ДиалогНаука

Система выявления мошеннических операций ДБО юридических лиц

ЗАО «ДиалогНаука»
Корольков Сергей
Технический директор

ДиалогНаука

План презентации

- Состояние дел в области безопасности ДБО
- Описание концепции защиты ДиалогНаука
- Вопросы

ДиалогНаука

План презентации

Состояние дел в области безопасности систем ДБО

ДиалогНаука

Необходимость защиты систем ДБО

- Сбербанк за первые 10 месяцев 2012 года зафиксировал в общей сложности 467 случаев хищения денежных средств со счетов клиентов в рамках дистанционно-банковского обслуживания (ДБО) на сумму более 362 миллиона рублей
- Из общего числа случаев хищения
  - 305 пришлось на счета физических лиц на сумму более 138 миллионов рублей,
  - 162 случая примерно на 224 миллиона рублей – на юридических лиц.

ДиалогНаука

Необходимость защиты систем ДБО

- Ежедневно в России фиксируется 15-20 попыток хищения денежных средств из систем дистанционного банковского обслуживания - в среднем за один раз хакеры пытаются похитить около 400 тысяч рублей
- Получили распространение все типы атак
  - хищение криптографических ключей
  - «Man in the Middle»
  - «Man in the Browser»
- USB ключи, любые СКЗИ и хранилища ключевой информации, работающие на клиентской рабочей станции не столь эффективны

ДиалогНаука

Ключевые требования к СВМО

Чего мы хотим от системы выявления мошеннических операций (далее СВМО) в первую очередь?

- Высокая эффективность выявления мошеннических операций
- Низкий процент ложных срабатываний
- Обработка в режиме реального времени или близком к нему
- Наличие функций самообучения
- Возможность проведения расследований инцидентов

ДиалогНаука

Рынок решений

- Решения бывают
  - От производителей SIEM систем
    - не учитывают российскую специфику
    - появляются дополнительные возможности за счет анализа данных системы ДБО, сетевого оборудования, web сервера и пр.
  - Специализированные системы выявления мошенничества
  - «Собственной разработки»
    - Можно получить эффективную систему
    - Главная проблема - они не продаются, нужно все делать самостоятельно
  - От производителя системы ДБО
    - зарубежные продукты обычно не учитывают российскую специфику
    - не имеют опыта разработки решений по анализу и корреляции большого количества различных событий
    - не могут работать с несколькими ДБО

ДиалогНаука

Условия внедрения СВМО

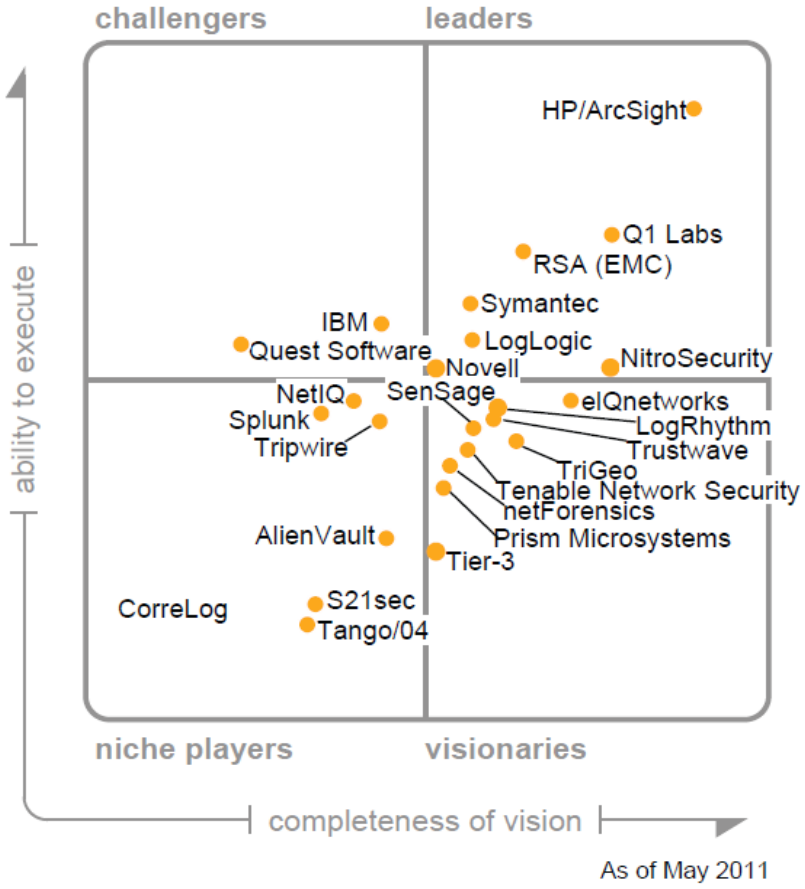
Почему мы представляем эту СВМО, а не другую?

