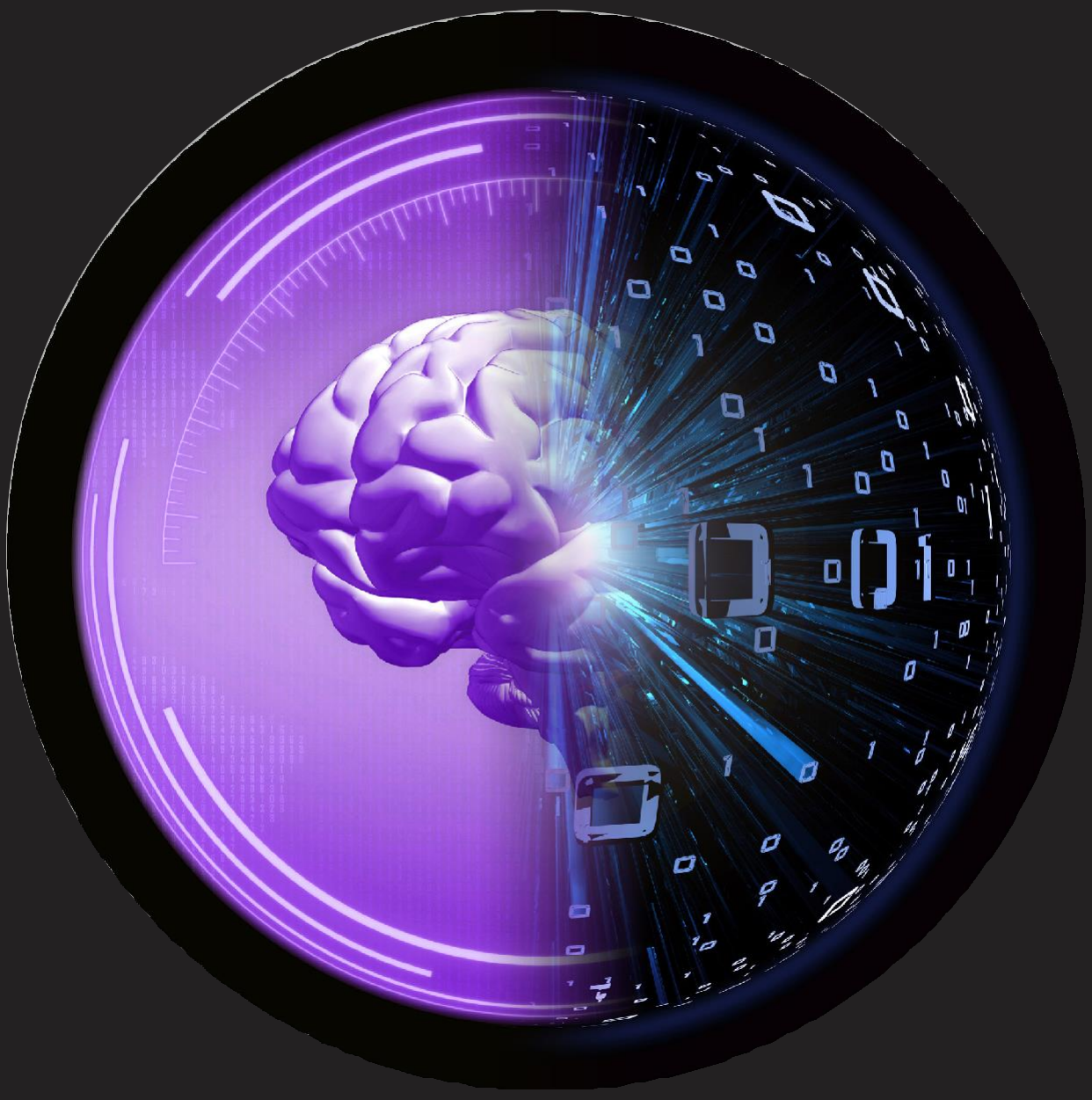
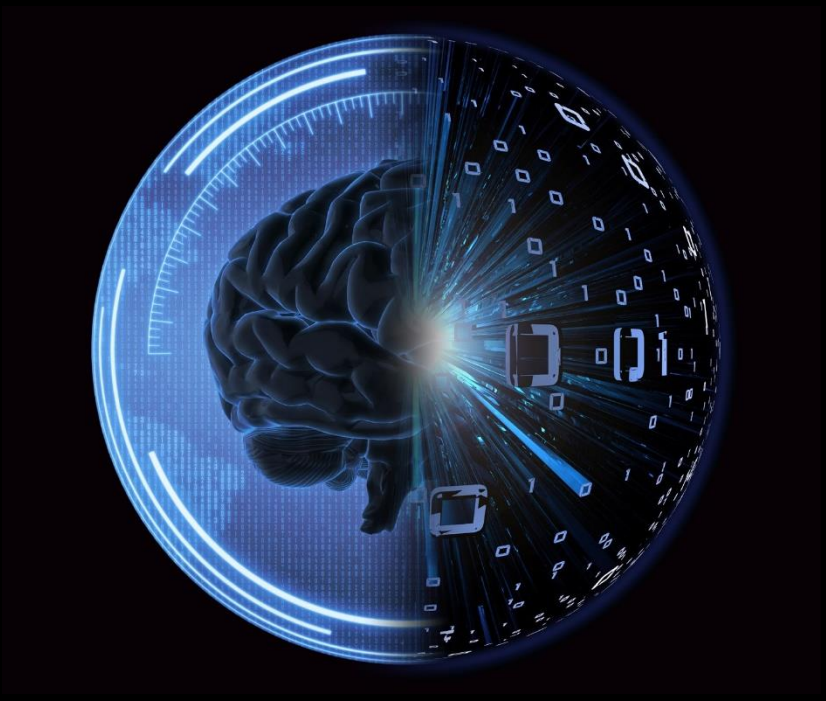
Deloitte.



Эволюция форензик-экспертизы

Deloitte.



Эволюция форензик-экспертизы

Совмещение возможностей человеческого и искусственного интеллекта

Схемы мошенничества появляются, распространяются и видоизменяются с молниеносной скоростью, чему способствуют развитие технологий, амбиции и изобретательность мошенников. Очевидная проблема, с которой организации сталкиваются при обнаружении, расследовании и борьбе с мошенничеством, заключается в том, что мошенников больше, чем компаний. Одно только внутреннее мошенничество обходится рядовой организации в 5% годового дохода[1]. Что касается внешнего мира, так он просто кишит мошенниками, достаточно талантливыми и мотивированными, чтобы представлять опасность, причем некоторые из них обладают лишь возможностью подключения и компьютером.

Один из шагов, который организации могут предпринять для более эффективного выявления и расследования атак, а также для их предотвращения в будущем — это объединить искусственный интеллект (ИИ), компьютерное осмысление и статистические концепции когнитивной аналитики с профессиональным расследованием мотивов и методов мошенников. Такой подход поможет следователям быстрее добраться до сути проблемы и определить основную причину инцидентов, чтобы улучшить свои возможности обнаружения и предотвратить повторные эпизоды. Интегрированный метод, основанный на аналитике – это будущее расследований и управления рисками мошенничества для многих организаций.

Текущие проблемы расследования мошенничества

Защита данных, интеллектуальной собственности и финансов становится всё более приоритетной задачей на уровне совета директоров, поскольку число мошенников увеличивается и они постоянно приспосабливаются к совершенствуемым средствам контроля и мониторинга. И хотя к безграничной преступной изобретательности восприимчивы большинство организаций, те, у кого отсутствуют меры по борьбе с мошенничеством, предсказуемо находятся в худшем положении и несут в два раза большие потери от мошенничества, чем те потери, что в среднем фиксируют компании, имеющие средства контроля.[2]

[1] "The Staggering Cost of Fraud" 2016 Global Fraud Study, Association of Certified Fraud Examiners (ACFE)

[2] Ibid.

Тем не менее, даже в организациях, где предусмотрены меры по борьбе с мошенничеством, расследованиям могут помешать несколько факторов.

Основной причиной является доверие к тестированию на основе правил. Тесты на основе правил обычно оценивают и отслеживают риски мошенничества по одному набору данных, давая только ответ «да» или «нет».

