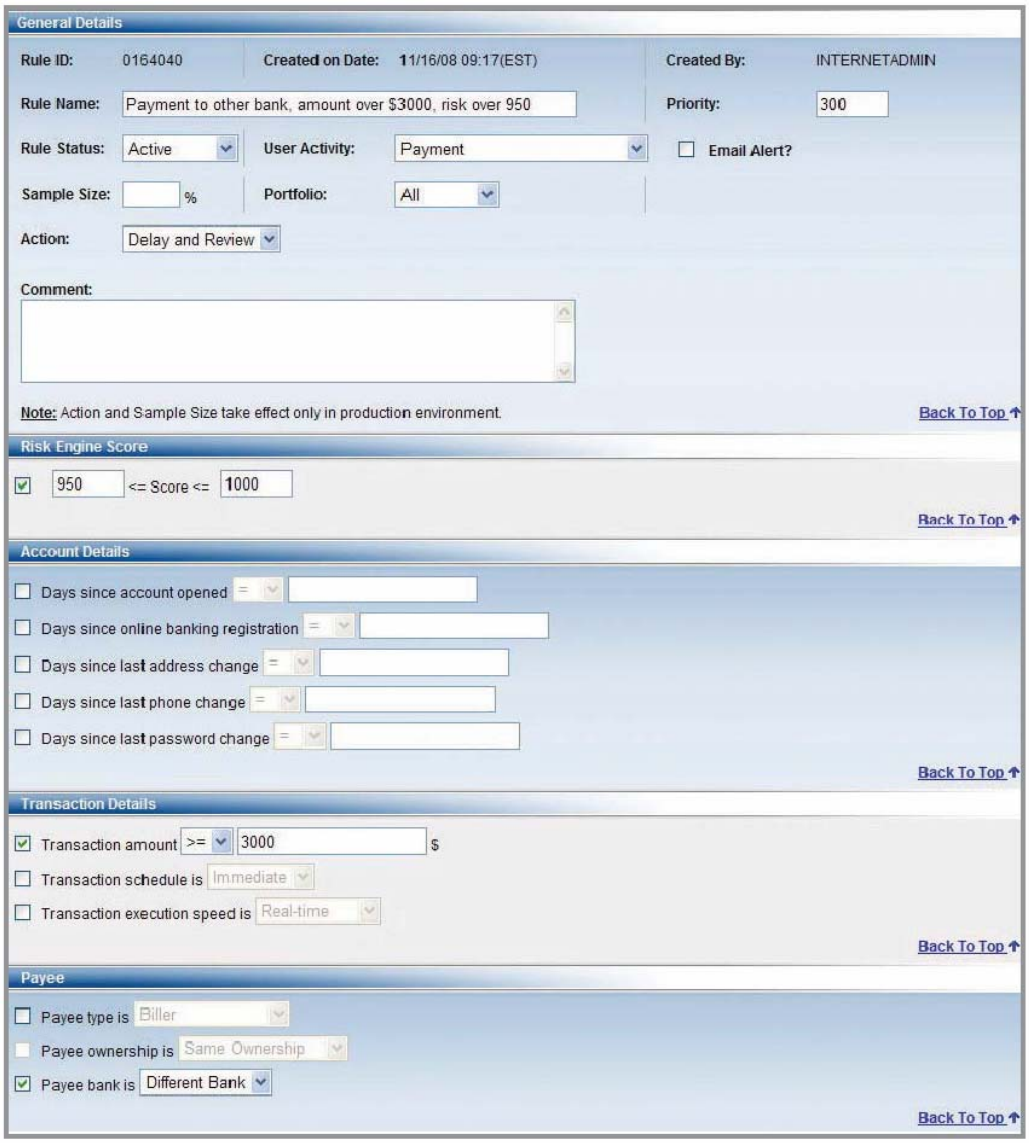


Рисунок 3: Интерфейс Редактора правил (Policy Manager). В данном примере рассмотрено новое правило под названием «Платеж в другой банк, сумма свыше 3000 долларов США, присвоенный риск более 950 баллов». Действие, выполняемое для транзакций, попадающих под действие данного правила – «задержать и проверить» («delay and review»), т.е. задержать выполнение операции до тех пор, пока эксперты по борьбе с мошенничествами не свяжутся с клиентом.

Режимы работы

При внедрении системы существуют два режима работы: режим просмотра и режим принятия решений в реальном времени.

Режим просмотра

В данном режиме система обрабатывает каждое действие в реальном времени и передает сведения о подозрительных действиях в приложение Case Management. После этого отдел финансового учреждения, занимающийся борьбой с мошенничествами, обращается к клиентам с просьбой подтвердить законность подозрительных операций. Данный режим является типовым для первого этапа внедрения, однако может являться штатным в ситуациях, когда финансовые средства не передаются в реальном времени.