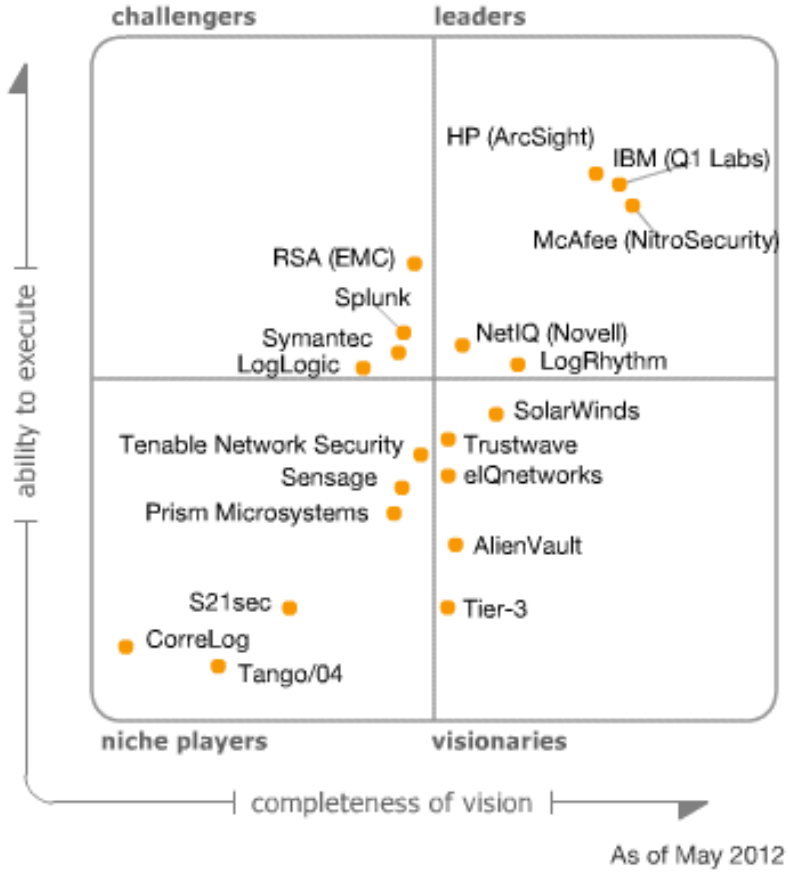
- В банке уже действует ДБО, как правило российская, и возможно не одна (филиалы Банка могут использовать разные системы)
- В Банке уже функционирует АБС
- Вероятно банк прошел сертификацию PCI DSS, а значит или имеет систему сбора и корреляции событий или хочет ее иметь

ДиалогНаука

Рынок SIEM решений

Какую систему сбора и корреляции событий банк имеет или хочет иметь?





Source: Gartner (May 2011)

ДиалогНаука

План презентации

Описание решения ДиалогНаука

ДиалогНаука

Что мы предлагаем

- Набор правил для ведущей SIEM системы Arcsight, учитывающих российскую специфику и опробованных в ряде крупных банков
- Преимущества решения:
  - Возможность интеграции с любыми ДБО и АБС, сетевым оборудованием и другими источниками для получения информации о действиях клиента ДБО
  - Неограниченные возможности производительности системы – до 3-4 тысяч транзакций в секунду
  - Наличие уже отработанных на практике наборов правил
  - Наличие огромного опыта внедрения SIEM системы и внедрения систем выявления мошеннических операций

ДиалогНаука

Концепция решения

- Система выявления мошеннических операций осуществляет анализ атрибутов каждого платежного поручения, условий в которых совершается операция, в режиме реального времени на основании данных получаемых из системы дистанционного банковского обслуживании и других систем Банка.
- На основании результатов такого анализа и в соответствии с определенными правилами, СВМО осуществляет расчет коэффициента характеризующего величину риска платежной операции.