Следователи сканируют данные на наличие потенциальных триггеров мошенничества, таких как платежи, превышающие пороговые значения, или долларовые транзакции в круглых числах. Помимо того, что возникают многочисленные ложные срабатывания, этот подход не оправдывает ожиданий в других отношениях. Например, прямой анализ кредиторской задолженности может выявить сомнительный прямой платеж. Однако он может пропустить сложные схемы, действующие на более низких уровнях финансовой структуры, которые требуют расширенного анализа таких факторов, как размер прибыли или данные о местоположении.

Разрозненные хранилища информации еще больше препятствуют проведению расследований с помощью аналитики. Организации часто пытаются балансировать между потребностью в локально адаптированных процессах и потенциальными преимуществами интегрированного обмена данными, в результате непреднамеренно создавая препятствия для проведения расследований. Компания, изучающая потенциальное мошенничество сотрудников, может анализировать отчеты о времени и расходах, но не замечать подсказки, содержащиеся в данных турагентов или в общедоступных социальных сетях.

Анализ данных турагента поможет определить, совершал ли сотрудник поездки, в отношении которых не было заявлено никаких расходов и которые потенциально были оплачены из вневедомственного фонда. Анализ социальных сетей может выявить настоящие действия в поездке или отношения с внешними сторонами, которые могут объяснить определенные транзакции.

Дополнительные наборы данных позволяют получить более содержательную информацию с помощью корреляций, которые можно провести.

Еще одна проблема — огромные, растущие объемы неструктурированных данных, накапливаемых в организациях, таких как видео, изображения, электронные письма и текстовые файлы. Хотя такие данные потенциально бесценны, к ним трудно получить доступ с помощью традиционных подходов и инструментов расследования, а тем более интегрировать и анализировать с помощью структурированных наборов данных.

Наконец, команды внутреннего аудита и комплаенс часто проигрывают в войнах с мошенничеством. Они полагаются на ручные процессы и специальный анализ данных, что требует значительных затрат денежных средств и времени. Им также часто не хватает штатных аналитиков, обладающих навыками следственной работы.

Путь к интегрированным расследованиям мошенничества на основе аналитики

Традиционная аналитика мошенничества — это форма расследования, основанная на интуиции. Аналитики формируют такие вопросы, используя тесты или правила, которые они создают на основе своих отраслевых знаний и опыта. Недостатки такого подхода можно увидеть на простом примере анализа дарительной активности клиентов в том или ином регионе. Создание тестов на мошенничество для потенциальных типов подарков может потребовать разработки десятков конкретных запросов, и даже тогда некоторые из них могут быть пропущены.

В противоположность вышесказанному, когнитивный метод анализа данных начинается с изучения транзакций для выявления ненормальных покупок подарков. При таком подходе сами данные подсказывают исследователям, где искать проблемы, в отличие от интуитивно направляемого расследования и, где во главе угла – опыт и знания экспертов. Вместо того, чтобы составлять десятки запросов, следователи могут применить свои навыки и опыт расследователей, чтобы изучить суженный набор приобретаемых предметов и выявить те немногие, которые требуют внимания. Такой подход сэкономит значительное количество времени и позволит заострить внимание на потенциально неблагоприятной деятельности. Это также сократит число ошибок и обеспечит более тщательный анализ — машина не пропускает тенденцию, которую часто может не заметить пара усталых глаз. Кроме того, выявление отклонений с помощью данных поможет написать более совершенные правила для поиска ненормативных значений и изучения причин их отклонения от нормы, что

Комплексный подход к расследованию мошенничества на основе анализа данных имеет несколько ключевых аспектов:

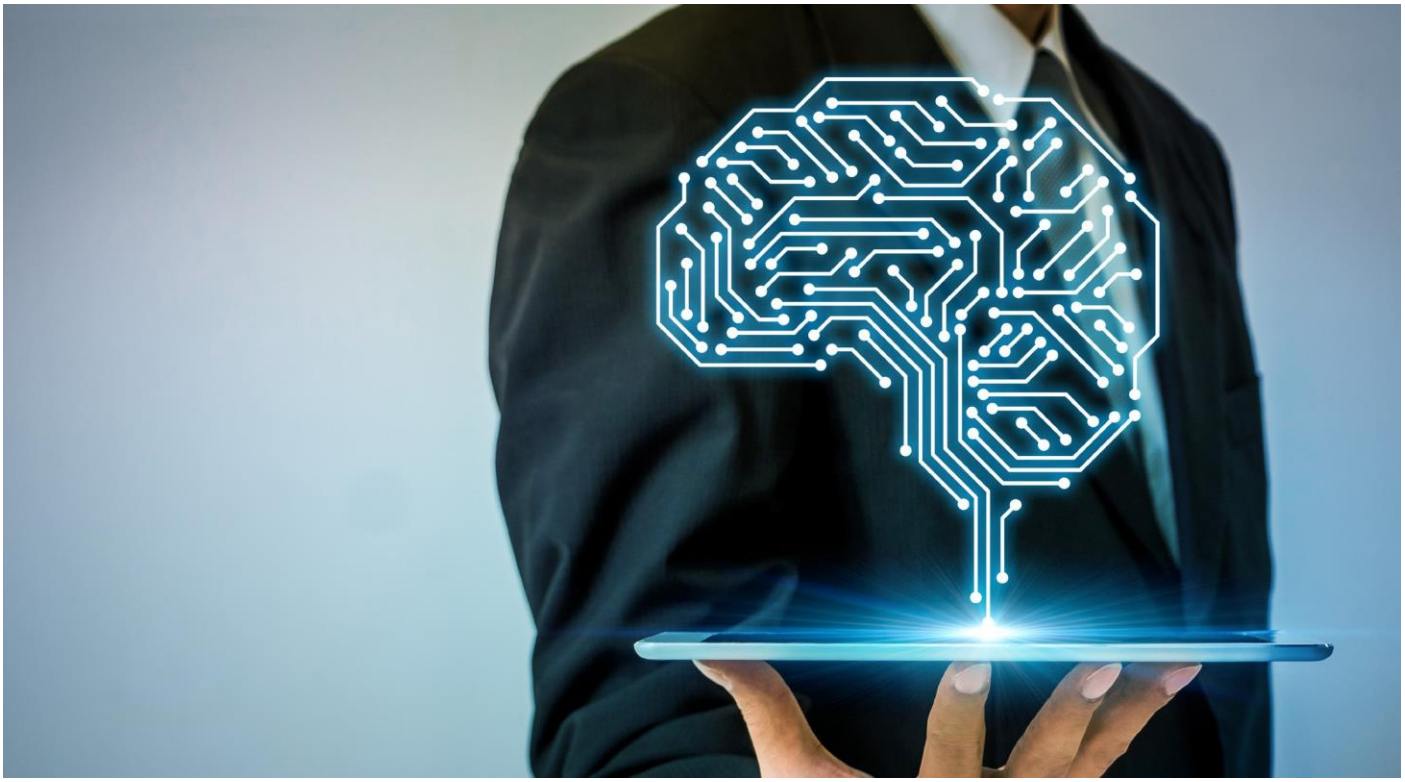
- **Высокий уровень аналитики.** Способность проводить расследование, анализируя данные, начинается с определения зрелости (развитости) организации - людей, процессов и инструментов анализа мошенничества и форензик-экспертизы. Факторы, влияющие на зрелость аналитики – это частота проведения анализа, типы используемых аналитических инструментов, а также то, проводится ли анализ изолированно или в комплексе, в рамках всего предприятия. При оценке аналитических возможностей важным фактором является значение, которое разные бизнес-подразделения придают аналитике в организации. Такие функции, как маркетинг, управление клиентским опытом и цепочка поставок, которые обычно сильны в аналитике, могут быть источниками помощи и ресурсов для расширения аналитических возможностей в рамках расследования.
- **Интегрированные витрины данных.** Возможность интегрировать структурированные и неструктурированные данные из внутренних и внешних источников в модели риска имеет основополагающее значение для расширенного анализа. Как упоминалось ранее, структурированные данные сами по себе дают весьма ограниченное представление о схемах, которые могут указывать на мошенническую деятельность. Точно так же, когда данные доступны только в разрозненных хранилищах внутри организации, связи между схемами могут быть скрыты. Интегрированный подход объединяет структурированные и неструктурированные данные по всему предприятию, а также данные из внешних источников, таких как списки особого контроля и социальные сети, чтобы представить более широкую картину действий и транзакций, которую опытные следователи, с помощью расширенной аналитики, могут собрать воедино с меньшим количеством ложных срабатываний.
- **Оценка риска всей организации, а не одной транзакции.** Сделки не совершают мошенничества. Это делают сотрудники, поставщики, клиенты и другие лица. Модели расширенной аналитики на основе данных, включающие текстовую аналитику и сетевой анализ, позволяют организациям ранжировать риски на уровне отдельных лиц или организаций, а не на уровне транзакций. Такой подход, основанный скорее на статистике, а не произвольном ранжировании рисков, может дать более широкую картину происходящего, чем анализ, проводимый по принципу «тест за тестом». Вместо того, чтобы субъективно присваивать оценки риска, позвольте данным «говорить». Это может повысить точность и эффективность ранжирования.
- **Применение прогностических инструментов.** Такие методы расширенной аналитики, как компьютерное осмысление и когнитивные вычисления, позволяют изучать транзакции, связанные со злоумышленниками. Понимание атрибутов мошенника, полученное в результате этого анализа и подкрепленное знаниями и опытом форензик-экспертов, может использоваться для «обучения» моделей, которые идентифицируют людей или организации, демонстрирующие те же или похожие черты в более широкой популяции. Искусственный интеллект и компьютерные программы имеют первостепенное значение при обнаружении цифрового следа, оставленного мошенниками.