Режим принятия решений в реальном времени

В данном режиме помимо отметки транзакций для просмотра система в реальном времени генерирует балл риска и рекомендованные для финансового учреждения меры. После этого финансовое учреждение может использовать результаты работы системы для принятия решения. Стандартными решениями, принимаемыми в реальном времени, являются следующие:

- Выполнение транзакции, но присвоение ей отметки для изучения в приложении Case Management;
- Задержка транзакции на заданный период времени для изучения с разрешением на выполнение, если изучение не будет завершено вовремя;
- Задержка транзакции на заданный период времени для изучения с запретом на выполнение, если изучение не будет завершено вовремя.

- Запрет выполнения операции, которая либо инициирована ресурсом, о котором известно, что им пользуются мошенники, либо связана с аналогичным счетом получателя. Данный режим работы обычно используется в ситуациях, когда перевод денежных средств выполняется в режиме реального времени (или в масштабе времени, близком к реальному) и не является обратимым. Для применения данного варианта от банка требуется поддержка режима синхронной работы, например, Web Services (SOAP) API.

Расследование: Case Management

После выполнения анализа каждого действия и расчета для него уникального балла риска система RSA Transaction Monitoring передает сведения о некоторых действиях в систему Case Management в соответствии с политикой управления рисками данного финансового учреждения. Это позволяет финансовому учреждению оптимизировать процедуры управления рисками и концентрировать силы на исследовании только тех операций, которые с большой степенью вероятности являются мошенническими.

Для облегчения работы аналитиков инциденты в системе Case Management представлены не отдельными операциями, а, скорее, отражают все операции, выполнявшиеся с конкретным счетом. Таким образом, аналитики имеют возможность рассмотреть в процессе анализа все или только некоторые действия пользователя .

Система Case Management предусматривает различные режимы работы, среди которых следующие:

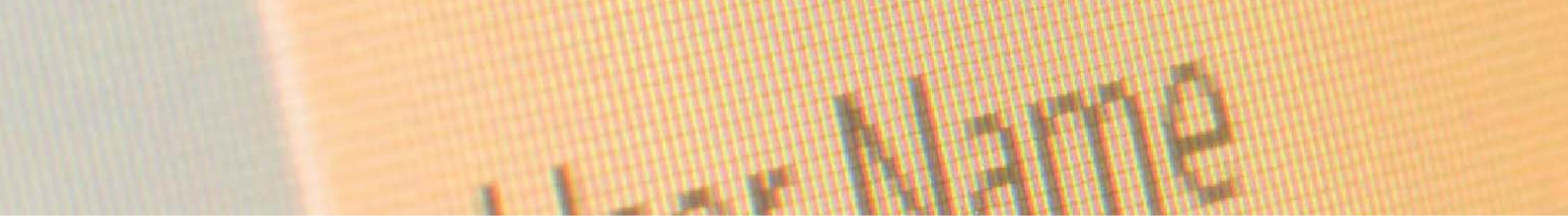
- Очередь процессов. Данный режим установлен по умолчанию. Инциденты с мошенничествами распределяются равномерно между всеми аналитиками, работающими в системе, с учетом внутренних приоритетов. После принятия решения по одному инциденту для изучения предлагается следующий инцидент с максимальным приоритетом. Во время обработки инцидента аналитиком информация об этом инциденте блокируется от изменения ее другими аналитиками до завершения процесса обработки.
- Очередь процессов, заданная аналитиком. Аналитик может создать очередь инцидентов в соответствии со своими собственными критериями фильтрации. Аналогично предыдущему режиму, аналитику после принятия решения по текущему инциденту не нужно возвращаться к списку инцидентов - он автоматически переходит к рассмотрению следующего инцидента согласно заданным параметрам фильтрации.

С целью облегчения работы аналитиков параметры фильтра сохраняются с привязкой к учетной записи пользователя.

- Поиск учетной записи пользователя. Аналитик может сконцентрироваться на определенной счетной записи и изучить все связанные с нею инциденты.
- Просмотр очереди. Аналитик просматривает все операции, ожидающие исследования в очереди. Данный режим работы в любой момент может обеспечить менеджеров системы полными сведениями о подозрительных действиях.
- Контроль операторов. Менеджеры системы могут следить за процессом работы конкретного аналитика.
- Исследуемые инциденты. Список всех инцидентов, включая возможности использования дополнительных фильтров и сортировки по многочисленным параметрам, позволяет более тщательно изучать инциденты, связанные с мошенничеством. Данный режим позволяет финансовым учреждениям проводить более глубокие, по сравнению с текущими, исследования схем действий мошенников. Отфильтрованные результаты могут быть экспортированы в формат Microsoft® Excel. Исследуемые инциденты помогают финансовому учреждению создавать определенные наборы правил, которые могут быть использованы в приложение Rules Management.

