Лекция 10. Информационная безопасность баз данных

Информационная безопасность баз данных (Database security) – система мер и средств, направленная на защиту сведений, находящихся в базах данных различного типа. Контроль за безопасностью баз данных необходим, содержащаяся в них информация всегда будет интересовать третьих лиц, и чем больше БД, тем более серьезного уровня защиты она требует.

Понятие базы данных

Под базой данных понимается не просто обработанная информация, хранящаяся в файле или группе файлов, а правильно организованная и подготовленная для пользователя. Для работы с базами используются программные средства защиты и управления – системы управления базами данных (СУБД), предполагающие применение языков программирования, обеспечивающих единые принципы описания, хранения и обработки информации. В качестве программной оболочки для баз данных чаще всего используются Oracle Database, MS SQL Server, MySQL (MariaDB) и ACCESS. Для описания содержимого применяются метаданные.

ОТ КОГО НУЖНО ЗАЩИЩАТЬСЯ?

БАЗЫ ДАННЫХ — ОСНОВНОЙ ИСТОЧНИК НАИБОЛЕЕ ЦЕННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИИ. КРОМЕ ВЛАДЕЛЬЦЕВ ДАННЫХ ЭТА ИНФОРМАЦИЯ ИНТЕРЕСУЕТ МНОЖЕСТВО ДРУГИХ ЛЮДЕЙ.

ИНСАЙДЕРЫ

Хищения информации сотрудниками с целью продажи конкурентам или использования на новом месте работы.

ХАКЕРЫ

Целенаправленные атаки на базы данных для получения доступа к ним.

ПРИВИЛЕГИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

Контроль действий администраторов баз данных, контрагентов

ХАЛАТНОСТЬ

Случайные утечки данных, совершенные по неосторожности.

В практике используются следующие типы БД:

- **фактографическая** – сюда вносят краткую описательную информацию об объектах некоторой системы в точно определенном формате;
- **документальная** – в нее включены документы или файлы разного типа: текстовые, графические, звуковые, мультимедийные;
- **распределенная** – БД, разные части которой хранятся на различных серверах, объединенных в сеть;
- **централизованная** – для данных, находящихся на одном сервере;
- **реляционная** – база с табличной организацией данных;
- **неструктурированная (NoSQL)** – БД, где задачи масштабируемости и доступности решаются за счет атомарности (англ. atomicity) и согласованности данных, без создания для них определенной (реляционной) структуры.

Задачи по обеспечению безопасности баз данных

Структурированная и систематизированная информация, размещенная в управляемых базах данных (СУБД), находящихся на выделенных серверах, легче поддается обработке и анализу, используется при выстраивании бизнес-процессов. Интерес у злоумышленников она вызывает больший, чем неструктурированная информация в разрозненных файлах и кратковременной памяти. Поэтому основными задачами по обеспечению безопасности становятся:

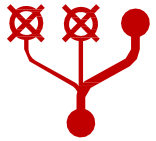
- защита информации от несанкционированного доступа (НСД) инсайдеров или внешних заинтересованных лиц;
- предотвращение уничтожения данных. Механизмы современных DBMS (систем управления СУБД, Database Management System) способны вычислить частично стертую и поврежденную информацию и откорректировать ошибку, поэтому речь идет об обеспечении безопасности от рисков полного уничтожения содержимого базы;
- защита от программных и аппаратных ошибок, сложностей с доступом к серверу, которые затрудняют или создают невозможность для пользователей обрабатывать информацию, содержащуюся в базах.

Задачи решаются различными способами, выбор средств обеспечения безопасности основывается на понимании угроз, направленных на содержимое БД.

Защита от утечек информации,
хранящейся в БД.

Аудит всех операций с БД
в режиме реального времени.

Контроль действий
привилегированных пользователей



Контроль удаленного доступа
сотрудников

Выявление и предотвращение попыток
внешнего вторжения в СУБД
.

Блокирование нежелательных запросов
к БД и веб-приложениям

Обнаружение всех БД в компании,
их классификация и сканирование на уязвимости

Угрозы

Выстраивание эффективной системы безопасности баз данных потребует оценки угроз с опорой на ценность информации и сложившуюся в сфере ее обращения практику преступного посягательства на данные. Так, одни средства используются для БД НИИ, и другие – для баз данных интернет-провайдеров. Среди основных:

- несанкционированное использование информации в БД системными администраторами, пользователями, хакерами;
- вирусные атаки с различными последствиями;
- SQL-инъекции, произвольно изменяющие код или переформатирующие базы;
- технические проблемы, снижение производительности, отказ в доступе, исключающие возможность использования информации;
- физический ущерб, нанесенный оборудованию или каналам связи;
- ошибки, недоработки, несанкционированные возможности в программах, управляющих базами, и ином ПО, наиболее уязвимы операционные системы.

Это наиболее типичные угрозы, с которыми приходится бороться в целях обеспечения информационной безопасности баз данных.

Доступ и привилегии

Первой задачей по обеспечению безопасности базы данных становится разграничение прав доступа и определение привилегий, позволяющих системным администраторам осуществлять управление, а пользователям получать доступ к данным.

Выделяется два типа привилегий:

- системные привилегии;
- привилегии объектов.

Системные позволяют администратору выполнять управленческие действия по отношению к базе и содержащимся в ней информационным объектам. Это как, например, указано для СУБД SQL Server, создание:

- самой БД;
- процедуры разграничения или обработки информации;
- представления;
- резервной БД;
- таблицы;
- триггера.