Развитие этой практики – важный шаг для перехода к упреждающей аналитике мошенничества. На смену команде, работающей по принципу «человек против машины» придет команда с принципом «человек плюс машина».

Раскрытие неизвестного, объединив аналитику и криминалистику

Как организация определяет, была ли она обманутой и не продолжается ли этом сейчас? Происходили ли мошеннические транзакции и другие неправомерные действия «под носом» у внутреннего аудита, сотрудников службы комплаенс и юридического отдела? Были ли обнаружены отдельные случаи мошенничества без дальнейшего расследования, призванного определить, удалось ли решить проблему?

Судя по постоянно растущим аппетитам и возможностям мошенников, ответить на эти вопросы, вероятно, будет всё сложнее. Применяя передовую аналитическую практику в сочетании с проверенными на практике методами форензик- экспертизы, организации смогут более успешно обнаруживать, изолировать и предотвращать мошенничество, а это в большой степени пойдет на благо деятельности и эффективности организации.



Наши контакты

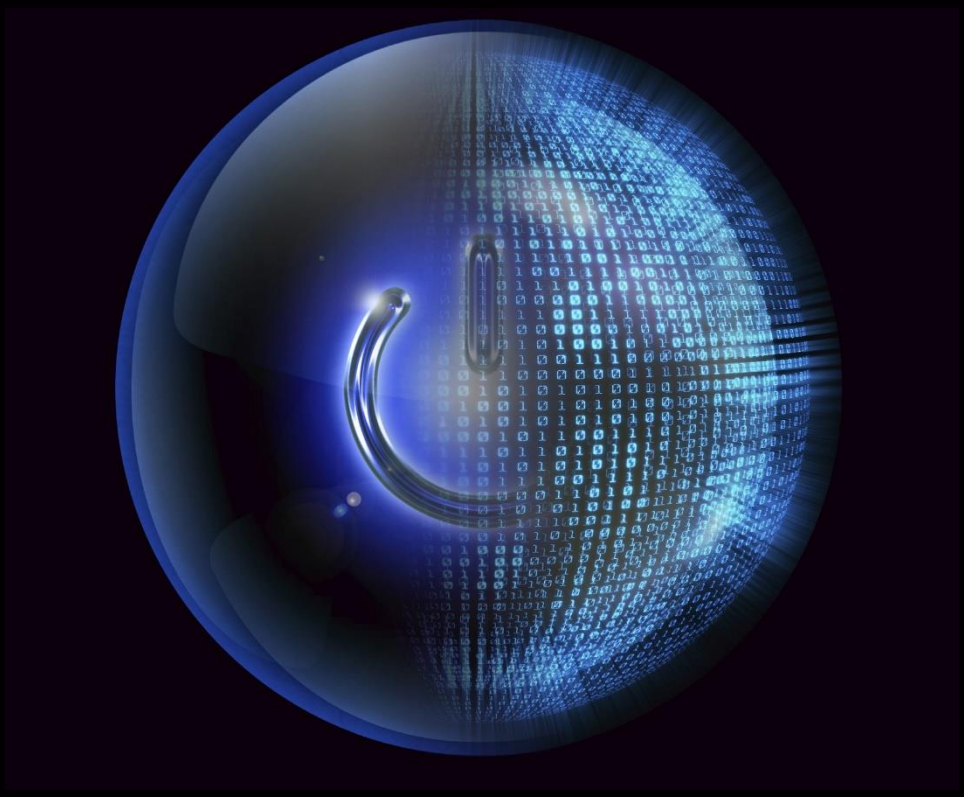
Дон Фанчер
Лидер глобальной практики | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 770 265 9290
dfancher@deloitte.com

Эд Риал
Директор| Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 212 436 5809
erial@deloitte.com

Сатиш Лалчанд
Директор | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Шуба Баласубраманьян
Директор| Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com

Deloitte.



Преодоление проблем с данными в форензик-расследованиях

Основа для интеграции человеческого и искусственного интеллекта

Традиционные меры компаний по борьбе с мошенничеством быстро теряют актуальность, поскольку частота и изобретательность мошеннических схем продолжает расти. Внутренние и внешние преступники используют множество уловок – мошенничество с закупками, мошенничество с расходами сотрудников, мошенничество с финансовой отчетностью, взяточничество и незаконное присвоение активов, таких как интеллектуальная собственность, кража данных.

Одни только эти угрозы побуждают компании рассматривать новые подходы к программам борьбы с мошенничеством и управления корпоративными рисками. А обеспечение соблюдения требований (комплаенс) еще больше повышает ставки.

Регулирующие органы всё больше ожидают от компаний контроля для предотвращения проблем, связанных с мошенничеством, включая рекомендации FINRA, соблюдение Закона о борьбе с коррупцией за рубежом (FCPA), требования Сарбейнса-Оксли и другие требования.

Как обсуждалось в более ранней точке зрения «Делойт», эволюция управления рисками мошенничества и криминалистических расследований включает анализ транзакций и данных с использованием информации, полученной в результате интеграции человеческого и машинного интеллекта, для усовершенствования борьбы с мошенничеством.

Организации разных отраслей и сами регулирующие органы начинают использовать интегрированные методы анализа данных для выявления потенциально мошеннических транзакций. Те, кто этого не сделает, могут быстро отстать и столкнуться с растущими финансовыми, репутационными, юридическими и нормативными рисками.

Одним из основополагающих факторов, который сильно влияет на ценность и эффективность аналитики и мониторинга, являются сами данные — насколько они хороши и насколько хорошо они используются. Данные могут как поддержать, так и завести в тупик криминалистические расследования, основанные на аналитике.

Проблем с данными предостаточно

К пробелам и недостаткам в мониторинге мошенничества и проведении расследования может привести множество факторов.

Огромные объемы данных. В настоящее время компании с помощью электронных средств собирают, обрабатывают и хранят больше информации, чем можно было представить даже 10 лет назад. И хотя рост объема данных впечатляет, еще более впечатляет растущее разнообразие источников данных, генерирующих этот объем, включая личные и служебные мобильные устройства, устройства, подключенные к интернету, платформы социальных сетей… этот список можно продолжать и постоянно расширять. Сбор, управление, мониторинг и анализ данных, наиболее важных для противодействия мошенничеству, уже является сложным процессом, и в дальнейшем он будет становиться всё сложнее.

Неправильный сбор и хранение. Системы, унаследованные из прошлого, часто разрабатывались с целью сбора информации для определенной цели, поэтому доступных данных может быть недостаточно для полноценного анализа. Например, временные метки транзакций и личности сотрудников, выполняющих транзакции, могут не сохраняться. В некоторых случаях доступны только текущие данные, а прошлая информация, имеющая решающее значение для криминалистической аналитики, может не сохраняться. Эти проблемы могут усугубляться, если системы не обновляются регулярно и для анализа не предоставляется дополнительная информация.

Ограниченный доступ к данным. В компании с децентрализованными операциями и источниками данных, разделенными по географическому признаку и отделам, может не хватать главной системы для глобальной консолидации данных, что препятствует взаимной корреляции. Крупные глобальные расследования могут охватывать несколько стран, каждая из которых поддерживает свою финансовую отчетность или систему управления предприятием, что затрудняет извлечение и анализ данных. Требования конфиденциальности и защиты данных в тех или иных юрисдикциях также ограничивать доступ.