ДиалогНаука

Концепция решения

- В общем случае, рассчитанный коэффициент риска присваивается платежному поручению в БД системы ДБО. Возможен вариант, когда указанный коэффициент присваивается платежному поручению в системе АБС, в системе СВМО или в иной системе.

- Система, осуществляющая обработку платежных операций (ДБО, АБС, иная процессинговая система) должна проводить транзакцию или отклонять ее с учетом величины риска конкретной транзакции. Иными словами, функционал АБС или ДБО должен иметь возможность отклонения транзакции при превышении коэффициента риска транзакции определенного порога.

Расчет коэффициента риска платежной операции

Расчет риска платежной операции происходит на основании анализа следующих характеристик:

- Наличие Получателя платежа в списках:
  - Атрибутов получателя «белом списке»
  - Имени получателя в «черном списке»
  - Организации получателя в «черном списке»
  - ИНН, номер счета в «черном списке»
- Тип платежа:
  - Платеж в федеральный орган
  - Внутрибанковский платеж
  - 222-П
  - Иной платеж

По этим признакам, квалифицируется большая часть операций: 70%-80% в зависимости от Банка.

«Белый» список формируется автоматически: если операция перевода определенному получателю прошла ранее и не была опротестована, то получатель автоматически попадает «белый» список.

ДиалогНаука

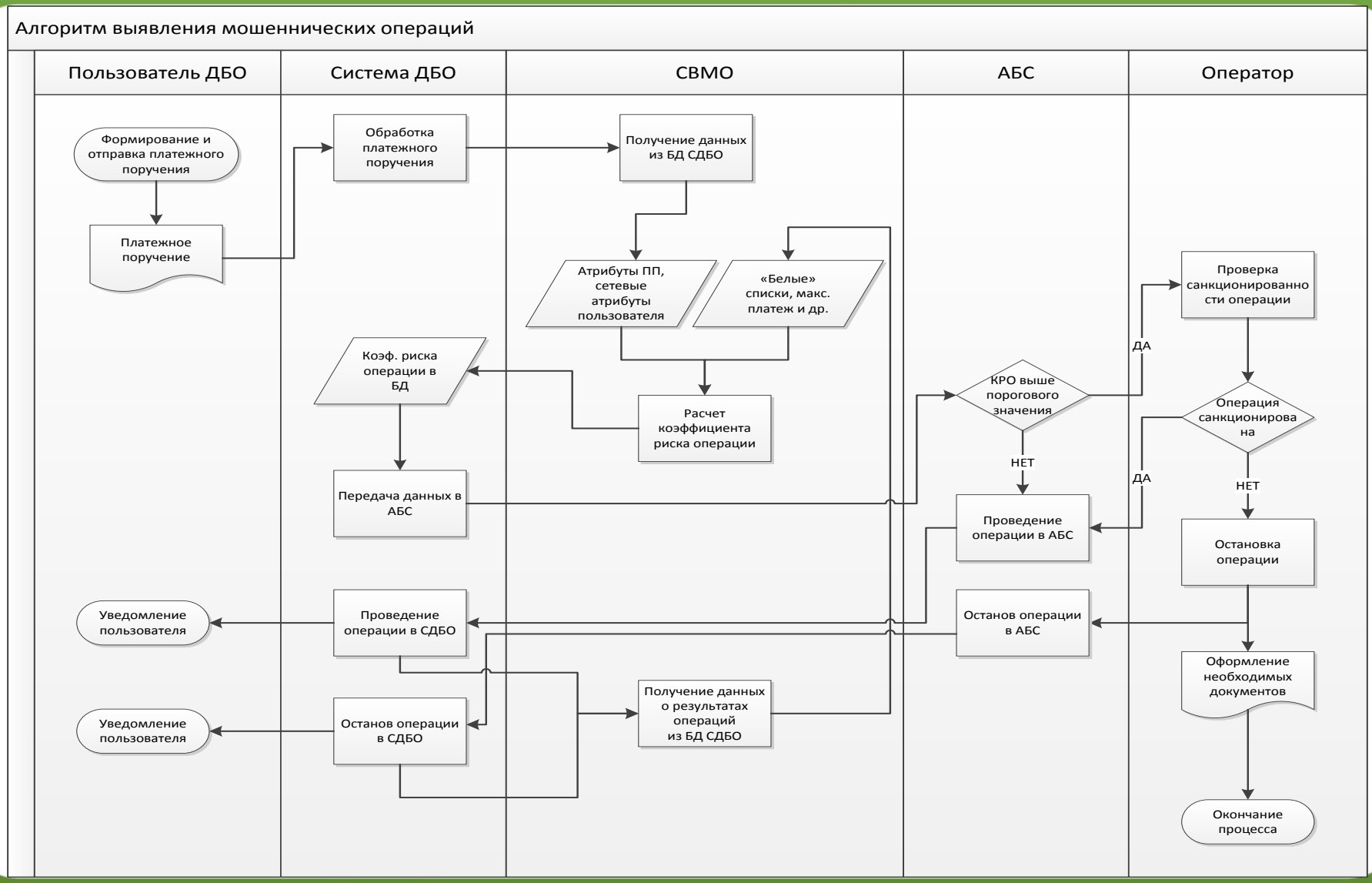
Расчет коэффициента риска платежной операции

