ГАРДА ТЕХНОЛОГИИ

ЗДРАВСТВУЙТЕ, ЭТО СЛУЖБА БЕЗОПАСНОСТИ БАНКА

Дмитрий Горлянский

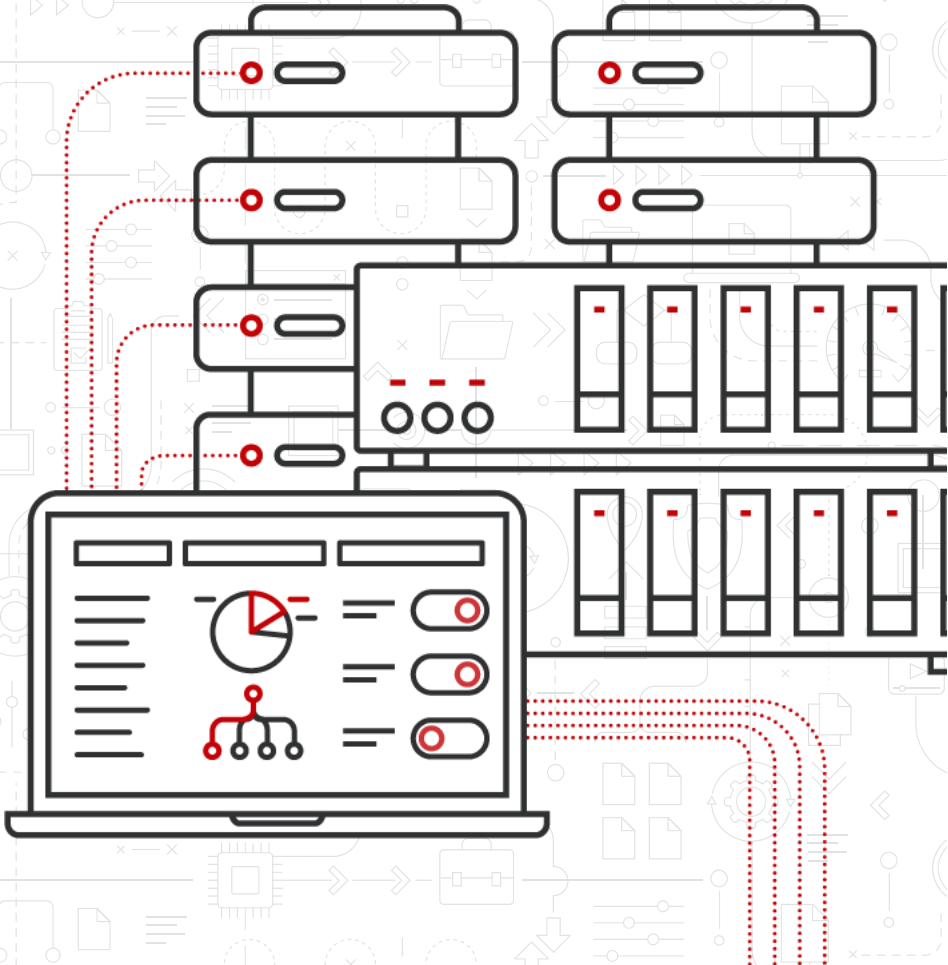
Руководитель направления технического сопровождения продаж

ПРОБЛЕМЫ ДЕТЕКТИРОВАНИЯ УТЕЧЕК НА ПЕРИМЕТРЕ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

- Большое количество возможных каналов
- Неконтролируемые АРМ
- Доступ к данным автоматизированных систем
- Различные форматы передачи данных
- Наличие хранилищ неструктурированных данных