Что касается конкретного инцидента, то объем информации по нему может быть увеличен, и аналитик имеет возможность добавлять комментарии и изменять статус инцидента с «открытого» («open») на «мошенничество подтверждено» («fraud confirmed»), «законность подтверждена» («genuine confirmed») и т.д. Результаты расследования в системе Case Management как в отношении подтвержденного мошеннического действия, так и в отношении подтвержденного законного действия возвращаются в Risk Engine.

В сочетании с приложением Policy Manager система Case Management также может быть использована для того, чтобы помочь финансовому учреждению управлять собственной политикой работы с рисками и внедрить новые online-услуги с обеспечением достаточного уровня безопасности.



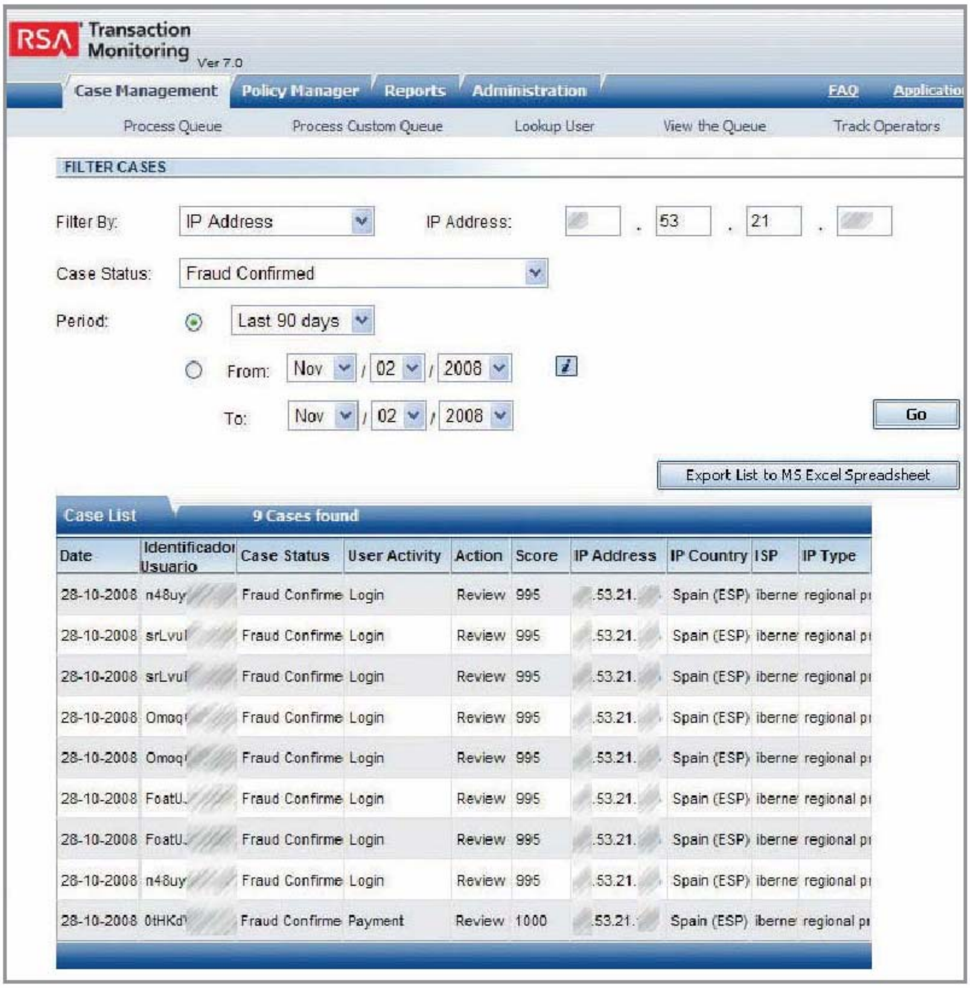


Рисунок 4: Case Management: режим расследуемых инцидентов. В данном режиме могут быть проанализированы заданные тенденции. Например, в данном случае обнаружен один IP, с которого был получен доступ к 6 счетам за один день.