Недостаточный набор навыков для обработки и анализа больших данных. Когда объемы данных невелики, базовых аналитических навыков и программ для работы с электронными таблицами бывает достаточно для проведения предварительного анализа структурированных данных из корпоративных систем и других программных приложений, а также неструктурированных данных, таких как электронные письма, тексты и голосовые записи. Но когда этот объем исчисляется миллионами, для анализа могут потребоваться технологии, расширенная аналитика и навыки форензик-экспертизы, которые недоступны во многих организациях. Могут требоваться значительные инвестиции в технологии и обучение, необходимые для соответствующего уровня мониторинга в отношении мошенничества.

Статическая отчетность, разработанная для обычного бизнеса. Юридические отделы, комплаенс-специалисты и службы внутреннего аудита могут столкнуться с препятствиями при сборе данных из таких источников, как отделы финансов, ИТ, закупок и продаж. Стандартные отчеты этих групп могут содержать ограниченную информацию. Так, если говорить о закупках, идентифицирующая информация, такая как контактное имя поставщика, адрес и номер телефона, может отсутствовать в стандартном отчете поставщика, а это ограничивает возможность сравнения контактной информации поставщика с данными сотрудников для потенциального определения совпадений. Часто при разработке отчетов плохо задавались параметры. Или, возможно, они были созданы много лет назад, когда типы информации, которые могут понадобиться следователям или службе комплаенс сегодня, даже не рассматривались.

Отсутствие разнообразных данных для корреляции полученных результатов. Компании, возможно, неполноценно исследуют внешние источники данных, такие как сторонние базы отчетов третьих сторон и социальные сети, что могло бы дать всестороннее представление о риске мошенничества, связанном с цепочкой поставок компании, каналом продаж и сотрудниками.

Любая из этих проблем в отдельности тормозит усилия сотрудников юридического отдела или практики комплаенс по применению компьютерного осмысления и когнитивной аналитики. В совокупности же они представляют собой серьезное препятствие и должны быть устранены при переходе к использованию передовых возможностей искусственного интеллекта в интересах более эффективного выявления мошенничества и его предотвращения.

Анализ данных для управления рисками мошенничества

Организации могут предпринять несколько шагов, чтобы подготовить эффективную основу для аналитических расследований и мониторинга мошенничества.

Привлекайте заинтересованные стороны к разработке плана трансформации. Те или иные отделы компании могут быть подготовлены для того, чтобы взять на себя аналитику и управление рисками мошенничества, хотя и другие отделы тоже должны нацелены на эту работу в будущем. Внутренний аудит, команды юристов и комплаенс, ИТ и бизнес-подразделения могут быть привлечены к аналитической работе и заинтересованы в ней.
Обсуждения с соответствующими заинтересованными сторонами могут выявить возможности сотрудничества и способы использования технологий, уже применяемых в других подразделениях организации. Кроме того, заинтересованные стороны помогут определить области высокого риска, требующие особого внимания, такие как отчеты о времени и расходах, управление поставщиками и платежи третьим лицам (см. «С чего начать»). Поддерживая связь на протяжении всей аналитической работы, специалисты по данным могут быть в курсе меняющихся потребностей бизнеса, а бизнес-пользователи могут понять, как данные хранятся, становятся доступны и как их защитить.

Централизуйте как можно больше данных для контроля мошенничества. Централизация всех корпоративных данных могла бы стать Святым Граалем в борьбе с мошенничеством, однако сегодня это нереалистично во многих организациях из-за разрозненных источников данных, различного географического расположения и пробелов в системной интеграции. Тем не менее, необходимо сделать акцент на объединении как можно большего количества данных – это обеспечит их целостность, согласованность и контроль, а также пойдет на пользу мониторингу и анализу мошенничества. Хорошей отправной точкой было бы рассмотрение требований и возможных препятствий для получения данных из разных отделов и географических регионов.

Установите безопасный, структурированный доступ к данным. Служба комплаенс, планирующая проводить аналитику, может извлечь пользу, заранее определив, как будут обрабатываться данные, где они будут храниться и кому будет разрешен доступ к ним. Среди факторов, которые необходимо учитывать – необходимые меры защиты от нарушений, а также политики и процедуры обработки личной информации и других конфиденциальных данных.

Привлеките соответствующие внешние данные. Внешние данные могут быть перенесены в централизованное хранилище для взаимной корреляции с внутренними данными.

Начните закладывать прочный технологический фундамент. Важно планировать инвестиции в технологии и программные приложения, которые осуществляют эффективный сбор и анализ данных для мониторинга мошенничества, и использовать одни и те же данные для различных целей. Технология должна позволять включать в анализ как структурированные, так и неструктурированные корпоративные данные.

Более качественные данные, расширенные криминалистические расследования и управление рисками мошенничества

Успех программы управления рисками мошенничества, основанной на аналитике, зависит от наличия и доступности точных, актуальных и подробных данных из/от разных географических мест, линий обслуживания, продуктов и внешних источников данных. Как упоминалось ранее, оптимальным было бы централизованное хранилище данных в масштабе всего предприятия, но в его отсутствие компании все же могут значительно улучшить свой мониторинг мошенничества и форензик-экспертизу, рассмотрев следующие вопросы:

- Какова стратегия управления продолжающимся ростом объема данных?
- Какой тип аналитических ресурсов соответствует специфике организации?
- Могут ли инструменты или идеи служить нескольким целям в организации?
- Каковы ключевые технологические тенденции в отрасли и как план трансформации организации позволит ей опережать отрасль?

Переход к программе, основанной на аналитике, включая ответы на эти вопросы, вероятно, потребует значительного времени и усилий. Как это обычно бывает при внедрении новой технологии, полезной отправной точкой может стать пилотная программа, использующая методологию *тестирование/ подтверждение/ внедрение/ масштабирование/ повторение*. Сосредоточение внимания на первых результатах и при этом понимание общей картины помогут компаниям справиться с будущими рисками мошенничества.

С чего начать

Попросите специалиста по рискам и комплаенс определить риски мошенничества, которые были бы лучшими мишенями для передовых методов аналитики, таких как компьютерное осмысление и когнитивные вычисления. Вы наверняка услышите о десятках таких угроз.

Одна команда по управлению рисками знала – чтобы обеспечить финансирование для широкого развертывания бизнеса, ей придется продемонстрировать окупаемость инвестиций в аналитику. Она составила список из более чем 100 областей риска и выбрала три, с которых можно начать анализ. Продемонстрированная ценность этой инициативы способствовала распространению аналитической деятельности на другие риски. Какой урок можно извлечь из этого? Начинайте с малого, выбирайте с умом, обуславливайте ценность того, чем вы занимаетесь.

Наши контакты

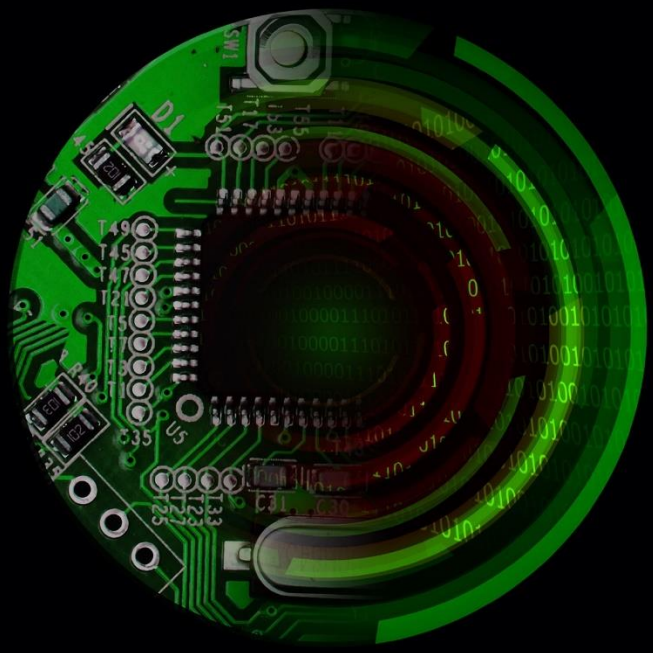
Дон Фанчер
Лидер глобальной практики |Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 770 265 9290
dfancher@deloitte.com

Сатиш Лалчанд
Директор | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Эд Риал
Директор | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 212 436 5809
erial@deloitte.com

Шуба Баласубраманьян
Директор | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com

Deloitte.