КОНТРОЛЬ ДОСТУПА ВМЕСТО РАСПРОСТРАНЕНИЯ

ГАРДА БД

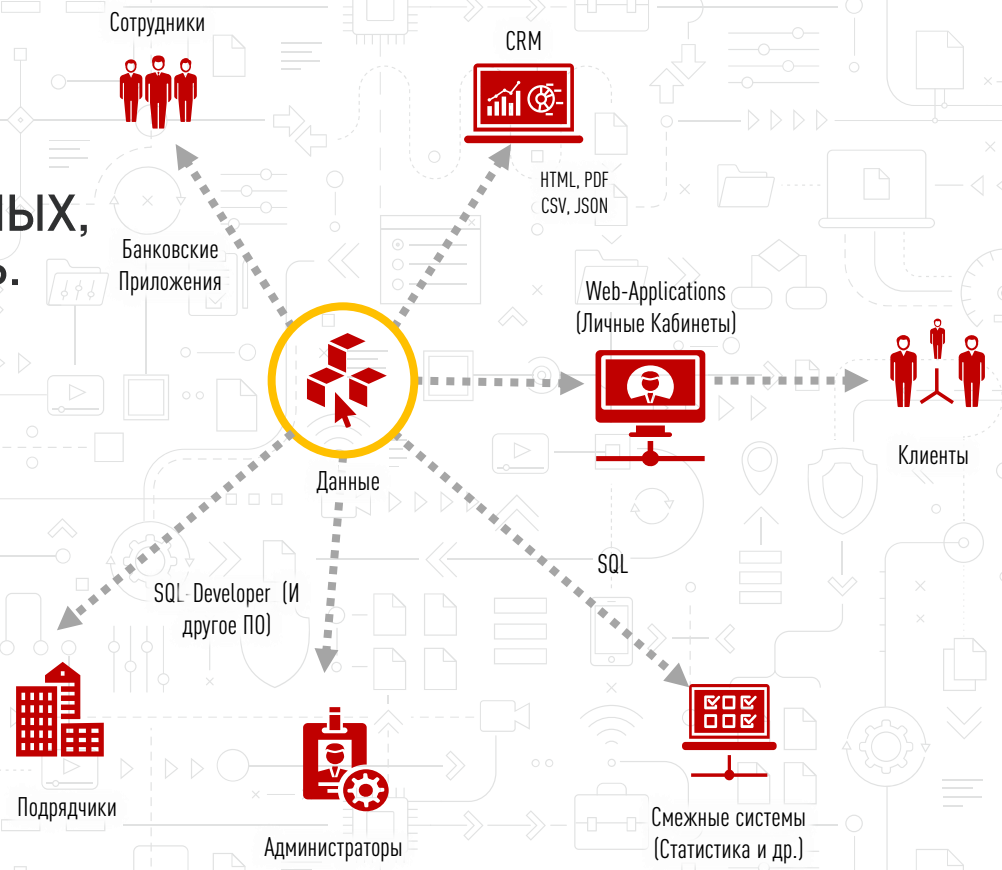
ГАРДА ТЕХНОЛОГИИ

ДАННЫЕ ХРАНЯТСЯ ЦЕНТРАЛИЗОВАНО.

ПРЕЖДЕ ЧЕМ ОСУЩЕСТВИТЬ УТЕЧКУ ДАННЫХ, ЗЛОУМЫШЛЕННИК ДОЛЖЕН ИХ ПОЛУЧИТЬ.

ПРЕИМУЩЕСТВА ПОДХОДА

- ☑ Независимость от каналов доступа
- ☑ Единое представление данных
- ☑ Структурированность данных и их формальное описание