Объектные привилегии определяют объем прав пользователя при работе с информационными объектами с учетом ограничений, диктуемых безопасностью. В СУБД чаще всего встречаются использование, выбор, вставка нового объекта, обновление и ссылки.

После определения объема привилегий встает вопрос разграничения прав доступа, что позволяет отсечь от информационных массивов пользователей, не имеющих определенного объема прав, например, сотрудников других подразделений компании. Если система управления предприятием сертифицируется по одному из международных стандартов, например, ISO 9001, и в БД содержится информация, используемая для формирования публичной отчетности, обязательной задачей становится разграничение привилегий, при этом третье лицо, не являющееся разработчиком БД, проводит аудит наличия разграничений. Должно быть подтверждение того, что лицу предоставлено наименьшее количество привилегий при работе с базами данных и не предложено избыточных прав на управление программой или изменение информации. Проблема завышенных привилегий отмечается экспертами как одна из основных уязвимостей, характерных для СУБД.

В единых для всей компании базах данных в целях безопасности сведений встает вопрос разграничения прав пользователей на доступ к различным информационным объектам, содержащимся в БД. Этот вопрос безопасности решается с использованием различных программных средств, позволяющих присвоить маркеры пользователям и объектам. Операции становятся возможными только при совпадении маркеров. В современных ПО решена задача разграничения доступа не только к элементам БД – файлам, документам, записям, но и к структурным параметрам, таким как элемент, поле, запись, набор данных.

•

Методики оценки уязвимости

Ряд требований по сертификации деятельности компании предполагает оценку уязвимости БД по различным методикам и параметрам с целью установления того, насколько обеспечена безопасность информации. Применяется ручное или автоматическое сканирование, направленное на поиск ошибок в программном коде, позволяющих несанкционированно получить доступ к данным, обойти элементы управления безопасностью, взломать защиту или скомпрометировать ее степень. Параллельно со сканированием уязвимостей обязателен непрерывный мониторинг, призванный выявить инциденты информационной безопасности или изменение файлов СУБД. Сканирование и мониторинг – обязательные механизмы оценки рисков для компаний, испытывающих необходимость в сертификации по ISO или размещающих свои ценные бумаги на иностранных фондовых рынках.

Мониторинг

Отсутствие сбоев в работе баз данных и постоянную доступность информации позволит выявить мониторинг активности. Он проводится в режиме реального времени одним из следующих методов:

- путем анализа трафика протокола (SQL), осуществляемого от сервера управления по сети;
- путем наблюдения за активностью локальной базы данных на каждом сервере для распределенных БД с использованием программных агентов, размещенных на сервере управления.

Дополнением к аудиту активности служит аудит действий, при котором в журнал активности записываются все операции, совершаемые пользователями в отношении элементов баз данных. Требования безопасности, согласно стандартам, предполагают, что администраторы не могут отключать или изменять правила поведения таких учетных регистров, изменять записи в них. Также такие системы мониторинга часто имеют право самостоятельно выявлять или отключать пользователей, чья активность покажется им подозрительной.

Аудит

- Внешний или внутренний аудит работоспособности баз данных позволит выявить системные проблемы или внезапные инциденты. Большинство администраторов БД используют внешние программные инструменты для организации аудита уязвимостей и проблем с безопасностью баз данных. Однако многие платформы для размещения баз данных способны предложить собственные инструменты аудита. Такой мониторинг на уровне хоста или провайдера станет контрольным инструментом, позволяющим доказать, что в БД не были внесены изменения.

Процесс и процедуры контроля

Настроенные процедуры контроля помогут решить задачи привлечения к ответственности лиц, нарушивших целостность или конфиденциальность информации. Программа обеспечения безопасности баз данных должна гарантировать регулярный анализ объема привилегий и прав доступа пользователей, выявляя изменения. Также для повышения степени безопасности БД часто используются:

- система двухфакторной аутентификации пользователей, иногда с использованием технических средств – токенов;
- система звуковой сигнализации при выявлении инцидентов информационной безопасности;
- система аварийного восстановления при уничтожении базы или ее части. Отказ от внедрения системы резервного копирования становится одной из наиболее частых ошибок.

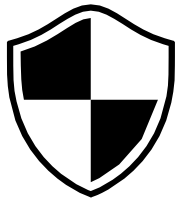
Иные программные решения защиты базы данных могут быть реализованы при внедрении DLP-системы, исключающей намеренные утечки данных.

Общие принципы управления безопасностью баз данных

Выстраивая систему защиты информации и комбинируя различные способы, оптимального эффекта можно добиться, последовательно совершая шаги:

- выбор защищенного сервера или платформы баз данных, предлагающих собственные системы аудита и мониторинга;
- ограничение физического доступа к компьютерам, на которых находятся элементы БД, и ограничение прав доступа пользователей при помощи программных решений;
- использование двухслойных решений для организации доступа, при которых пользователь получает допуск к CRM или иной бизнес-системе, содержащим только ссылки на элементы БД. Это минимизирует риск неправомерного использования, изменения или копирования информации;
- обеспечить наличие системы резервного копирования и восстановления базы после сбоев;
- исключение возможности запуска любых программ или процессов на сервере с БД.