Преодоление технологических проблем в аналитических расследованиях

Создание механизма интеграции человеческого и машинного интеллекта

Мошенничество может быть простым, как, например, намеренное совершение двойного платежа. Оно может быть очень изощренным, поскольку мошенники разыгрывают хитроумную игру, состоящую из переплетенных транзакций и махинаций третьих лиц. Какой бы хитрой ни была схема, мошенничество постоянно истощает активы организации и угрожает средствам к существованию людей. И пока мошенники расширяют свой репертуар, организации в разных отраслях начинают использовать интегрированные методы анализа данных для выявления потенциально мошеннических транзакций.

В недавних публикациях «Делойт» обсуждалось, как анализ данных о транзакциях может улучшить возможности борьбы с мошенничеством, а также как использование и качество данных способствуют получению аналитических результатов. Технологии аналитики, используемые для извлечения данных и реализации их ценности, являются не менее важным фактором, который создает свои собственные проблемы. Юридические и комплаенс-команды могут более эффективно применять и интегрировать технологии, понимая эти препятствия и применяя стратегии их устранения.

Технологические проблемы в расследовании мошенничества

Расширенная аналитика проникает в расследования мошенничества, но это еще только начало пути. Юридические и комплаенс-команды продолжают использовать различные устаревшие системы для проведения проверок с большим объемом данных. Как правило, аналитические методы реализуются на специальных предприятиях и обычно используются продавцами. Инструменты все еще недостаточно развиты, что усложняет долгосрочное планирование и инвестиции.

Команда юристов или комплаенс-специалистов, стремящаяся улучшить свои возможности аналитики в противодействии мошенничеству, может столкнуться с рядом проблем.

Существующая технология может быть неполноценной, и заменить ее непросто. Расширенная аналитика всё больше прокладывает себе дорогу, но технологии, которые сейчас используются юристами и комплаенс-специалистами, как правило, не соответствуют этому тренду. Существующие инструменты часто не согласуются с возникающими бизнес-проблемами, которые стоят на повестке у этих сотрудников, такими как реагирование на новые нормативные требования или общеотраслевые риски. Для обработки результатов анализов аналитикам может не хватать интуитивных способов, таких как визуализация. Создание большого количества трудно настраиваемых предупреждений и правил для мониторинга, чем широко пользуется служба комплаенс, отнимает у аналитиков слишком много времени и усилий.

Между тем, технологии, которые могли бы более эффективно решать бизнес-задачи, быстро развиваются. Стремительно растет число поставщиков и технологических решений, как специфичных для аналитики мошенничества, так и более широкого профиля, и это затрудняет выбор. Часто отделы юридического и комплаенс-профиля в конечном итоге покупают инструменты, ожидая при этом их скорого устаревания, что приведет к очередному раунду расходов на их обновление.

Текущие операционные структуры (пока) не соответствуют инструментам. Приобретение новых инструментов аналитики — это отправная точка, а не цель. Решение о том, как юридический и комплаенс-персонал будет использовать инструменты, требует дополнительных затрат времени и ресурсов на разработку вариантов использования и преобразование данных. Универсальность приобретенных инструментов для использования юристами и комплаенс-службой, а также такие инструменты, как программное обеспечение для визуализации, которое планируется использовать в других отделах компании – всё это возможные проблемы для организаций, которые пытаются управлять различными бизнес-подразделениями и имеют дело с очень разными географическими регионами.

Специалисты по расследованию могут не знать, как использовать новые технологии, или могут противиться их использованию. Компании нередко приобретают аналитические инструменты или другие ИТ-системы с аналитическими возможностями, такие как клиентские приложения для маркетинга, облачные системы электронной почты или даже инструменты налоговых технологий. Тем не менее, юридический и комплаенс-персонал часто не знаком с данными и функциями, доступными в этих инструментах. Даже если они знают, как их использовать, как это часто бывает с инструментами электронного обнаружения, им часто мешают хранилища данных организации. Люди, у которых был плохой опыт работы с технологиями, предпочитают прочесывать бумагу, а не довериться технологии. Простота использования и конфигурация приложения – по-прежнему нелегкая задача, особенно когда компании пытаются еще больше объединить аналитиков данных, владельцев бизнеса, юристов и комплаенс-специалистов с операционными подразделениями бизнеса.

Аутсорсинг может «запереть» организацию в технологическом решении поставщика. Технологии анализа мошенничества должны быть гибкими, чтобы реагировать на сигналы осведомителей или угрозы в течение нескольких дней или недель, а не месяцев или дольше. Передача функций проектирования, разработки и внедрения инструмента исключительно поставщику, который плохо понимает потребности организации, может увеличить стоимость технологии и непрозрачность изменений в ней, эксплуатационные расходы.

Ключи к лучшей технологии противодействия мошенничеству

Технологические проблемы не присущи конкретно юристам и комплаенс-специалистам. Ведь каждому технологическому управлению в той или иной организации, вероятно, приходилось сталкиваться с такими универсальными проблемами и преодолевать их. Успешное преодоление становится возможным в более широкой экосистеме стратегий, процессов, людей и данных. Стратегия определяет бизнес-задачу, которую необходимо решить. Люди внедряют и запускают технологическое решение. Процесс включает в себя этапы решения проблемы. Данные информируют о действиях в экосистеме.

Стратегия. Стратегия согласовывает инвестиции в технологии с ключевыми приоритетами юридического отдела и комплаенс-службы. Продумывание динамики угроз мошенничества и способов реагирования на них может иметь неоценимое значение при разработке технологического плана и механизмов тестирования технологии перед ее приобретением. Обычная практика включает проверку действенности концепции, основываясь на новом риске, пробеле в нормативно-правовом регулировании или недавних отраслевых проблемах. В зависимости от результатов, новые долгосрочные решения могут наращиваться с течением времени. Инициативу должно продвигать бизнес-подразделение, которое будет использовать технологию.

Люди. Простота и удобство использования новой технологии помогает той роли, которую юристы, комплаенс-специалисты и другие заинтересованные стороны бизнеса будут играть во внедрении и развертывании аналитики. Затронутое риском бизнес-подразделение берет на себя ведущую роль, другие же заинтересованные стороны организации должны участвовать в определении того, кто будет использовать технологию для разработки аналитики и обзора результатов, как они будут обучаться и как будут решаться вопросы удобства использования и доступности.

Процессы. Одним из важных преимуществ аналитики является то, что она может раскрыть информацию, которая поможет улучшить повседневные бизнес-процессы. Понимание того, какие процессы нужно будет изменить и как, важно для разработки технологического плана (инженерного решения).

Слишком часто результаты форензик-экспертизы получают лишь поверхностное внимание, а затем забываются. Особое внимание следует уделить тому, как будет поддерживаться технологический продукт, включая обратную связь, которая помогает в технологических усовершенствованиях и корректировках того, как люди выполняют свою работу.

Данные. Данные необходимо анализировать и интерпретировать в контексте решаемой бизнес-задачи. Такая функция, как управление данными помогает определять и отслеживать используемые источники данных. Интеллектуальный анализ раскрывает суть с помощью таких инструментов, как прогнозная аналитика, анализ текста, оценка и настройка моделей, а также визуализация.

При том что сами юристы и комплаенс-группы могут иметь ограниченные аналитические возможности и ресурсы, те типы инструментов, что им необходимы, часто широко используются в других подразделениях их организации. Отделы маркетинга извлекают данные для сегментации и таргетирования клиентов. Группы внутреннего аудита отбирают транзакции с помощью инструментов, используемых для баз данных. Специалисты по цепочке поставок используют инструменты визуализации для управления логистикой. Юристы и комплаенс-группы могут извлечь выгоду из изучения потенциальных возможностей обмена технологиями и синергии в бизнесе; это позволит сократить расходы и эффективно использовать уже сделанные инвестиции при разработке и внедрении технологического продукта, который соответствует их области. Но им потребуется потратить время на обучение, чтобы понять и эффективно использовать эти инструменты.

Заслуживают изучения и две другие возможности. Технология разбора случаев может быть полезна для выявления системной подозрительной активности в течение более длительного периода времени, что может привести к выявлению недооцененных проблем, с которыми сталкивается компания. Роботизированная автоматизация процессов (RPA) за счет сокращения громоздких ручных процессов предоставит эффективный механизм для получения доступа к данным или достижения более эффективного пути решения.