АУДИТ ДОСТУПА СРЕДСТВАМИ СУБД

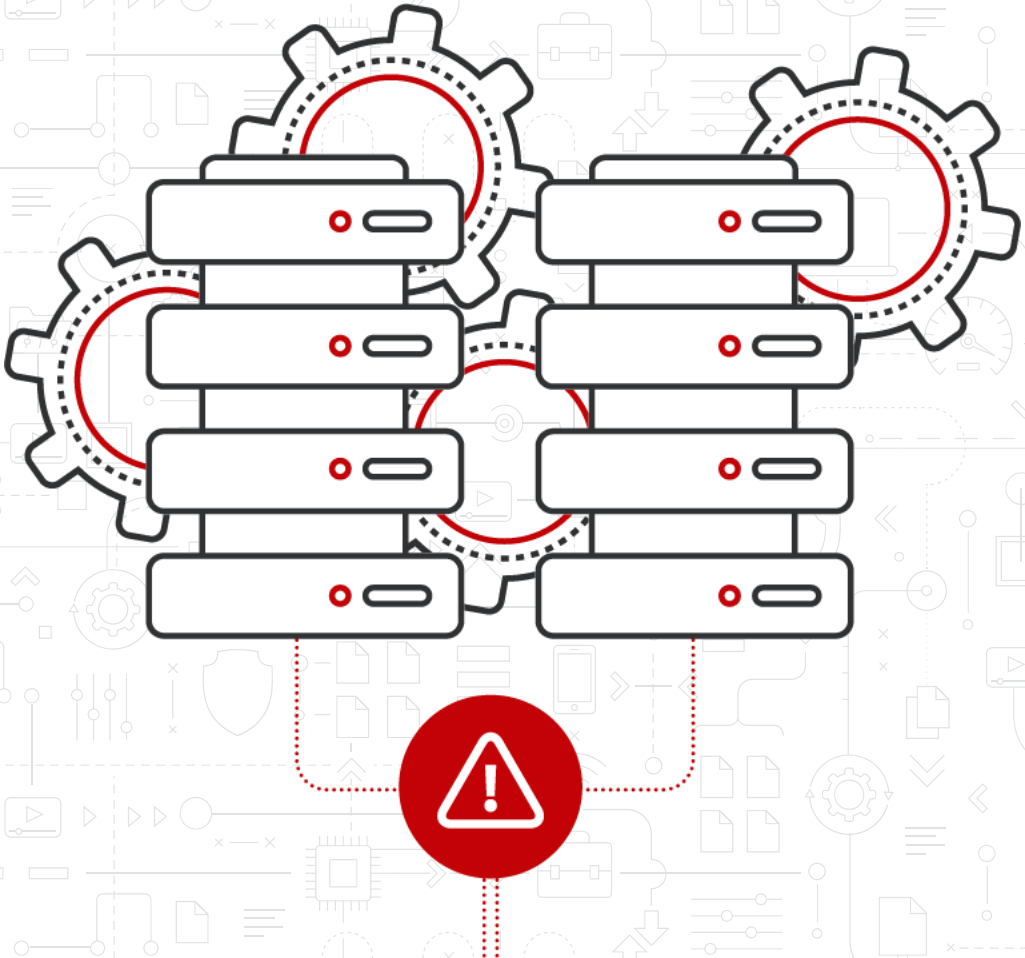
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

АУДИТ ДОСТУПА К ДАННЫМ В СУБД ВХОДИТ ВО ВСЕ МИРОВЫЕ СТАНДАРТЫ БЕЗОПАСНОСТИ.

НЕДОСТАТКИ АУДИТА СРЕДСТВАМИ СУБД

- Нагрузка на аппаратную часть
- Сложность настройки
- Возможность отключения
- Сложность анализа



ВОЗМОЖНОСТИ DAM/DBF СИСТЕМ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

1. АНАЛИЗ ТРАФИКА

Анализ сетевого и локального трафика и проверка на легитимность запросов пользователей и ответов БД.

2. ДОЛГОСРОЧНОЕ ХРАНЕНИЕ ИНФОРМАЦИИ

Обработка данных (например, проверка на регулярные выражения) и сохранение всех запросов и ответов для ретроспективного анализа.

3. ПОИСК БАЗ

Обнаружение всех активных СУБД, выявление фактов их перемещения/изменения. Контроль за созданием новых ИС/АС.

