



Решения для защиты от внутренних угроз



Константин Демин

Старший эксперт
Облачные и инфраструктурные решения

Умышленные нарушения внутреннего характера



Число фишинговых атак выросло в 1,5 раза

\$ 3,92 млн

Средний ущерб
от утечки данных

> 25 тысяч
записей

Средний объем утечки

\$ 150

Средний ущерб от одной
утерянной записи



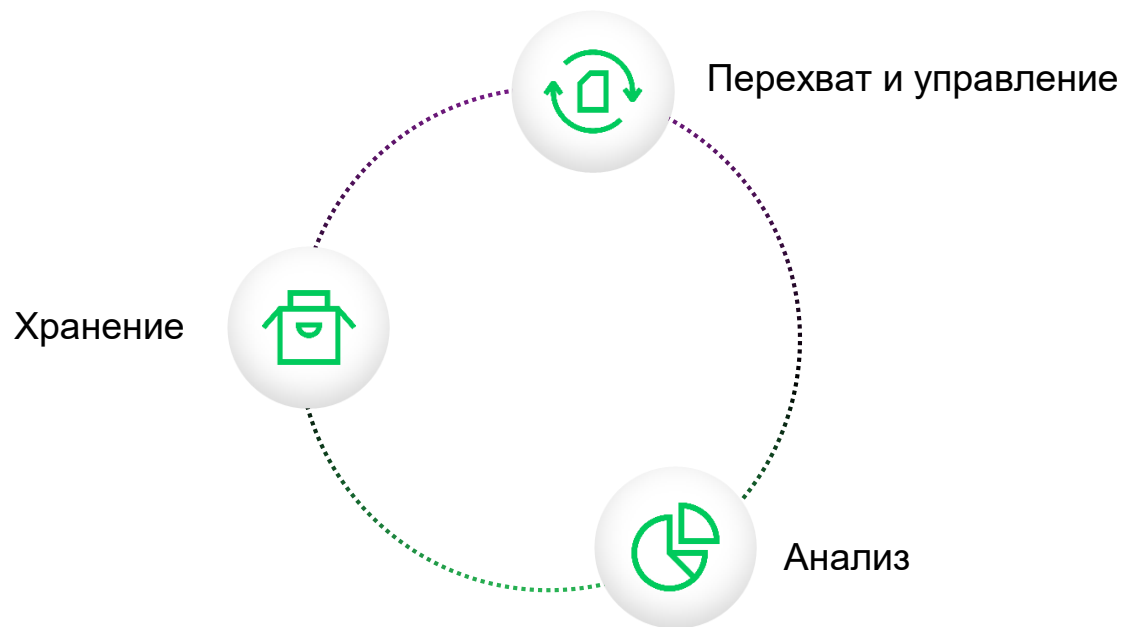


Услуга «МегаФон DLP» на основе решения «Гарда Технологии»

Защитите ваши данные!

Принцип работы

Принцип работы «МегаФон DLP» прост — он заключается в совместной работе трёх подсистем



Модули неразрывны друг с другом и поставляются на единой аппаратной платформе



Все программные компоненты не требуют дополнительного лицензирования



Политика безопасности

Интерактивное создание политики с оценкой результата

Примеры политик:

- Передача ПДн по каналам (почта\мессенджер\облака);
- Передача данных с базой клиентов (поиск похожих);
- Посещение запрещенных ресурсов;
- Поиск работы;
- Подделка документов;
- Запрещенные фразы;
- Другое.



Быстрый поиск

Поиск в базе накопленных объектов осуществляется так же просто, как поиск информации в популярных поисковых системах

- Найденные объекты представлены в удобном для чтения виде
- В распоряжении пользователя большое количество уточняющих критериев поиска
- Поиск не зависит от типа файлов и возможен внутри архивов
- Возможность сохранения шаблонов поиска и регулярное сканирование позволяет получать уведомления о происходящих событиях, не внося их в список политик
- Система хранит полную копию всех коммуникаций — при появлении новых правил и политик вы можете сразу провести ретроспективный анализ по архиву. В любой другой системе такие данные были бы утрачены навсегда



Критерии поиска



Ключевые слова и фразы

В том числе во вложениях и архивах, включая изображения и отсканированные документы



Поиск по регулярным выражениям



Имя файла, свойство документа, тип, размер и пр.