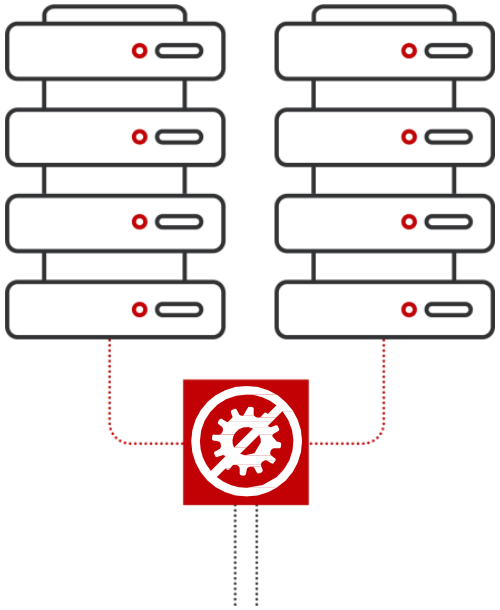
ПРИМЕРЫ РЕШАЕМЫХ ЗАДАЧ



- Предотвращение выгрузки и продажи критичных данных клиентов, в том числе персональных данных, данных кредитных карт и т.д.
- Контроль манипуляций с клиентскими базами, накрутки KPI менеджерами
- Проверка БД на обезличенность при их передаче (например при их клонировании для целей тестирования)
- Разграничение доступа к СУБД для аттестации информационных систем
- Выявление не оптимально настроенных конфигураций СУБД с точки зрения стандартов и лучших практик по информационной безопасности
- Предотвращение мошенничества и прямых хищений денежных средств с использованием БД и бизнес-приложений компании
- Выявление несанкционированного разворачивания теневых, нелегитимных и неконтролируемых баз данных со стороны администраторов
- И другие

ПОМОГУТ ЛИ ШТАТНЫЕ СРЕДСТВА КОНТРОЛЯ?

ИСПОЛЬЗОВАНИЕ ШТАТНЫХ СРЕДСТВ АУДИТА БАЗ ДАННЫХ ВЛЕЧЁТ ЗА СОБОЙ ДОПОЛНИТЕЛЬНЫЕ ЗАТРАТЫ И НЕ ОБЕСПЕЧИВАЕТ ПОЛНОГО КОНТРОЛЯ



- Требуют постоянного ручного контроля и специфических знаний пользователя
- Существенно снижают производительность СУБД (10-40%)
- Отсутствие контроля привилегированных пользователей
- Невозможность блокировки действий пользователей
- Нет идентификации пользователя в трёхзвенной архитектуре
- Отсутствие механизмов реагирования при нарушении
- Невозможность расследования инцидента при нарушении работоспособности самой СУБД

ПРИНЦИП РАБОТЫ

Анализ сетевого трафика с возможностью мониторинга или блокировки нелегитимных запросов пользователей и получаемых данных из СУБД

Сканирование баз данных, находящихся под контролем,

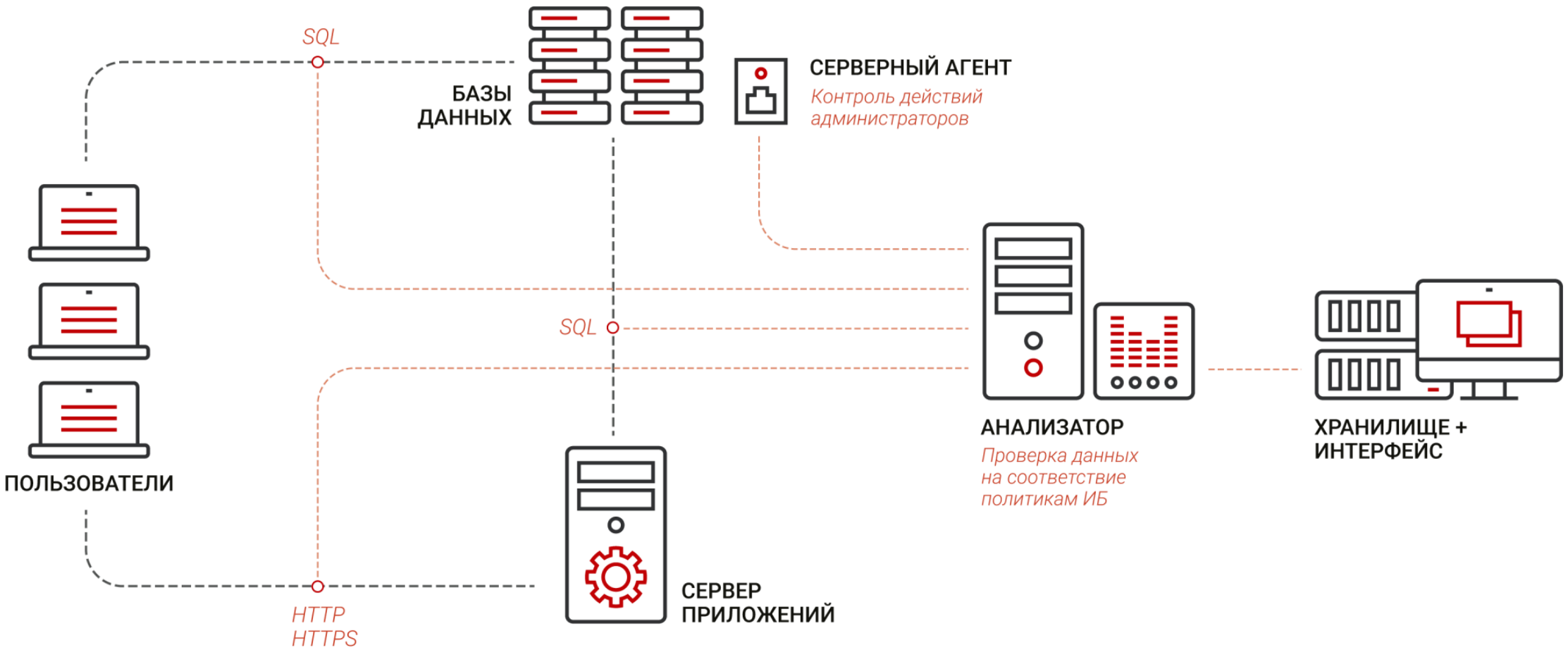
Обработка данных и долгосрочное хранение всех запросов и ответов для ретроспективного анализа