4. СКАНИРОВАНИЕ БАЗ

Классификация данных в СУБД. Выявление уязвимостей СУБД (неоптимальных настроек). Построение матриц доступа к СУБД.

5. АНАЛИТИКА/ОТЧЕТЫ + UBA

Выявление нарушения политик безопасности. Отклонения от модели типичного поведения пользователей.

6. СИСТЕМА ОПОВЕЩЕНИЯ

Дашборды, уведомления о событиях по e-mail, передача данных во внешние SIEM-системы.

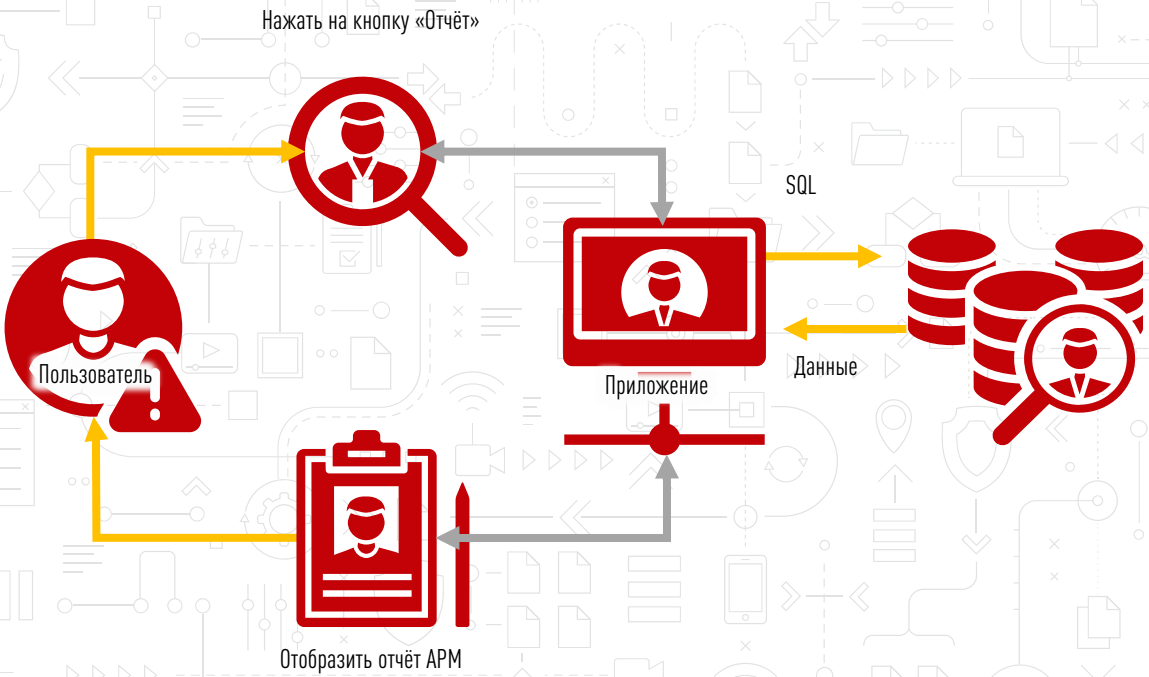
ПРИВЯЗКА ПОЛИТИК К БИЗНЕС-ПРОЦЕССАМ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

ПОЛИТИКИ МОЖНО НАСТРОИТЬ В СООТВЕТСТВИИ С ТИПОВЫМИ ДЕЙСТВИЯМИ ПОЛЬЗОВАТЕЛЯ:

- Аудит действий
- Возможность выявлять нарушения



ВОПРОС:

Как отличить утечку данных от штатной работы?