Идентификатор IM-службы Skype, ICQ, MSN и т.д.



VoIP – логин / телефон



Доменная учётная запись пользователя в Active Directory

Импорт информации о сотрудниках с сервера авторизации LDAP



Поиск похожих документов



IP-адрес, протокол, порт



ID пользователя соц. сети



Адрес электронной почты



Декодирование трафика

Контролируйте все необходимые каналы передачи информации следующими сетевыми протоколами



Почтовые и новостные протоколы

SMTP; SMTPs; IMAP4; POP3; POP3s; MAPI; NNTP; S/MIME; MS Exchange; HTTP; HTTPs (методы GET и POST) v 1.0, v 1.1; FTP; FTP over HTTP; туннелирующие протоколы IP-in-IP, L2TP, PPTP, PPOE; Telnet; протокол аутентификации Kerberos 5



Файлообменные сети

BitTorrent (standard 11031); Gnutella (v0.6); E-Mule (v0.49b); Direct Connect Protocol (dc++ v0.707)



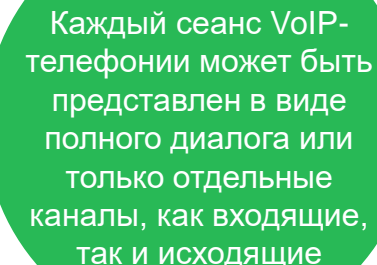
VoIP-телефония

SIP v .2.0 (RFC 2543bis/3261); SDP, H.323 v .2; H.245 v .7; H.225 v .4; T.38; Megaco/H248; MGCP, SKINNY; H.263 ABC; H.264 (single NAL unit mode), включая видеотелефонию



Мессенджеры

OSCAR (ICQ v7, v 8, v9); HTTPIM (обмен сообщениями в социальных сетях); MSNP v.12, v.13 (службы MSN Messenger, Windows Live Messenger); YMSG v9.0.0.2034 (Yahoo Messenger Protocol); IRC; MMP (Mail.Ru Агент); Skype; MS Lync; XMPP (Google Talk, Jabber QIP, SMS)



Каждый сеанс VoIP-телефонии может быть представлен в виде полного диалога или только отдельные каналы, как входящие, так и исходящие



Контроль рабочих мест

Обеспечьте комплексный мониторинг компьютеров

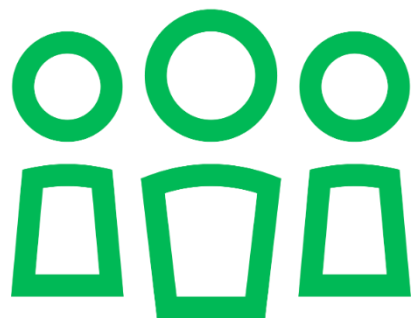


МегаФон DLP не только анализирует коммуникации и информацию об использовании программ и периферии, но и даёт широкие возможности по контролю рабочих мест

- Теневое копирование данных, передаваемых на внешние устройства
- Контроль печати
- Снимки экрана рабочего стола по расписанию или условию
- Просмотр и запись экрана рабочего стола в реальном времени
- Контроль Skype, Telegram, Viber
- Контроль HTTPS (соцсети, веб-почта, другие сайты и сервисы)
- Контроль приложений и журналирование активности
- Блокировка использования приложений
- Блокировка подключаемых устройств (белые списки)
- Блокировка передачи конфиденциальных данных
- Сканирование рабочих мест для обнаружения конфиденциальных данных
- Перехват облачных хранилищ



Взаимосвязи сотрудников



Интерактивный отчёт наглядно демонстрирует облако коммуникаций сотрудника как внутри компании, так и связи с внешней средой, отражает интенсивность коммуникаций и средства передачи информации