Аналитическая отчетность и поведенческий анализ (UBA), выявление нарушений политик безопасности

Автоматический поиск новых СУБД, не стоящих на контроле, классификация их по типу хранимых данных

Система оповещения уведомляет о событиях по электронной почте, передает данные во внешние SIEM- системы, отображает отчёты на главном экране

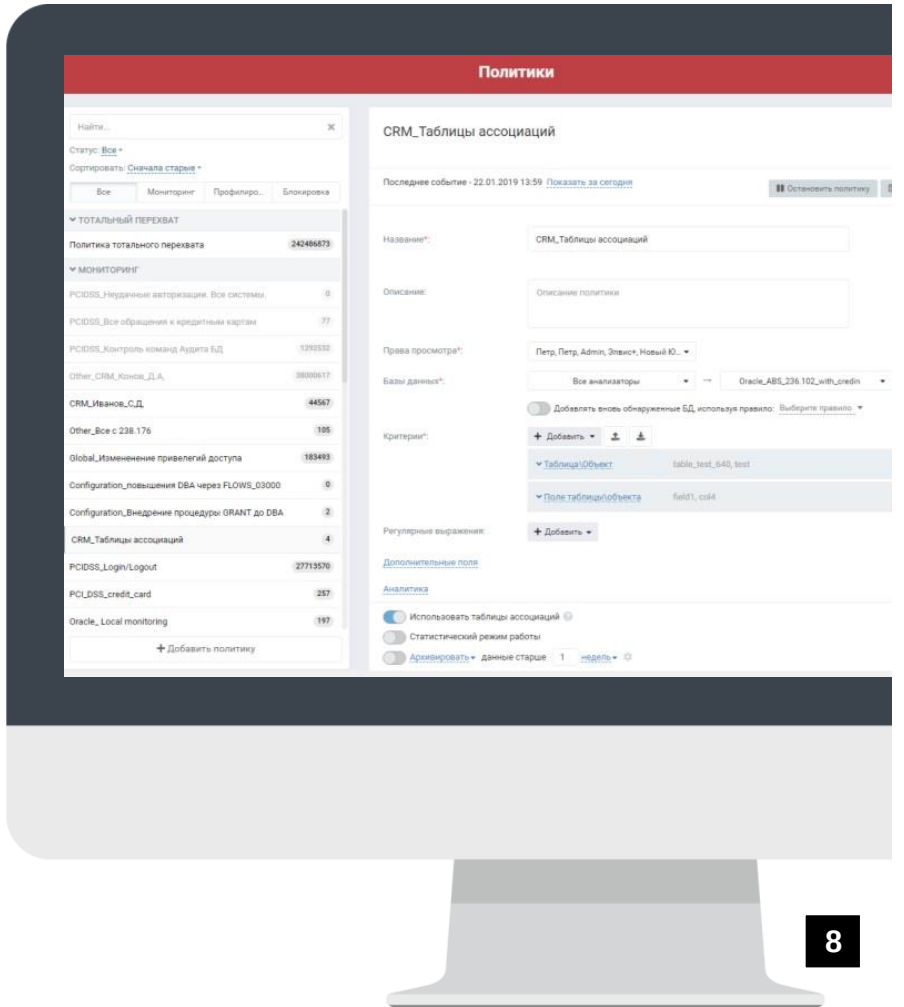
СХЕМА ИНТЕГРАЦИИ В СЕТЬ ЗАКАЗЧИКА



ПОЛИТИКИ БЕЗОПАСНОСТИ

ПРАВИЛА РАБОТЫ СИСТЕМЫ ЗАДАЮТСЯ В КОНСТРУКТОРЕ ПОЛИТИК БЕЗОПАСНОСТИ

- ☑ Большой выбор критериев и их объединений.
- ☑ Предустановленные шаблоны регулярных выражений (персональные данные, банковские карты и т.д.).
- ☑ Синхронизация с LDAP – возможность обогащения перехваченной информации.
- ☑ Экспорт результатов работы политик в SIEM.
- ☑ Архивация перехваченных данных по конкретной политике.
- ☑ Политики блокировки позволяют предотвращать нежелательные операции с СУБД
- ☑ Список предустановленных политик ИБ:
  - Помогают в регулярных задачах ИБ
  - Закрывают требования регуляторов
  - Эффективно защищают БД «из коробки»



КРИТЕРИИ ФОРМИРОВАНИЯ ПОЛИТИК

- IP-адрес клиента
- Имя пользователя в БД
- Имя пользователя в ОС
- Название клиентского ПО
- Результат аутентификации
- Дата/время запроса
- Запрашиваемые/передаваемые поля таблицы, синонимы, представления
- Объём данных ответа/запроса
- Имя объекта БД
- Ключевое слово
- Тип SQL-команды
- Количество записей в ответе