Подготовка отчетов

Система RSA Transaction Monitoring готовит сводные отчёты для менеджеров и специалистов, принимающих решения, предоставляя удобный доступ к структурированным системным данным высокого уровня. Данные отчеты содержат точные агрегированные данные, например, процент исследованных инцидентов, процент тех исследованных инцидентов, которые подтверждены в качестве мошеннических или законных действий, коэффициент ложных тревог и причины назначения балла риска. В системе предусмотрены перечисленные ниже настраиваемые отчеты:

– Оперативный отчет суммирует рабочие характеристики системы и помогает ответить на такие вопросы, как: «Сколько операций было обработано системой? Сколько из них было отмечено для изучения? Сколько из них было в дальнейшем изучено? Каков коэффициент ложных срабатываний?»

– Отчет об анализе правил показывает эффективность правил, заданных специалистом финансового учреждения, и режимов тестирования, поэтому специалисты по работе с рисками смогут увидеть количество операций, попадающих под действие данного правила, и количество операций, признанных мошенническими в результате расследования.

– Отчет об анализе действий предоставляет статистические сведения, относящиеся к каждому решению / действию, предпринятому финансовым учреждением.

– Отчет о базе необработанных данных содержит журнал действий, выполненных отделом расследования инцидентов. Эта информация позволит произвести быструю диагностику и проконтролировать неисследованные инциденты.

Усиление режима безопасности при совместной работе с действующими системами аутентификации

Система RSA Transaction Monitoring может работать совместно с любой существующей системой аутентификации, включая:

- статические имена пользователей и пароли;
- генераторы одноразовых паролей от различных поставщиков;
- смарт карты EMV/CAP;
- списки TAN или iTAN, карты лото/скретч-карты/матрицы;
- аутентификация через SMS для мобильных устройств;
- системы на базе PKI/клиентского приложения (не на базе веб-браузера).

Методы интеграции

Система RSA Transaction Monitoring может быть быстро внедрена с использованием одного из нескольких поддерживаемых методов интеграции.

Каждый метод предназначен для решения особых коммерческих задач с учетом технических и временных ограничений финансового учреждения. К указанным методам интеграции относятся следующие:

- Web Services (SOAP) API позволяет финансовым учреждениям вводить в систему дополнительные данные, что повышает успешность профилирования транзакций. Благодаря синхронному режиму, API имеет возможность снабжать финансовое учреждение рекомендациями по каждому запросу, касающемуся операций с повышенным уровнем риска. Это наиболее широко используемый метод интеграции, поскольку он дает возможность воспользоваться преимуществами всех функций системы RSA Transaction Monitoring.
- HTML Beacon представляет собой невидимое изображение размером 1x1 пиксел, размещенное на веб-странице финансового учреждения. Путем вызова данного изображения с сервера RSA, HTML Beacon собирают информацию из банковской online-системы. HTML Beacon является наиболее быстрым для внедрения вариантом, поскольку для данной функции не требуется разворачивания программных или аппаратных средств в центре обработке данных финансового учреждения.
- Log File Analysis использует информацию, которая собрана в журнальных файлах, уже созданных банковскими online-серверами финансового учреждения. Данный подход не требует интеграции с банковской системой, что позволяет быстро внедрить RSA Transaction Monitoring с низким операционным риском. Данный метод интеграции должен использоваться в качестве способа быстрого запуска до тех пор, пока не будут установлены API.

Локальные модели и модели «программное обеспечение как услуга» (SaaS)

Система RSA Transaction Monitoring может быть установлена в виде полностью настраиваемой модели типа «программное обеспечение как услуга» (SaaS) или в виде локальной версии (on-premise) с использованием имеющейся ИТ-инфраструктуры. Оба варианта внедрения поддерживают схему «защита на будущее» системы RSA Transaction Monitoring и позволяют финансовым учреждениям в полной мере применять технологии RSA, предназначенные для борьбы с появляющимися схемами мошенничества.

RSA – это Ваш проверенный партнер

RSA - отделение компании EMC, занимающееся проблемами обеспечения информационной безопасности, является экспертом в области защиты централизованных информационных систем и помогает обеспечить защиту информации в течение всего времени ее существования. RSA снабжает клиентов эффективными средствами защиты важных информационных ресурсов и средствами online-идентификации, независимо от сферы деятельности и уровня развития предприятия. RSA также предлагает технологии централизованного сбора, хранения и обработки журналов регистрации событий, упрощающие задачи по обеспечению соответствия требованиям и стандартам.

RSA предлагает ведущие в отрасли решения по управлению идентификационной информацией и контролю доступа, управлению шифрованием и ключами защиты, а также решения по защите от мошенничества. Эти решения применяются для защиты персональных данных миллионов пользователей, сведений о выполняемых ими операциях и данных, создаваемых в результате выполнения этих операций. Дополнительные сведения приведены на сайтах www.RSA.com и www.EMC.com.

TM SB 1108

RSA®
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com