Расчет риска платежной операции происходит на основании анализа следующих характеристик:

- Сумма платежа:
  - Низкая/средняя/высокая
  - Больше чем максимально ранее зафиксированная сумма
- Тип аутентификации и количество попыток аутентификации
- Атрибуты плательщика (в случае если доступно)
  - IP адрес (новый/старый)
  - MAC адрес (новый/старый)
- Данные об использовании сервера ДБО пользователем
  - Порядок загрузки страниц/форм системы ДБО
  - Время загрузки страниц/форм
- Время проведения транзакции
  - Типичное/нетипичное
- Другие характеристика платежа
  - Множественные транзакции на разных получателей с одинаковым назначением
  - Использование одного шаблона для разных получателей

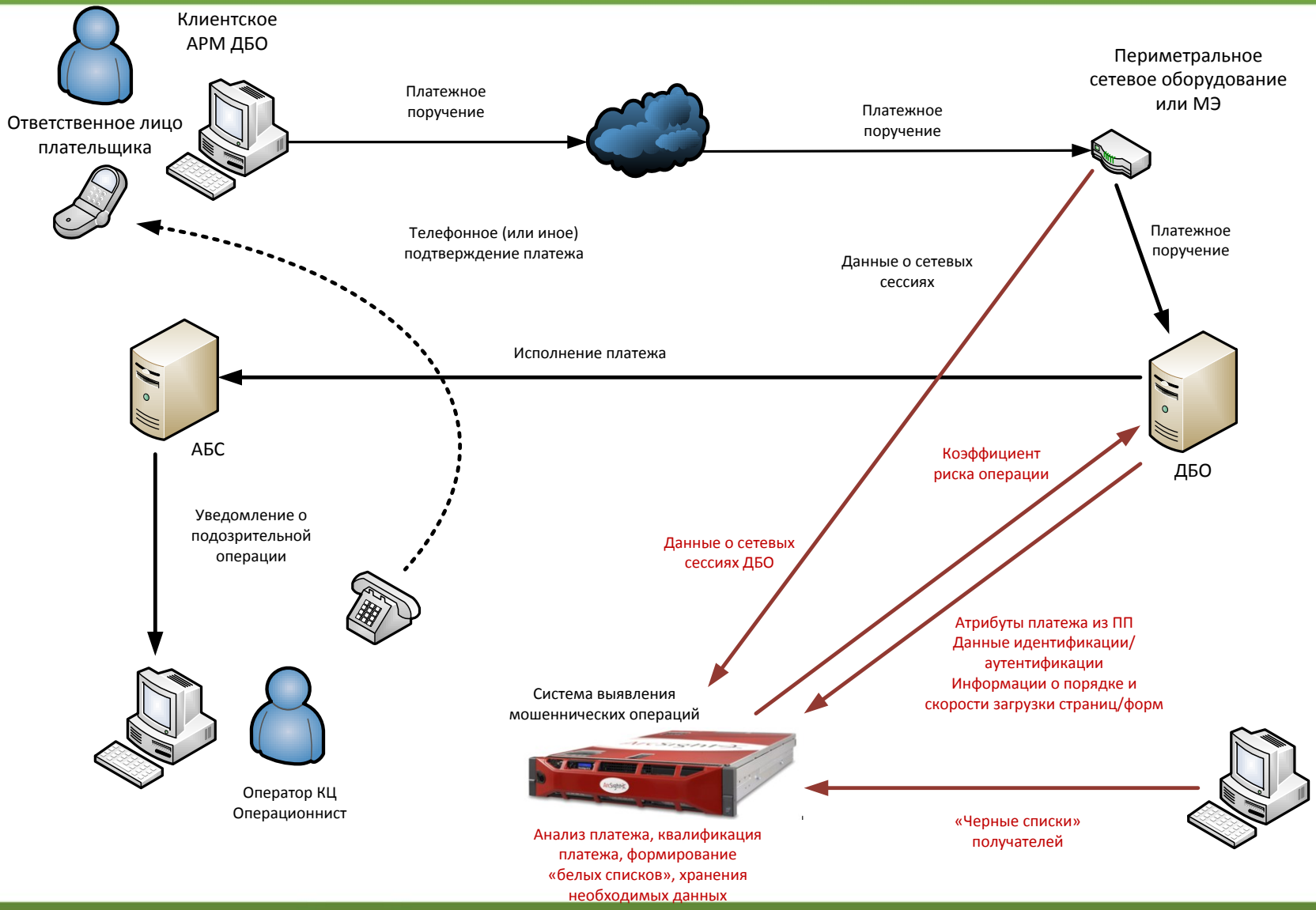