Компоненты технологического продукта

По мере того как юристы и комплаенс-группы решают упомянутые здесь проблемы, они извлекут пользу из понимания некоторых основных компонентов интегрированной технологии для анализа данных.

Управление данными. Основной функционал включает архитектуру и защиту данных, а также политики и процедуры, связанные с их хранением. Поскольку следы мошенничества часто обнаруживаются в деталях, функционал управления данными критически важен, чтобы адекватные и точные данные были легко доступны для расследования.

Интеллектуальный анализ данных и текста. Основные функции включают обнаружение аномалий или экстремальных значений; прогнозную аналитику для выявления сходства на основе известных случаев мошенничества; поиск и анализ текста, часто с использованием решений для электронного обнаружения; оценку и настройку модели; визуализацию.

Разбор случаев. Основной функционал включает оперативные отчеты, вычисляемые метрики, аналитическую «линзу», в том числе организацию в фокусе и тенденции; гибкую регулировку требований; системный рабочий процесс; хорошо задокументированный и изложенный порядок рассмотрения вышестоящими инстанциями. Гибкость этого функционала особенно ценна при разработке нового рабочего процесса или при формировании мер в ответ на новое нормативное положение.

Роботизированная автоматизация процессов. Области, где может быть эффективно внедрена RPA, включают проверку документов, анализ клиентов и элементы комплексной проверки третьих сторон.

Понимание ценности аналитики

Юристы и комплаенс-специалисты стремятся к аналитическим выводам, и в этой связи заслуживают внимания несколько моментов. Во-первых, технология сама по себе не может решить все нормативные или криминалистические проблемы. Организации также нужна команда, которая понимает инструмент, может задавать правильные вопросы, вовлекает ключевых заинтересованных лиц и использует результаты.

Также полезно рассмотреть, что потребуется, если угроза мошенничества станет критической. Могут ли юристы или комплаенс-специалисты быстро и всесторонне отреагировать?
Насколько прозрачны системы и данные? Можно ли внести новые данные и творчески изучить их новыми способами? Может ли организация показать регулирующим органам и другим органам власти, что она использует технологии как для изучения выявленных угроз, так и для маркировки похожих, потенциально проблемных транзакций и людей?

Тщательная оценка и развертывание технологических инструментов, необходимых для борьбы с мошенничеством с помощью расширенной аналитики, помогут организациям решить эти вопросы и более эффективно бороться с мошенничеством.

Наши контакты

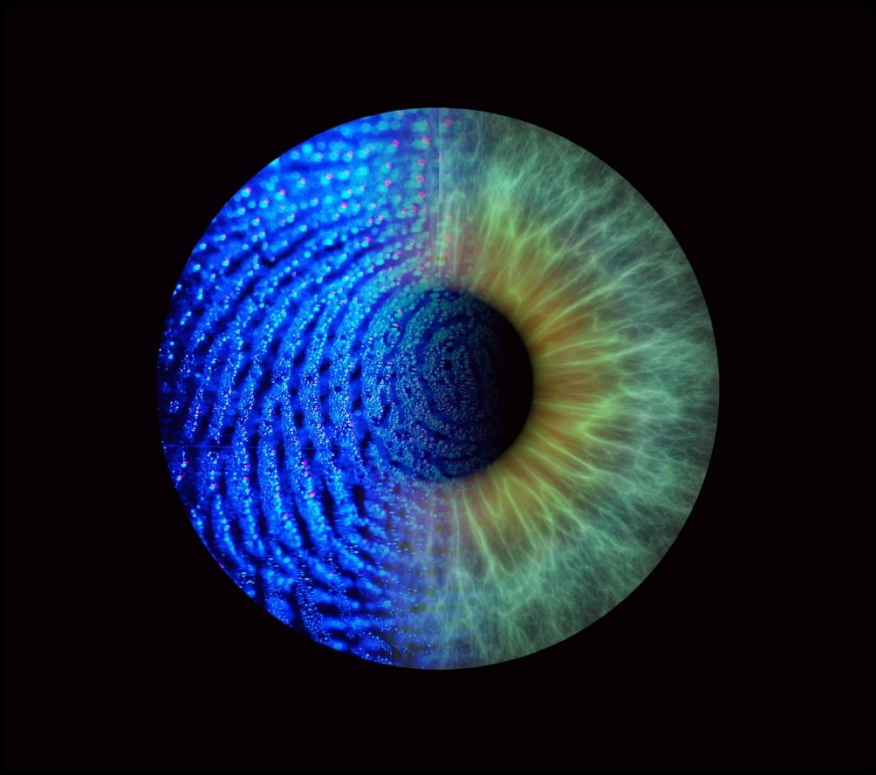
Дон Фанчер
Лидер глобальной практики
Deloitte Risk
and Financial Advisory
Deloitte Financial Advisory
Services LLP
+1 770 265 9290
dfancher@deloitte.com

Эд Риал
Директор
Deloitte Risk and
Financial Advisory
Deloitte Financial Advisory
Services LLP
+1 212 436 5809
erial@deloitte.com

Сатиш Лалчанд
Директор
Deloitte Risk
and Financial Advisory
Deloitte Transactions and
Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Шуба Баласубраманьян
Директор
Deloitte Risk and
Financial Advisory
Deloitte Financial Advisory
Services LLP
+1 469 387 3497
subalasubramanian@ deloitte.com

Deloitte.



Непрерывный мониторинг мошенничества и форензик-расследования

Признание и устранение риска быть атакованным с неожиданной стороны

Звонок осведомителя на горячую линию побуждает к расследованию мошенничества на тендере. Анализ заработной платы обнаруживает «сотрудников-призраков». Аудит поставщика указывает на возможный коммерческий сговор. Любой акт мошенничества, будь то внутренний или внешний, успешный или неудачный, заставляет организацию решать критические вопросы. Кто в этом участвует? Во что обошлась компании эта схема? Как долго это продолжается?

В недавних обзорах Deloitte обсуждались ключевые аспекты противодействия аналитике:

Проблемы в борьбе с мошенничеством

Чем дольше мошенники остаются незамеченными, тем больший финансовый ущерб они причиняют. И восстановление со временем становится все труднее. Длительность осуществления типичных схем мошенничества усиливает необходимость постоянного мониторинга для выявления угроз. Исследования показали, что более половины случаев мошенничества продолжаются как минимум 18 месяцев до обнаружения, а почти треть остается незамеченной в течение двух и более лет.

Обнаружению и предотвращению мошенничества мешают различные факторы, в том числе огромные объемы данных, недостаточные навыки криминалистической аналитики, а также затраты на необходимые технологии и обучение. Организация, которая нанимает специалистов по данным для проведения анализа мошенничества, может обнаружить, что они могут обрабатывать цифры, но им не хватает важных знаний в предметной области.

Часто борьба с мошенничеством начинается по факту случившегося, при этом ресурсы сосредоточены на преследовании преступников после инцидента в ущерб обнаружению и предотвращению. Внутренний аудит, сотрудники цепочки поставок и другие отделы могут искать факты мошенничества в своих обособленных хранилищах данных, упуская возможности для сотрудничества и обмена информацией. Риски подчас отслеживаются на основе установленных критериев и прошлых инцидентов, вместо проведения анализа данных, который учитывает потенциальные неизвестные угрозы.

Постоянно развивающиеся технологии создают другие проблемы. Распространение цифровых устройств повышает эффективность и автоматизацию, но также повышает подверженность организации риску, поскольку внутренний аудит может отставать от бизнес-подразделений в развертывании технологий и в компетенции.

Характер и возможности непрерывного мониторинга мошенничества

Непрерывный мониторинг можно рассматривать как автоматизированный процесс, который маркирует подозрительные транзакции в момент их совершения. Процесс может управляться правилами, например, выдавать оповещение каждый раз, когда транзакция превышает пороговую сумму или обрабатывается в нерабочее время.

Однако в данном контексте непрерывность – понятие относительное. Круглосуточный мониторинг в режиме реального времени может быть ненужным или бесполезным, особенно при обнаружении сложных схем мошенничества. Исследования показали, что случаи мошенничества обычно развиваются во времени. Одна транзакция может мало что значить, но мониторинг тенденции транзакций на ежемесячной, еженедельной или другой основе может говорить о многом.

Упреждающий мониторинг с использованием расширенной аналитики может помочь организациям выявлять тенденции, а также новые схемы, не основанные на известных случаях мошенничества. Вместо того, чтобы полагаться на правила, аналитика дает новые идеи, основанные на том, что показывают данные.