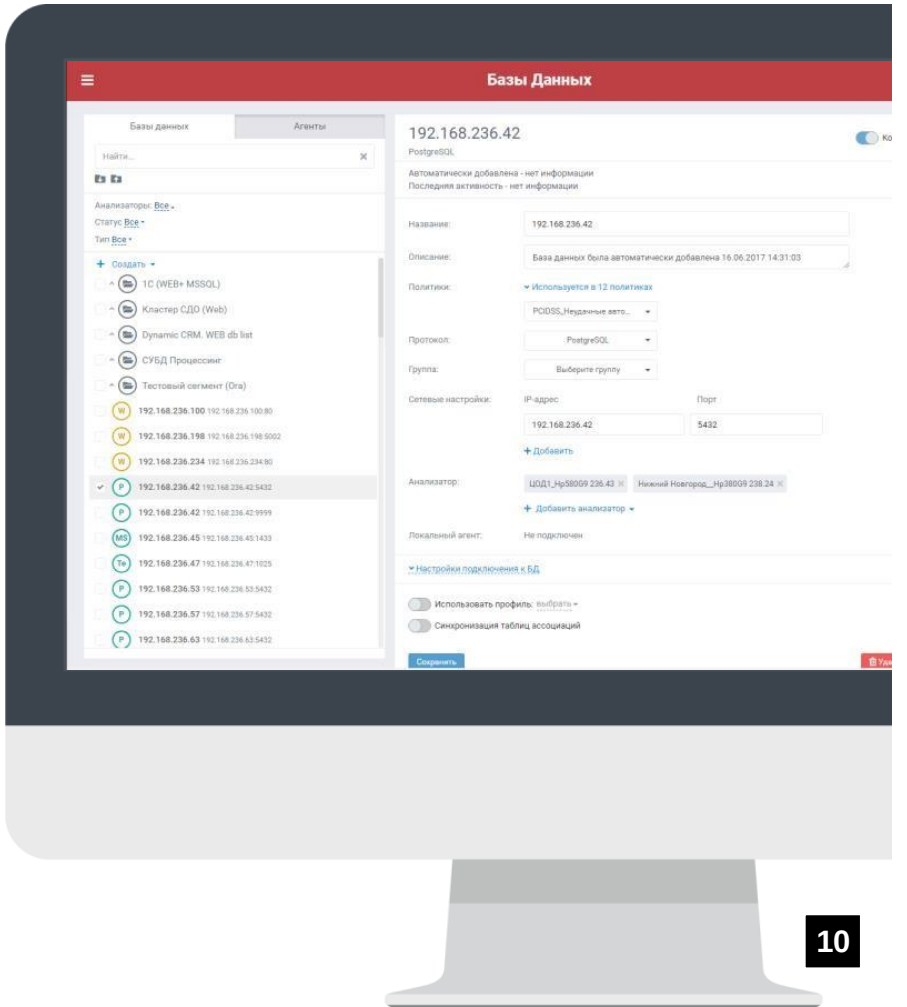
ОБНАРУЖЕН ИБ
И КЛАССИФИКАЦИЯ БД

СИСТЕМА АВТОМАТИЧЕСКИ НАХОДИТ НОВЫЕ БД, НЕ СТОЯЩИЕ НА КОНТРОЛЕ, И КЛАССИФИЦИРУЕТ ИХ ПО ТИПУ ХРАНИМЫХ ДАННЫХ (НАПРИМЕР, ВЫЯВЛЯЕТ ПЕРСОНАЛЬНЫЕ ДАННЫЕ).

На основе типа данных автоматически сформирует политики ИБ для новой базы данных.

Постановка на контроль также может осуществляться автоматически.

- Всегда актуальный перечень СУБД компании.
- Обнаружение новых БД (создание новых ИС/АС).
- Выявление открытия новых портов, изменения IP-адресов СУБД.
- Контроль обезличенности баз данных компании



СКАНИРОВАНИЕ БАЗ ДАННЫХ

ЭТО ПОЗВОЛЯЕТ РЕШАТЬ ЗАДАЧИ, СВЯЗАННЫЕ НЕ ТОЛЬКО С КОНТРОЛЕМ ДОСТУПА, НО И С НЕКОРРЕКТНЫМИ НАСТРОЙКАМИ БЕЗОПАСНОСТИ

КЛАССИФИКАЦИЯ

- Поиск местонахождения критичной информации
- Создание политик по результатам сканирования
- Настройка уровня угроз

УЯЗВИМОСТИ

- Неустановленные обновления
- Проверка оптимальности конфигурации СУБД
- База проверок на уязвимости