ДиалогНаука

Расчет риска платежной операции



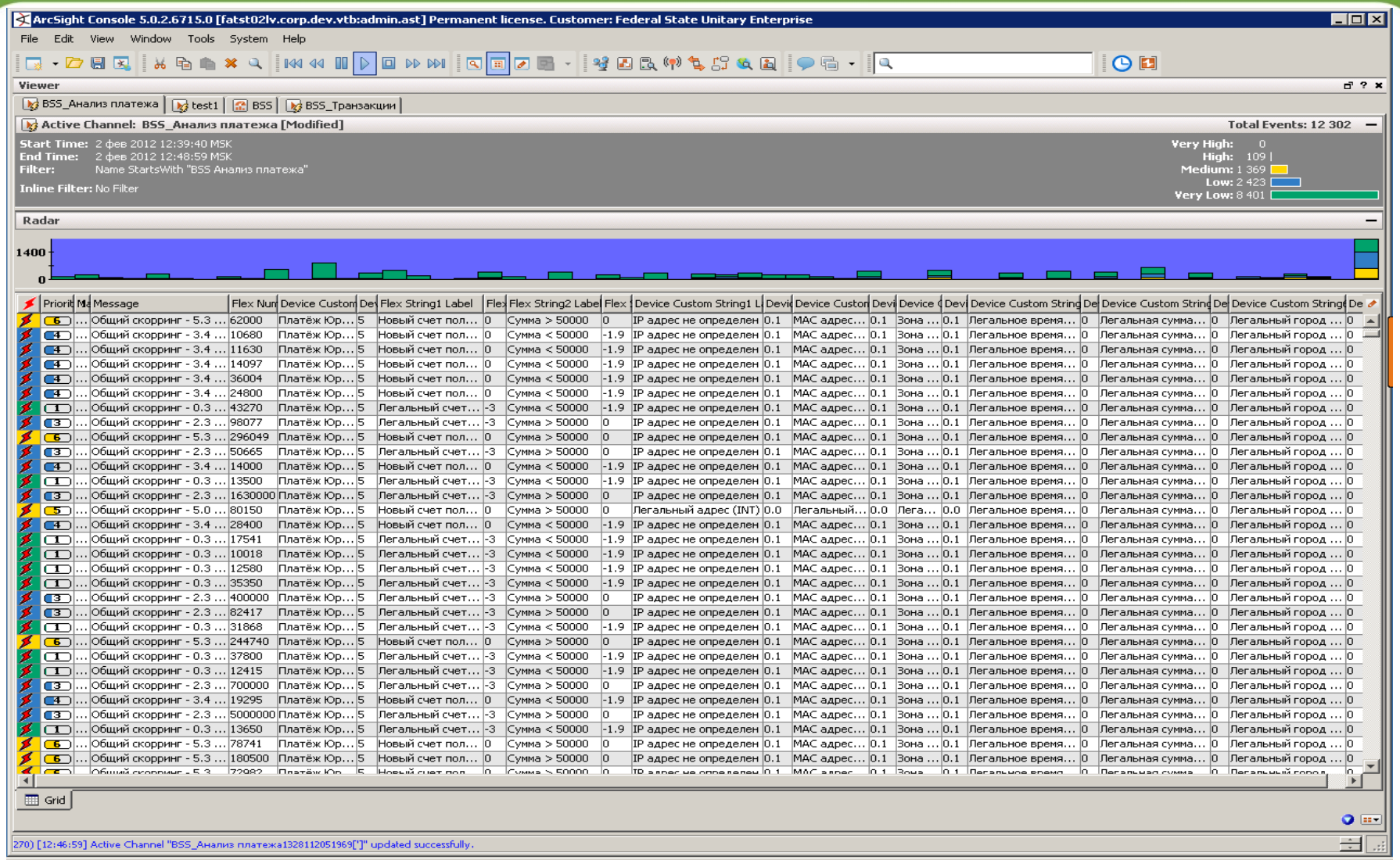
ДиалогНаука

Схема интеграции СВМО



ДиалогНаука

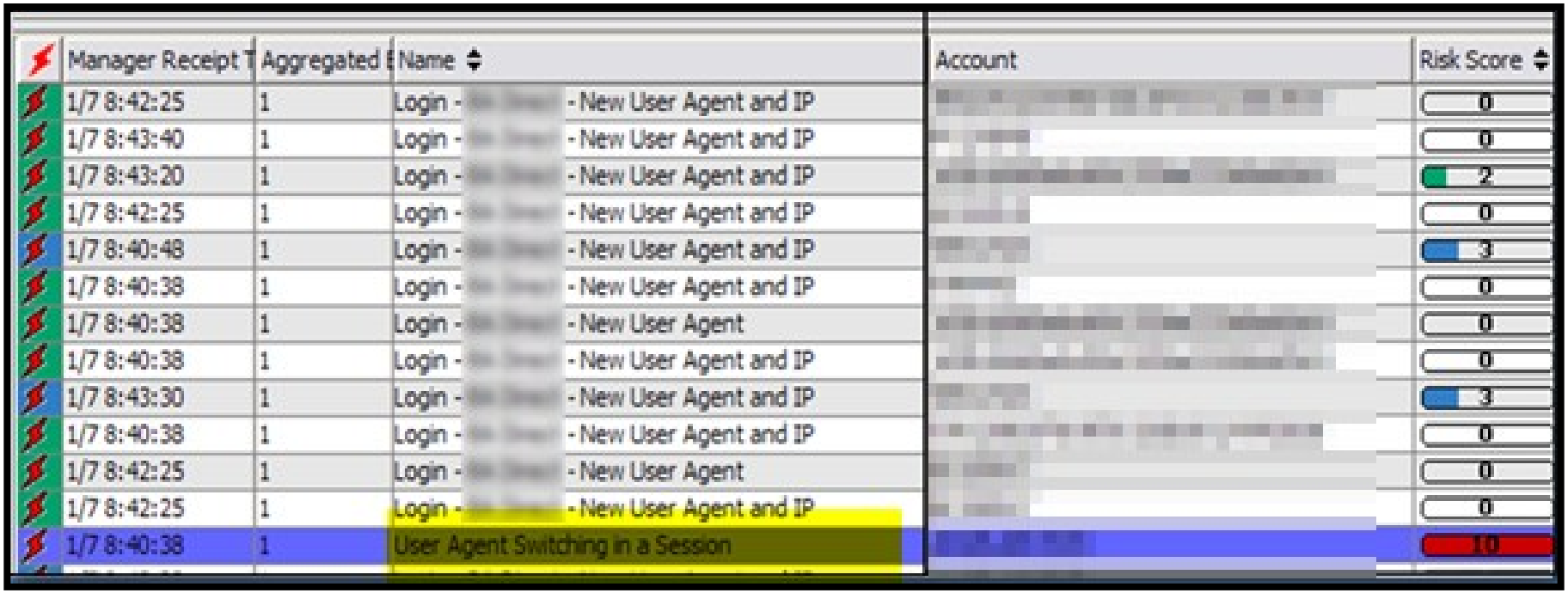
Примеры работы системы



ДиалогНаука

Примеры работы системы

- Выявление атаки “Man in the Middle”. Выявляется за счет быстрого изменения параметров соединения