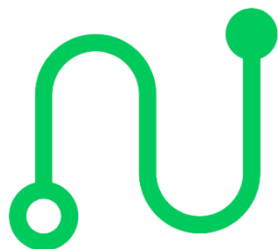
МЕГАФОН



Контентные маршруты

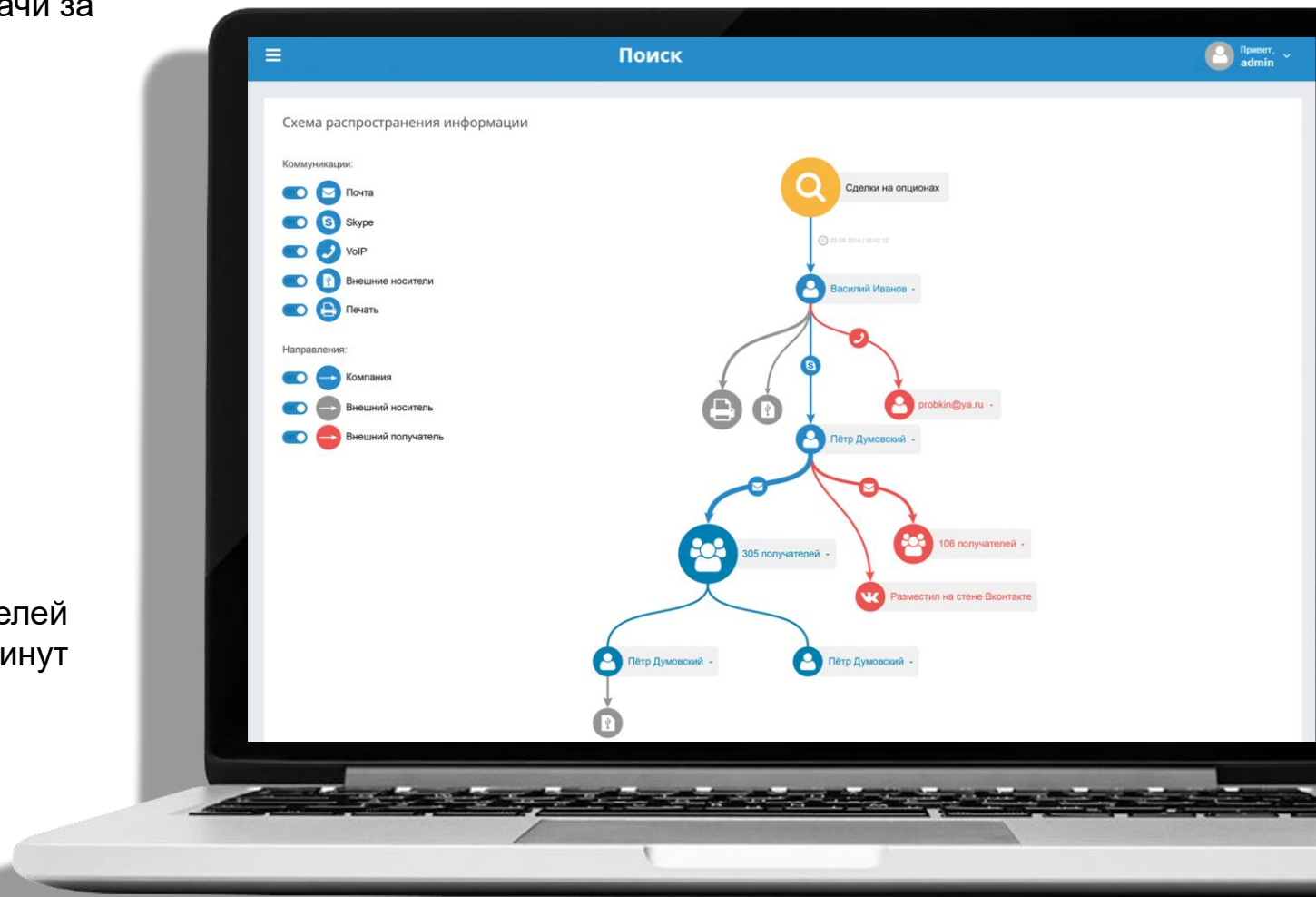
МегаФон DLP наглядно представляет маршрут движения любой информации от первой коммуникации до момента передачи за пределы организации.