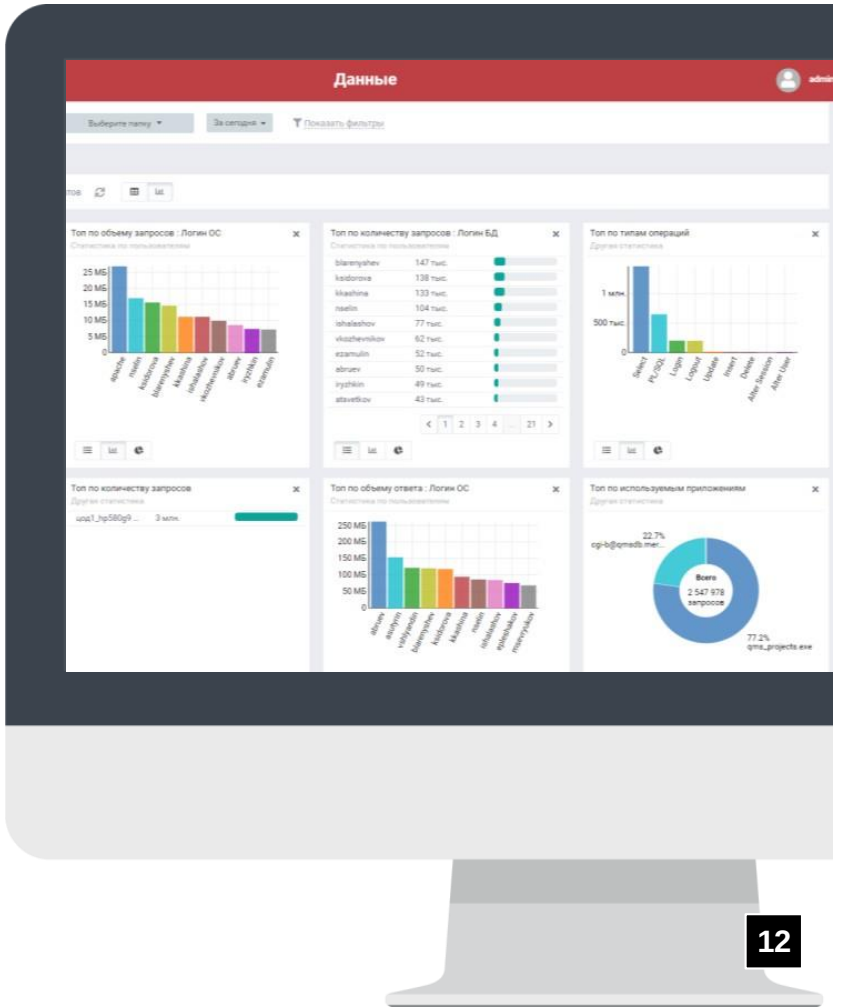
МАТРИЦЫ ДОСТУПА

- Построение карты доступа вида «Пользователь – Объект доступа (таблицы ,функции) – Типа прав доступа»
- Сравнение текущей картины с эталонной

КОНТРОЛЬ И АНАЛИТИКА

ВСТРОЕННЫЕ СРЕДСТВА АНАЛИТИКИ ПОЗВОЛЯЮТ ВЫЯВЛЯТЬ ОТКЛОНЕНИЯ В ОБЫЧНЫХ СЦЕНАРИЯХ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ БД И ПРЕДОСТАВЛЯЮТ НАГЛЯДНЫЕ СТАТИСТИЧЕСКИЕ ОТЧЕТЫ.

- ☑ Интерактивная отчётность
- ☑ Конструктор отчётов с возможностью анализа любого объёма данных за любой промежуток времени
- ☑ Возможность создания индивидуального дашборда
- ☑ Поведенческий анализ пользователей БД (UEBA)
- ☑ Уведомление о нарушениях по электронной почте
- ☑ Уведомление о выявленных аномалиях в SIEM



СЕТЕВОЙ ЭКРАН

БЛОКИРУЕТ НЕЖЕЛАТЕЛЬНЫЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ, ПРОТИВОРЕЧАЩИЕ ПОЛИТИКАМ БЕЗОПАСНОСТИ.

Умная система самообучения анализирует деятельность операторов БД для предотвращения ложных срабатываний. Для гарантирования доступности защищаемых баз данных сетевой экран ставится в режиме отказоустойчивого кластера.

- ☑ Возможность дешифрации HTTPS-трафика по принципу Man In the middle (MITM)
- ☑ Возможность реализации системы разграничения прав доступа к СУБД для аттестации ИС, использующих несертифицированные СУБД

Блокировка реализуется по принципу L3 Reverse Proxy Firewall чему обеспечивается повышенная отказоустойчиивость.

Гибкий конструктор политик и блокировки по правилам на агенте предотвращают утечку данных с уведомлениями о заблокированных сессиях в интерфейсе системы.

ЗЕРКАЛИРОВАНИЕ ТРАФИКА

ПРИМЕНЯЕТСЯ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ, КОТОРЫЕ ОБРАЩАЮТСЯ К БД НАПРЯМУЮ ИЛИ ЧЕРЕЗ ТРЕХЗВЕННЫЕ ПРИЛОЖЕНИЯ.

ИСПОЛЬЗУЮТСЯ АГЕНТЫ ДЛЯ КОНТРОЛЯ ЛОКАЛЬНЫХ ПОДКЛЮЧЕНИЙ ЛИБО ПЕРЕНАПРАВЛЕНИЯ ВСЕГО СЕТЕВОГО ТРАФИКА К БАЗАМ ДАННЫХ.

ГОРИЗОНТАЛЬНОЕ МАСШТАБИРОВАНИЕ

Позволяет защищать высоконагруженные, в том числе территориально-распределенные системы любого масштаба из единого интерфейса

ЗАЩИТА «БОЛЬШИХ ДАННЫХ»

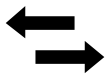
ГАРДА БД ОБЕСПЕЧИВАЕТ ЗАЩИТУ BIG DATA:

РЕЛЯЦИОННЫХ (ХРАНЯТСЯ В ТАБЛИЦАХ),

НЕ РЕЛЯЦИОННЫХ (ХРАНЯТСЯ В СПЕЦИАЛЬНЫХ КЛАСТЕРНЫХ ХРАНИЛИЩАХ С ВОЗМОЖНОСТЬЮ РАСПРЕДЕЛЕННОЙ ОБРАБОТКИ).