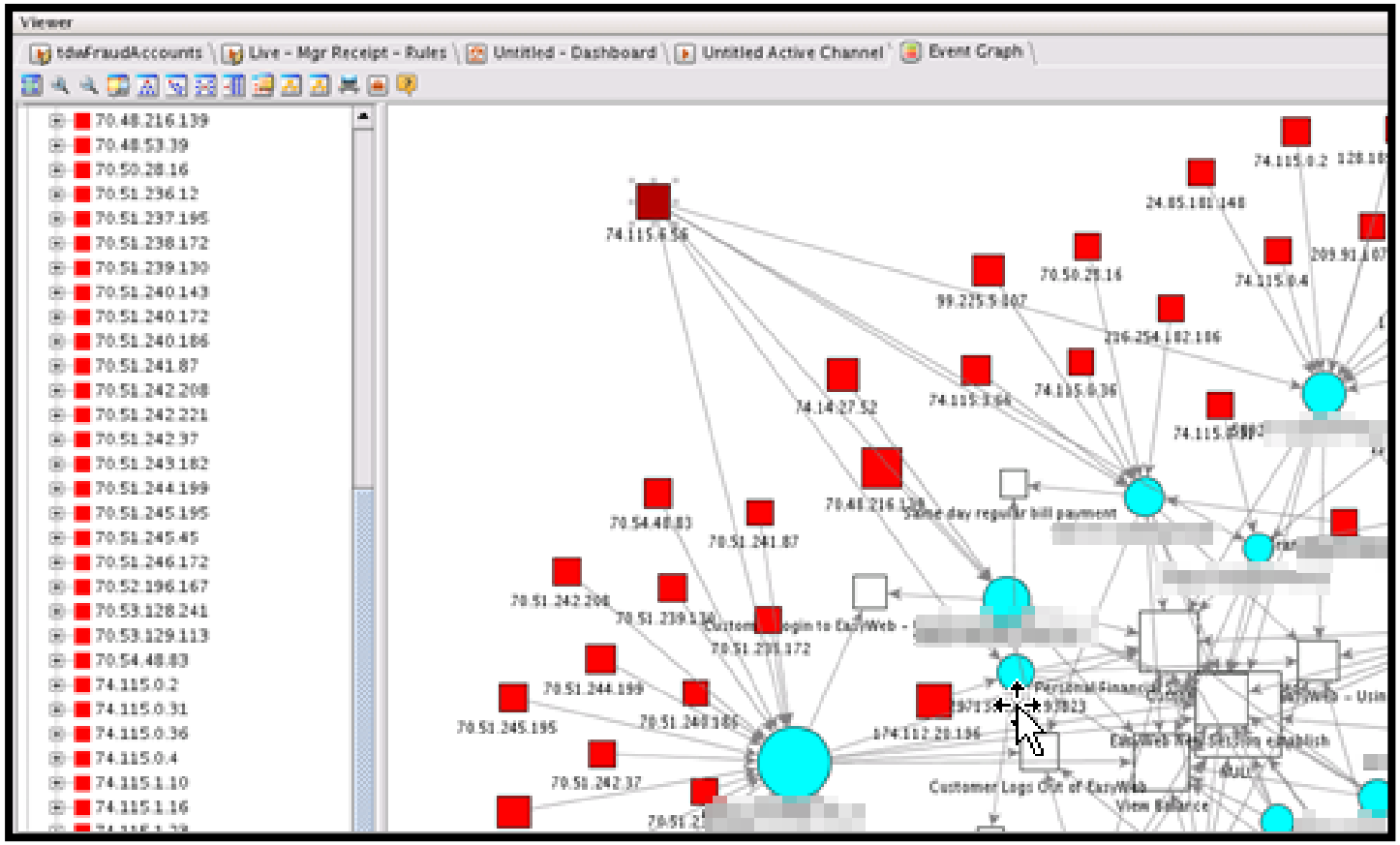


Manager Receipt T	Aggregated E	Name	Account	Risk Score
1/7 8:42:25	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:43:40	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:43:20	1	Login - [redacted] - New User Agent and IP	[redacted]	2
1/7 8:42:25	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:40:48	1	Login - [redacted] - New User Agent and IP	[redacted]	3
1/7 8:40:38	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:40:38	1	Login - [redacted] - New User Agent	[redacted]	0
1/7 8:40:38	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:43:30	1	Login - [redacted] - New User Agent and IP	[redacted]	3
1/7 8:40:38	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:42:25	1	Login - [redacted] - New User Agent	[redacted]	0
1/7 8:42:25	1	Login - [redacted] - New User Agent and IP	[redacted]	0
1/7 8:40:38	1	User Agent Switching in a Session	[redacted]	10