В маршруте учитываются как пользователи, так и каналы передачи информации



Отчёт позволяет оперативно расследовать инцидент, выявить сговоры и найти несанкционированных обладателей информации до того, как конфиденциальные данные покинут компанию

МЕГАФОН



Юридический аспект

Для легального использования DLP-систем необходимо принять ряд организационно-распорядительных мер



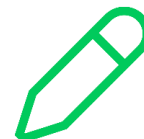
Документальное определение информации ограниченного доступа



Правила работы с информацией ограниченного доступа



Запрет на использование корпоративных ресурсов в личных целях



Внесение изменений в трудовые договоры и правила внутреннего трудового распорядка





Услуга «Защита баз данных» на основе решения «Гарда Технологии»

Защитите ваши данные!

Принцип работы



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



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



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



Сканирование баз данных, находящихся под контролем



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

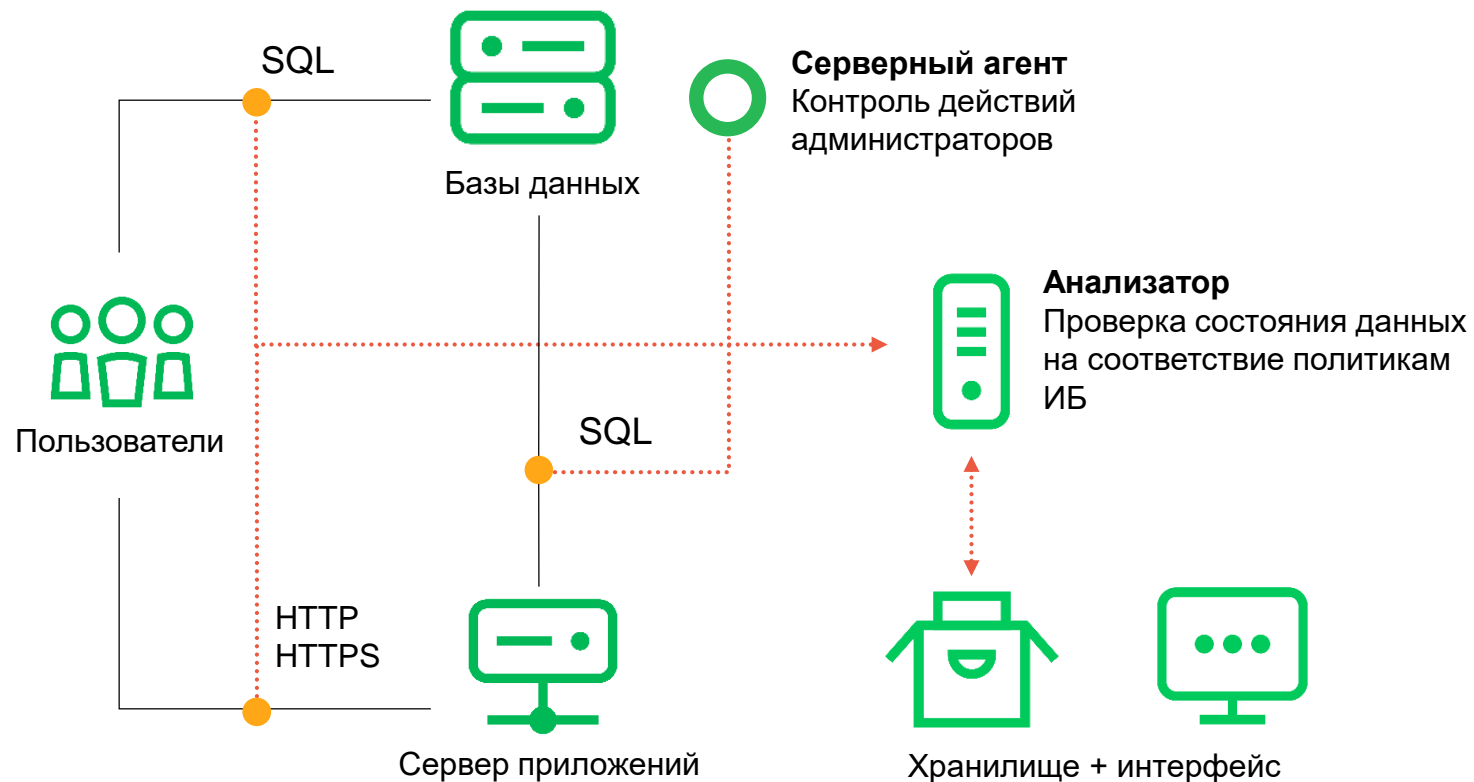


Система оповещения уведомляет о событиях по электронной почте, передает данные во внешние SIEM-системы, отображает отчёты на главном экране