Внимание к нескольким соображениям поможет организации получить более ощутимую отдачу от своей деятельности по мониторингу:

Воспользуйтесь сдерживающим эффектом. Люди могут начать подчиняться правилам, когда за ними наблюдают машины или другие люди. Само существование мониторинга, о котором должным образом сообщается, может способствовать соблюдению протоколов, политик и руководств.

Делайте работу в пределах компании. Проведение мониторинга внутри организации вместо обращения к внешней стороне дает несколько преимуществ, включая безопасность данных и конфиденциальность. Данные можно более легко анализировать на постоянной основе, а штатный персонал может узнать, как работает технологический продукт и как его обслуживать. Кроме того, если в будущем технологию потребуется расширить, работа может выполняться в рамках организационной инфраструктуры и не требует дополнительного экспорта данных.

Настройте мониторинг для конкретных рисков. Разнородные организации, отрасли и местоположения могут представлять различные риски и угрозы. Могут сильно различаться форматы данных, сложность и доступность. Понимание тенденций и адаптация решений по борьбе с мошенничеством к конкретным организационным характеристикам и ситуациям с участием бизнес-подразделений поможет извлечь большую пользу из мониторинга рисков мошенничества.

Используйте имеющиеся ресурсы. Некоторые из инструментов, необходимых для проведения мониторинга, могут уже существовать в организации в таких службах, как финансы и цепочка поставок. Могут существовать возможности для использования этих инструментов в управлении рисками. Такое сотрудничество улучшит взаимодействие между подразделениями бизнеса и повысит осведомленность о мошенничестве.

Используйте разные методы. Различные риски могут потребовать различных аналитических инструментов. Неконтролируемое моделирование создает статистические профили обычных транзакций или объектов и идентифицирует значения, выходящие за пределы этих профилей. В контролируемом моделировании используются задокументированные случаи мошенничества и результаты неконтролируемого моделирования для изучения характеристик мошенничества, классификации новых наблюдаемых эпизодов как мошеннических и обнаружения того, чего не может человеческое наблюдение. Если предполагаемая схема включает сговор, может потребоваться сетевой анализ. И, если важные подсказки кроются в неструктурированном тексте, обработка естественного языка может быть ценным подспорьем.

Привлеките заинтересованные стороны. Управление рисками больше не является обязанностью только внутреннего аудита и службы комплаенс. Бизнес-подразделения и другие функции должны играть роль в понимании, выявлении и устранении рисков мошенничества.

Сосредоточьте усилия. Технологические продукты для мониторинга сложны, затрагивают разрозненные части бизнеса. Инвестиции и время, необходимые для их внедрения, могут показаться огромными. Вместо того, чтобы забрасывать широкую сеть, рассмотрите возможность проведения целенаправленной конкретной проверки концепции, чтобы понять, как работает технологический продукт и какую пользу он потенциально может принести.

Хватит гоняться за мошенниками, начните предотвращать такие случаи

Создание эффективного мониторинга мошенничества может показаться монументальной задачей, требующей значительных инвестиций, серьезной инициативы по внедрению и огромных усилий для получения необходимых данных. Пусть эта перспектива не ошеломляет вас, однако.

Начните с отказа от идеи, что требуются идеальная ситуация и точные данные. Развертывание аналитики — это лишь часть более длительного и масштабного процесса управления корпоративными рисками и обеспечения соответствия требованиям. Это критически важная часть, но, всё же, только одна.

Затем проведите оценку текущего состояния и сориентируйтесь, где находятся необходимые данные, а также инфраструктура и инструменты, доступные для осуществления непрерывного мониторинга. Затем определите цели, установите области сосредоточения внимания и расставьте приоритеты в потребностях и действиях.

При таком подходе возможности мониторинга могут итеративно улучшаться с течением времени, обеспечивая более глубокое понимание, меньшее количество ложных срабатываний и устойчивую организацию, менее уязвимую к угрозам мошенничества.

Наши контакты

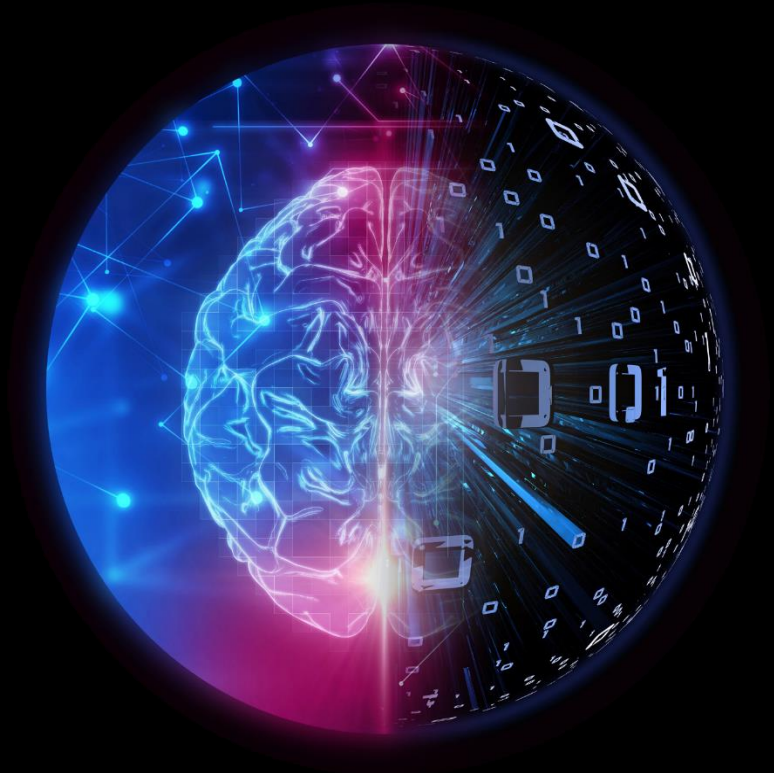
Дон Фанчер
Лидер глобальной практики | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 770 265 9290
dfancher@deloitte.com

Эд Риал
Директор| Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 212 436 5809
erial@deloitte.com

Сатиш Лалчанд
Директор | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Шуба Баласубраманьян
Директор| Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com

Deloitte.



Форензик-аналитика в расследованиях мошенничеств

Выявление редких событий, которые могут обрушить бизнес

Абстрактно «редкое событие» — это просто явление, которое происходит нечасто. В реальном мире этот сухой неологизм может привести к серьезным нарушениям и далеко идущим последствиям. Редкое событие может принять форму крупномасштабного бедствия – смертельной бури, эпидемии, финансового кризиса. Для бизнеса редким событием может быть кибератака или мошенничество сотрудников.

В качестве альтернативы, это может быть недостаток продукта, который проявляется на рынке и угрожает операциям, прибыли и бренду. Или даже неправомерные действия субподрядчика могут создать новые риски несоблюдения требований для вас и других участников цепочки поставок.

Человечество еще не придумало, как предотвратить бури, пандемии и аварии. Но предприятия используют криминалистическую аналитику и осуществляют прорывы в борьбе с редкими событиями, совершаемыми злоумышленниками, с небрежными операциями и с угрозами несоблюдения требований. Криминалистическая аналитика сочетает расширенную аналитику с судебно-бухгалтерскими и следственными методами для выявления потенциально редких событий, имеющих последствия — «игл в огромных стогах» данных и информации, которые могут сигнализировать о проблемах в процессе работы.

Криминалистическая аналитика, крайне необходимая для удовлетворения растущих нормативных и потребительских требований по предотвращению мошенничества, может выявлять сигналы о возникающих рисках на месяцы или даже годы раньше, чем это было бы возможно без нее.

Криминалистическая аналитика, которая полагается на достижения в области вычислительной мощности и управления данными, является важнейшей функцией в будущих расследованиях. В предыдущих выпусках изучались и другие аспекты аналитики в борьбе с мошенничеством – потребность в доступных и точных данных; технологии, необходимые для извлечения данных и реализации их ценности; непрерывный мониторинг транзакций и действий, процесс, который дает неоценимый вклад для криминалистического анализа.

Ресурсы форензик-аналитики

Обнаружение схем мошенничества долгое время включало поиск закономерностей в поведении, действиях, отношениях людей и движении денег. Форензик-аналитика помогает организациям выявлять и предотвращать акты мошенничества за счет интеграции анализа данных на основе искусственного интеллекта с квалифицированным расследованием мотивов и методов мошенников.