ДиалогНаука

Примеры работы системы

- Пример выявления входа в ДБО с IP адреса из «черного списка»



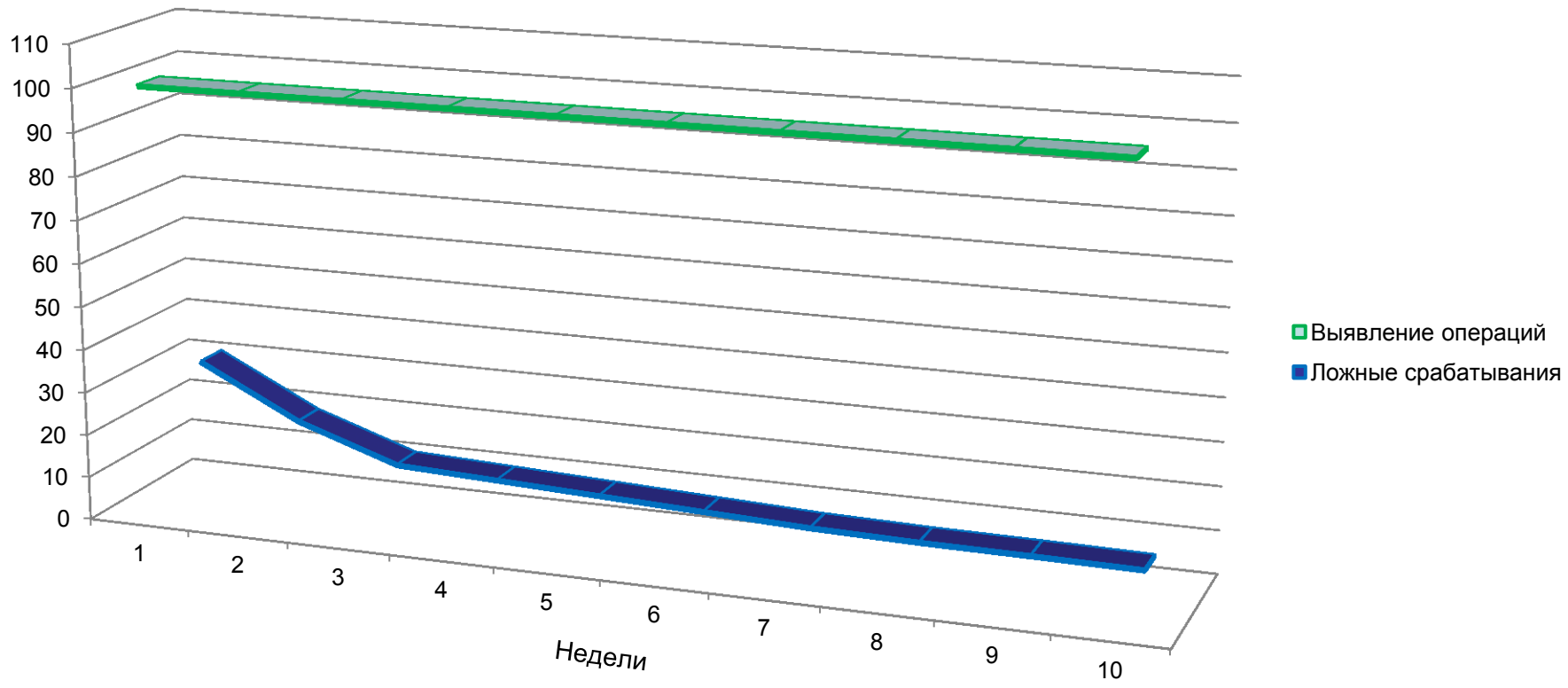
Работы по внедрению СВМО

Этапы проведения работ по внедрению СВМО

- Сбор информации о системе ДБО, АБС
- Разработка технического решения СВМО
- Установка СВМО и настройка подключений в ДБО, АБС
- Обучение СВМО путем анализа транзакций за 2-3 месяца
- Опытная эксплуатация СВМО, настройка пороговых коэффициентов
- Запуск в промышленную эксплуатацию

ДиалогНаука

Обучение системы



ДиалогНаука

План презентации

Вопросы

Вопросы

ЗАО «ДиалогНаука»
Корольков Сергей
Технический директор

Телефон: +7 (495) 980-67-76
e-mail: SKorolkov@DialogNauka.ru