Зеркалирование

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

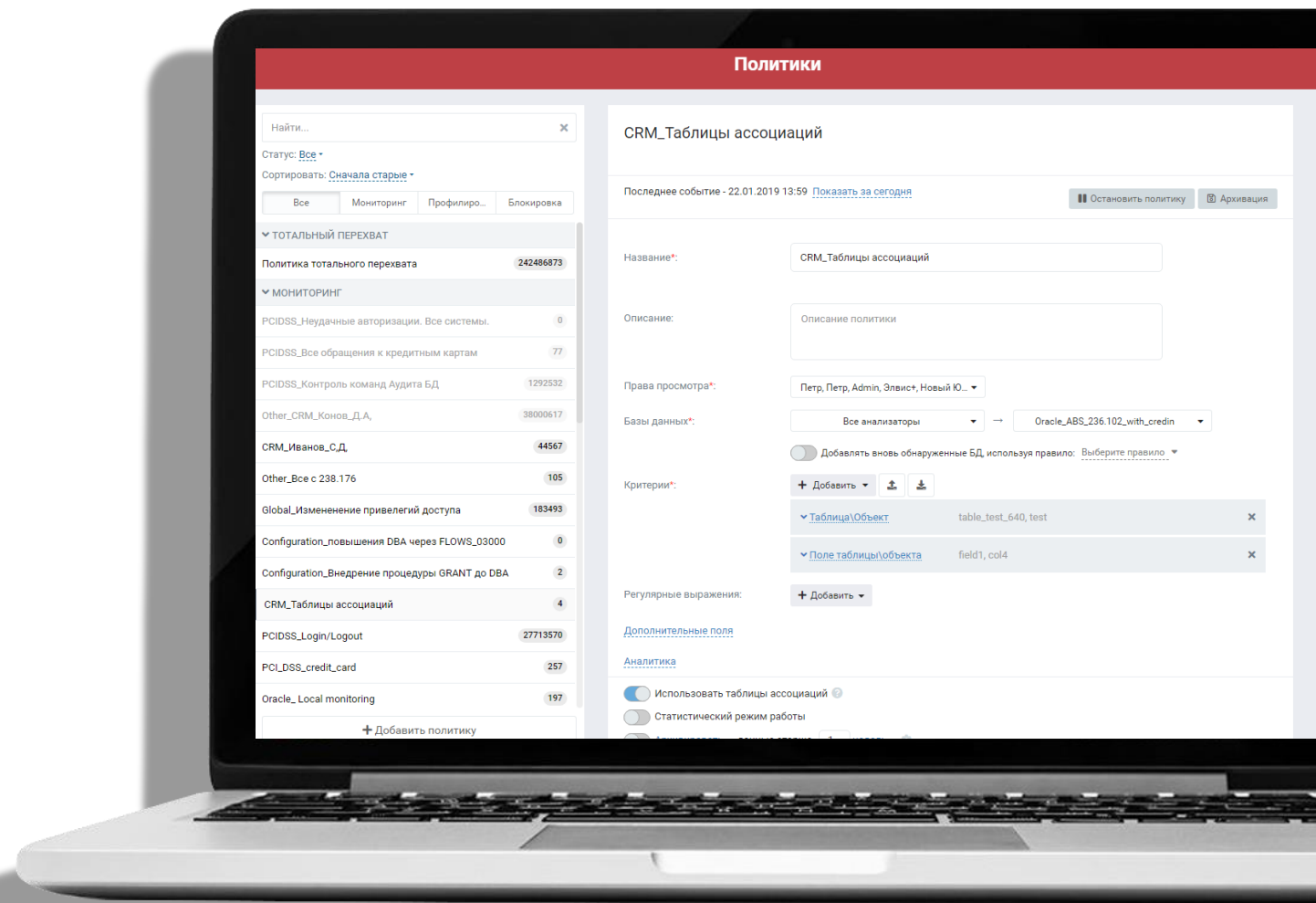
Политики безопасности

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»



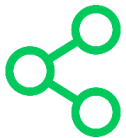
Критерии формирования политик

- 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



Сканирование баз данных

«Защита баз данных» проводит сканирование контролируемых баз данных. Это позволяет решать задачи, связанные не только с контролем доступа, но и с некорректными настройками безопасности.



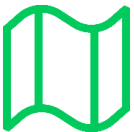
Классификация

- 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) – Тип прав доступа»
- Сравнение текущей картины с эталонной