Журнал данных. Возможность группировки данных по времени – логинам - приложениям и другим свойствам

Контролируем доступ к любым Big Data системам через Rest API



Полностью поддерживаем протокол HTTP до уровня данных

Поддержка Hortonworks Data Platform

Унифицируем подходы к защите реляционных и NoSQL баз данных

ЗАЩИТА BIG DATA

- Контроль доступа к Big Data системам Rest API
- Поддержка протокола http/https
- Поддержка Hortonworks Data Platform
- Унификация подходов к защите реляционных и NoSQL баз данных
- Профиль учитывает особенности рабо каждого сотрудника

ДАННЫЕ ВАШЕЙ КОМПАНИИ ХРАНЯТСЯ В BIG DATA, ЕСЛИ ОНИ:

- ✓ Занимают большой объём >100 Тб
- ✓ Слабо структурированы
- ✓ Приходят из множества источников
- ✓ Должны обрабатываться в режиме реального времени
- ✓ Растут в размере хранения более чем на 60% в год

ДИНАМИЧЕСКОЕ ПРОФИЛИРОВАНИЕ (UEBA)

Встроенные средства аналитики позволяют выявлять отклонения от обычных сценариев работы пользователей БД и формируют наглядные отчёты по инцидентам.

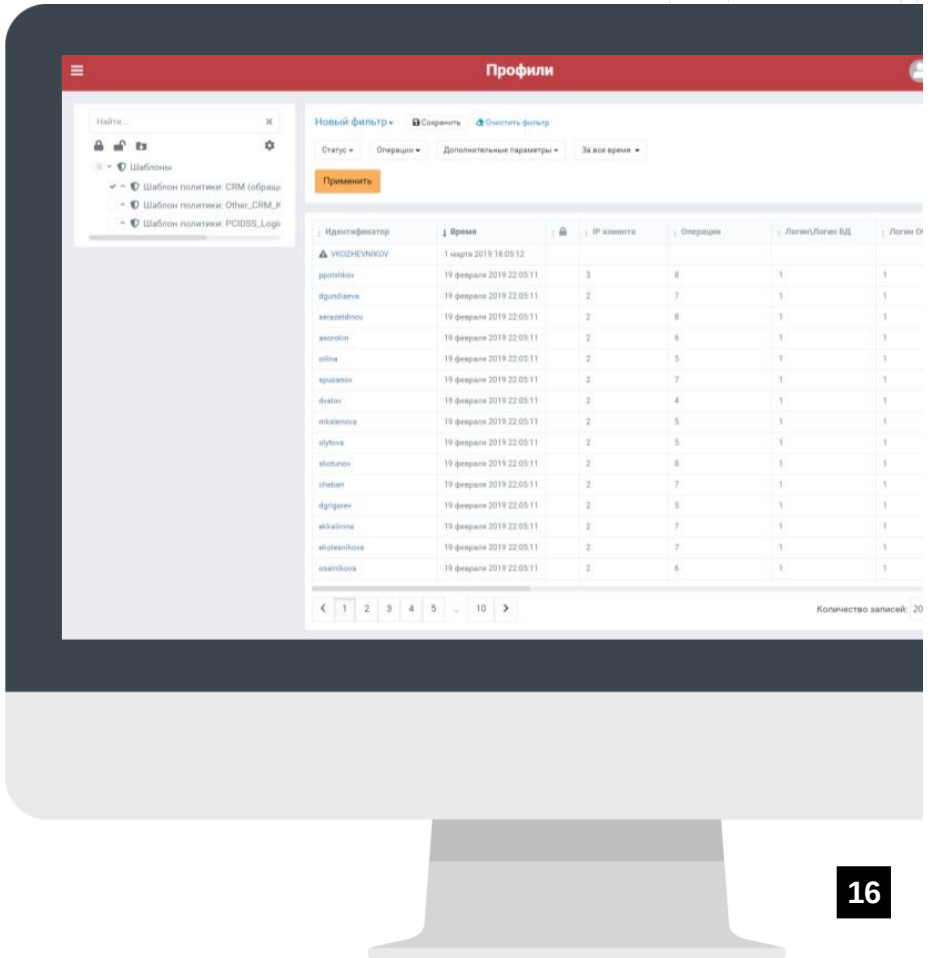
АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ ПРОФИЛЕЙ В РЕЖИМЕ ОБУЧЕНИЯ

Учитываются:

- Логины, приложения, IP-адреса, названия таблиц и полей
- Особенности работы каждого сотрудника
- Информация о регионе

ВЫЯВЛЕНИЕ ОТКЛОНЕНИЙ ОТ ПРОФИЛЕЙ

- Нетипичное поведение для данного пользователя
- (Чужие IP-адреса, ранее не используемые таблицы,
  приложения и рабочие места);
- Статистические аномалии
  - Большое количество запросов
  - Большие выгрузки
  - Много неуспешных авторизаций



КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ И 1С

КОНТРОЛЬ ВЕБ-ПРИЛОЖЕНИЙ

- Детальный разбор HTTP/HTTPS-трафика с выделением данных из веб-форм
- Возможность дешифрации HTTPS-трафика как в пассивном, так и в режимах работы «вразрыв»
- Персонификация пользователей с возможностью выделения учетных записей
- По протоколам передачи данных HTTP/HTTPS
- По протоколам аутентификации Kerberos, NTLM
- Аутентификация (web form authentification)
- Детальный разбор http/https-трафика с выделением данных из веб-форм

МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМАХ 1С

Служба информационной безопасности в интерфейсе системы видит не только обращения к СУБД, но и все пользовательские действия, позволяющие понимать, какая информация, находящаяся в системе 1С, была модифицирована, а к какой были обращения со стороны пользователей, с привязкой к учётным записям.