В дополнение к применению в борьбе с мошенничеством, форензик-аналитика может использоваться для решения операционных проблем, например, дать ответы на вопросы, как процессы и средства контроля организации могут создавать уязвимости, а также как они реагируют на данные о возможных проблемах. Так, один автопроизводитель обнаружил, что дефекты можно было выявить в среднем на полтора года раньше, если бы была использована криминалистическая аналитика.

Применение криминалистической аналитики в управлении рисками несколько отличается от ее использования в таких областях, как финансовое прогнозирование и определение целевой клиентуры. В последних случаях цель состоит в том, чтобы определить предсказуемые модели поведения, такие как предпочтения клиентов и покупательская активность в определенных ценовых категориях. В риск-менеджменте цель аналитики противоположна – найти активность за пределами нормы, что является гораздо более сложной задачей.

Успешному прогнозированию событий, происходящих в течение ничтожного процента времени, могут сильно мешать ложные срабатывания и напрасные усилия. Используя хорошо разработанную форензик-аналитику, организации смогли сократить

Методы, используемые для решения этих проблем, включают:

Репозиторий объединяет разрозненные источники данных, поэтому аналитические модели могут идентифицировать и консолидировать сигналы со всего предприятия. Разрозненные хранилища и многочисленные разрозненные витрины данных часто дают фрагментарное представление о потенциальных рисках. Данные могут собираться и использоваться для одной цели, будучи эффективно отделены от других источников данных. Репозиторий объединяет как внутренние, так и внешние наборы данных, обеспечивая более четкое и полное представление о рисках и связанных с ними демаскирующих признаках.

Сетевое картирование и анализ исследуют связи мошенника или целые сети, чтобы выявить других людей, совершающих аналогичные действия, а также ключевые фигуры, управляющие схемами сети сговора.

В **неконтролируемом моделировании** используются алгоритмы, которые просеивают данные без информации о предыдущих случаях рассматриваемого редкого события. Модели помогают раскрывать новые схемы мошенничества, выявляя подозрительные отклонения от нормальных моделей поведения и выявляя экстремальные значения и аномалии на детальном уровне, вплоть до идентификатора транзакции, сотрудника или кода продукта. Например, закупки в количествах, несовместимых с прошлой практикой или фактическими потребностями в закупках, могут быть признаны следствием смены поставщиков.

Контролируемое моделирование включает в себя разработку алгоритмов, которые определяют сходство между группами исторических моделей мошенничества и определяют, что отличает их от остальной совокупности данных.

Например, чтобы классифицировать прошлые случаи мошенничества по уровню риска (высокий или низкий), могут быть разработаны уравнения регрессии, древовидные схемы решений и нейронные сети. Полученный алгоритм затем можно использовать для оценки новых случаев, чтобы определить их уровень риска, отслеживать источники данных для таких случаев на постоянной основе и даже выявлять и оценивать прошлые паттерны, которые могут относиться к текущему расследованию.

Аналитика текстов и машинное распознавание образов становятся все более ценными инструментами расследования на фоне стремительного роста неструктурированных данных, включая электронную почту, обмен сообщениями, аудио и видео. Методы обработки естественного языка (NLP) могут определить, что передается в массивах таких данных, информацию, которая может опровергнуть предположительно надежные структурированные данные. Например, NLP помог одной компании обнаружить электронную таблицу, которая показывала, что конкретный товар закупался с использованием стандартного кода продукта. Однако анализ примечаний покупателя, сопровождающих заказ, показал, что в транзакцию были включены посторонние предметы, такие как телевизоры и ноутбуки.

В другом случае применения NLP использовался искусственный интеллект для просмотра аудиофайлов из контактного центра, чтобы определить, не оказывают ли агенты давления на клиентов, заставляя их покупать продукты, которые им не следует покупать. Анализ включал тон голоса агентов и уровень стресса клиентов. NLP также поможет определить незаметные связи между людьми путем анализа сходства в их комментариях.

Использование описанных выше подходов значительно улучшается за счет участия человека в процессе, что является ключевым компонентом форензик-аналитики. Опытные, знающие люди могут как проводить расследования на основе аналитики, так и предоставлять отзывы о ее полезности и эффективности, расширять возможности и охват проводимых исследований.

Рекомендации по развертыванию аналитики

При применении форензик-аналитики требуют рассмотрения несколько методов:

Тренинги и самопознание. Аналитики могут извлечь уроки из различных источников данных, таких как проблемы риска, с которыми организация сталкивалась в прошлом. Соответствующие модели могут со временем адаптироваться к будущим рискам, тем самым расширяя сферу действия и более эффективно используя ресурсы форензик.

Тестирование на ретроспективных данных. Организации могут научно протестировать эффективность криминалистической аналитики, чтобы решить, стоит ли ее использовать. Тестирование на ретроспективных данных поможет убедиться, что модели и алгоритмы распознавания повторяющихся схем работают хорошо и эффективны в поиске подозрительных закономерностей.

Итеративный подход. По мере внедрения технологии форензик-аналитики, модели можно итеративно дорабатывать, адаптировать и масштабировать, чтобы они реагировали на новые и развивающиеся схемы мошенничества и в то же время постоянно получали более широкое представление о рисках, с которыми может столкнуться предприятие. Этот подход позволяет организации создавать платформу криминалистической аналитики поэтапно, шаг за шагом, с вкладом и проверкой со стороны заинтересованных сторон, при этом оставаясь на шаг впереди злоумышленников.

Обратная связь и постоянное совершенствование. Как только технология форензик-аналитика внедрена, ее эффективность можно постоянно повышать, опираясь на отзывы по результатам каждого расследования и постоянно растущий объем знаний и идей в области судебной бухгалтерии и расследований, а также используя вклад заинтересованных сторон по всему предприятию.

Рекомендации по расширенной аналитике

Как отмечалось ранее, использовать форензик-аналитику для выявления редких событий и других рисков гораздо сложнее, чем применять аналитику для сегментации клиентов или прогнозирования спроса. Неэффективность ресурсов, проблемы безопасности, нарушения нормативных требований, нарушения патентных прав, сомнительные методы продаж, а также мошенничество, растраты и злоупотребления входят в список угроз, требующих продуманного использования аналитических ресурсов. Вот некоторые подходы и инструменты, которые следует учитывать при формулировании возможностей форензик-аналитики:

Контекстный анализ. Эффективная аналитика предполагает детальное изучение различных контекстов и использование различных инструментов.

Вероятностные баллы. Форензик-аналитика включает извлечение различных типов данных и применение различных алгоритмов и моделей для выявления схем подозрительной деятельности. Эти усилия в конечном итоге объединяются для присвоения вероятностных оценок классам-сущностям, которые помечены как потенциальные угрозы.

Многослойность. Информационные потоки могут быть расставлены по приоритетам, а аналитика может быть предназначена для сканирования различных источников данных для поиска различных проблем. Послойная аналитика данных обеспечит надежную систему безопасности, упрощая поиск подозрительных отклонений от операционных норм.

Совокупность. Набор алгоритмов, которые организация использует для изучения рисков мошенничества, в конечном итоге может быть объединен в структуру, которая оценивает и ранжирует различные транзакции и объекты на основе их относительной подозрительности и важности, помогая расставить приоритеты в расследованиях мошенничества.

Незаменимая техническая возможность

Сложность и требования современного мира вынуждают организации понимать риски, с которыми они сталкиваются, и принимать меры для защиты своей деятельности от мошенничества, расточительства, злоупотреблений и возможных санкций со стороны регулирующих органов.

Продолжают появляться новые схемы мошенничества. Регулирующие органы все больше приспосабливаются к роли форензик-аналитики в управлении рисками. Они сами используют такие инструменты для выявления недостатков в соблюдении требований и все чаще ожидают не меньшего от тех, кто находится под их надзором.

Форензик-аналитика поможет организациям найти потенциально «смертоносные» иголки в стоге сена, защитить активы, повысить конкурентоспособность, сэкономить деньги и усилить соблюдение нормативных требований.

Наши контакты

Дон Фанчер
Лидер глобальной практики | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 770 265 9290
dfancher@deloitte.com

Эд Риал
Директор| Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 212 436 5809
erial@deloitte.com

Сатиш Лалчанд
Директор | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Шуба Баласубраманьян
Директор| Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com

Deloitte.