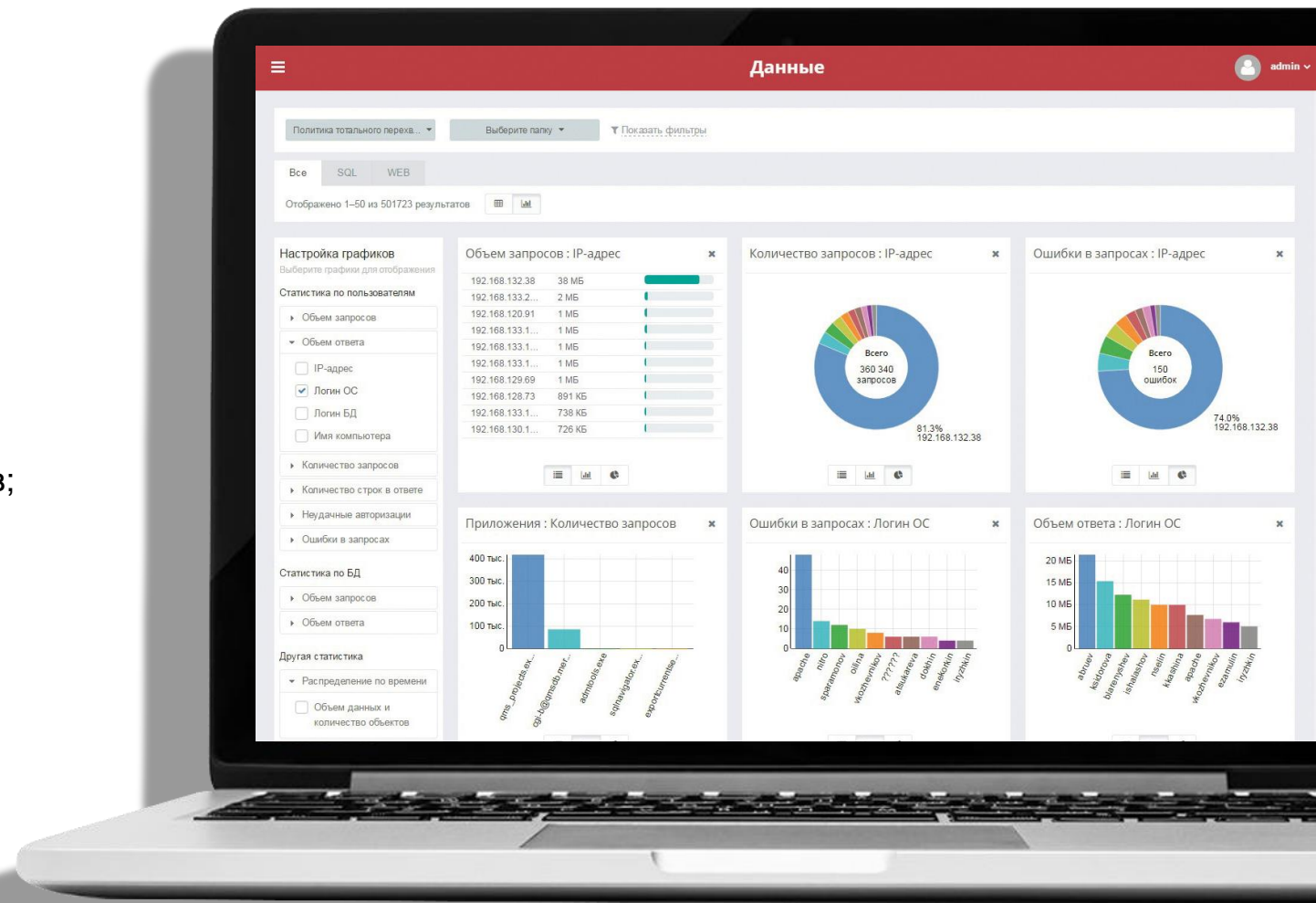


Контроль и аналитика

Встроенные средства аналитики позволяют выявлять отклонения в обычных сценариях работы пользователей БД и предоставляют наглядные статистические отчеты

- Интерактивная отчетность;
- Конструктор отчетов с возможностью анализа любого объема данных за любой промежуток времени;
- Возможность создания индивидуальной панели отчетов;
- Поведенческий анализ пользователей БД (UEBA);
- Уведомление о нарушениях по электронной почте;
- Уведомление о выявленных аномалиях в SIEM.

МЕГАФОН



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 «взрыв»;
- Персонификация пользователей с возможностью выделения учетных записей;
- По протоколам передачи данных HTTP/HTTPS;
- По протоколам аутентификации Kerberos, NTLM;
- Аутентификация (web form authentication).



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



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





Платформа для повышения осведомленности сотрудников

МегаФон SA –

это платформа по повышению осведомленности сотрудников в сфере информационной безопасности с понятным запоминающимся контентом и возможностью проверить знания при помощи имитированных фишинговых атак.



Security Awareness от МегаФона: платформа для повышения осведомленности сотрудников