ЗАЩИТА ОТ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ

МОДУЛЬ «СЕРВЕРНЫЙ АГЕНТ»

- Позволяет протоколировать и/или блокировать действия на сервере БД
- Не оказывает существенного влияния на серверы баз данных
- Позволяет контролировать изменение конфигурационных файлов СУБД

Инновационные технологии позволили минимизировать влияние серверного агента на сервер.

Поддерживаются ОС семейства Redhat, AIX, Windows Server, Solaris, Suse

ОСОБЕННОСТИ РЕШЕНИЯ

ГАРДА БД

- Возможность ретроспективного анализа по сохраненным данным объёмом свыше 100 ТБ
- Возможность анализа трафика на скорости более 10 Гбит/с
- Аудит доступа к БД всех филиалов компании из единого центра
- Полноценная работа с трёхзвенной архитектурой взаимодействия с БД
- Интеграция со всеми популярными SIEM
- Минимальное влияние на производительность сети и серверов СУБД
- Интерактивные отчеты и понятная аналитика на основе всех запросов и ответов БД, статистика инцидентов
- Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени
- Встроенная система выявления аномалий и поведенческого анализа действий пользователей
- Отсутствие стороннего лицензирования

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Поддержка распределённой кластерной инсталляции и централизованного управления из единого интерфейса
- Множество способов подачи трафика (агенты, подача данных с TAP-устройств/SPAN, GRE, ERSPAN)
- Высокая производительность (обработка 10ГБит/с и выше), неограниченная возможность кластеризации
- Сетевой экран с функцией блокировки и динамической балансировки трафика
- Возможность дешифрации HTTPS-трафика как в пассивном режиме, так и при инсталляции «вразрыв»
- Персонификация пользователей с возможностью выделения учетных записей
- Контроль привилегированных пользователей
- Гибко настраиваемые фильтры, автоматическое формирование списков критериев для использования в политиках
- Инцидент-менеджмент
- Сводные отчёты (в том числе отчёт по уязвимостям)
- Встроенный модуль контроля Web-приложений, не требующий отдельных лицензий
- Контроль неявных обращений к СУБД
- Динамическое профилирование (UEBA) с уведомлениями и отчётами
- Доменная авторизация

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ (ИТОГО)

АГЕНТСКИЕ РЕШЕНИЯ ПОД ПОПУЛЯРНЫЕ СУБД

- Агенты с функцией перенаправления трафика, контроля локальных подключений и блокировки доступа к СУБД под операционные системы Linux, Windows, AIX, Solaris и пр.

ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ БАЗ ДАННЫХ

- Автоматическое обнаружение новых баз данных.
- Реагирование на изменения настроек имеющихся баз
- Сканирование баз данных на наличие конфиденциальной информации, номеров кредитных карт, ИНН и пр.
- Проверка БД на обезличенность

СКАНИРОВАНИЕ НА УЯЗВИМОСТИ

- Активные предустановленные учетные записи
- Неустановленные патчи
- Учетные записи с простыми паролями
- Расширенные привилегии доступа к

МОНИТОРИНГ В РЕАЛЬНОМ ВРЕМЕНИ

- Гибкий конструктор политик безопасности пом осуществлять контроль и выявление потенциал инцидентов в режиме реального времени
- Большой список предустановленных политик для часто решаемых задач безопасности

СИСТЕМА ОТЧЁТНОСТИ

- Детализированная отчетность по всем событиям безопасности и операциям пользователей СУБД
- Наличие базы предустановленных отчетов

УВЕДОМЛЕНИЕ О СОБЫТИЙ

- SIEM
- Электронная почта
- Отчёт на главном экранеK

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ (ИТОГО)

ГАРДА БД

УМНЫЙ ПОИСК

- Контентный — по запросам, ответам, переменным и регулярным выражениям (ИНН, номера карт и пр.).
- Атрибутивный — по IP-адресам, учетным записям, текстам ошибок и пр.

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ

- Хранение всех ответов и запросов пользователей и приложений с возможностью ретроспективного анализа за любой период времени.
- Маскирование платёжных данных в хранилище

КОНТРОЛЬ БИЗНЕС-ПРИЛОЖЕНИЙ

- SAP Business Object
- Microsoft Dynamics CRM
- 1С
- Веб-формы
- Гибкие настройки для работы с любыми бизнес-приложениями на основе HTTP(s)-протоколов

КОНТРОЛИРУЕМЫЕ СУБД

- Oracle
- Microsoft SQL
- MySQL
- SAP HANA
- PostgreSQL
- Teradata
- Sybase ASE
- IBM Netezza
- IBM DB2
- Линтер
- Apache
- Cassandra
- Sun MySQL
- Firebird
- Interbase
- Tarantool
- MongoDB
- Kafka5
- Hive5
- Ред База Данных
- SPARK

ПОДДЕРЖИВАЕМЫЕ ОС

- ОС Solaris
- ОС Ubuntu
- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- ОС Windows Server
- ОС SUSE Enterprise Linux
- AIX

Благодарю за внимание!