Платформа в лёгкой и понятной форме повышает осведомлённость сотрудников в сфере информационной безопасности и цифровой гигиены.

При помощи имитации фишинговых рассылок у компании есть возможность проверить степень уязвимости сотрудников к действиям злоумышленника.



Теория

Практика



Обучающие курсы



Тестовые задания



Имитация фишинга



Вирусные вложения



Подробная аналитика



Выявление уязвимых сотрудников

Преимущества платформы «МегаФон SA»



Решение легко интегрировать

Загрузите список пользователей с минимальным набором информации и начинайте работать. Внедрение системы не требует больших трудозатрат.



Авторские курсы

Квалифицированные специалисты Secure-T могут разработать авторские курсы для соответствия платформы целям и задачам компании.



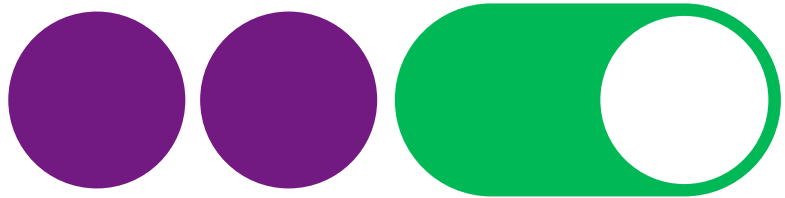
Адаптация под ваши требования

Благодаря гибкости платформы каждый заказчик может адаптировать периодичность обучения, необходимый набор курсов и частоту фишинговых рассылок для соответствия внутренней политике безопасности компании.



Аналитические отчеты

Выгрузка отчетов с подробным описанием процесса прохождения обучения и результатов тестирования сотрудников.



Технологии включают бизнес



Константин Демин
Старший эксперт
Облачные и инфраструктурные решения

+7 924 409 10 39
Konstantin.demin@MegaFon.ru