ПРОБЛЕМЫ КОНТРОЛЯ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ

ГАРДА ФАЙЛЫ

ГАРДА ТЕХНОЛОГИИ

- Большой объём данных и их разнообразие
- Классификация данных
- 60% корпоративных данных – не приносит пользы. Копии, неиспользуемые файлы, медиа контент
- Большое количество пользователей и прав доступа
- Проблемы с настройкой прав
- Нерациональное использование СХД (Актуально для IT)

80% ВСЕЙ КОРПОРАТИВНОЙ ИНФОРМАЦИИ – НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ

Файловые сервера, корпоративные порталы, папки Microsoft Exchange, Microsoft SharePoint, сетевые и облачные хранилища, в которых находится множество различных документов, в том числе и с содержанием критически важной информации

ИСПОЛЬЗОВАНИЕ DAG СИСТЕМ

ГАРДА ФАЙЛЫ

ГАРДА ТЕХНОЛОГИИ

DATA ACCESS GOVERNANCE — СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ К НЕСТРУКТУРИРОВАННЫМ ДАННЫМ

Что за данные хранятся в сетевых папках и на компьютерах сотрудников?

У кого на самом деле есть доступ к данным?

Какие данные наиболее критичны?

Какие данные не используются?

Кто, когда, к каким данным имел доступ?

Кто является ответственным за тот или иной файл / каталог?

- Классификация данных в массиве файловых хранилищ
- Аудит всех действия с данными для анализа в режиме реального времени
- Аудит прав доступа, выявление рисков и проблем
- Детектирование аномальной активности
- Активное реагирование

ОПТИМИЗАЦИЯ СХД

ГАРДА ФАЙЛЫ ГАРДА ТЕХНОЛОГИИ

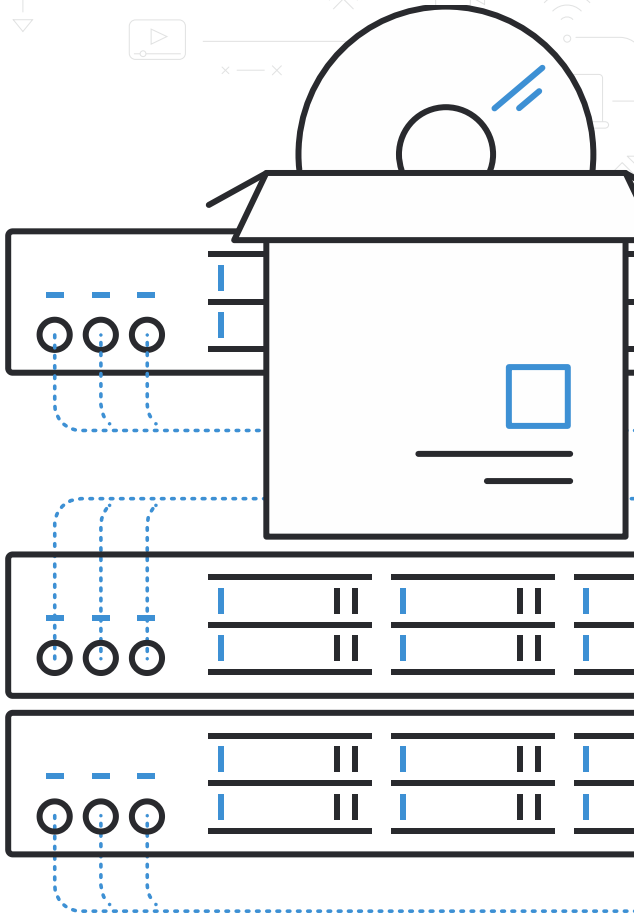
- Графики активности на файловых серверах и других хранилищах неструктурированных данных, выявление периодов повышенной нагрузки

- Причины повышенной нагрузки:
  - Кто из сотрудников или технических учетных записей (приложения и сервисы) является её причиной
  - Какие действия и в каком количестве вызывают эту нагрузку

- Отчеты (в том числе автоматизированные) о файлах с самым большим объёмом, о файлах мультимедиа-форматов (MPEG, AVI и др.)

- Отчеты о дубликатах файлов, их количестве и объеме

- Отчеты о неиспользуемых файлах



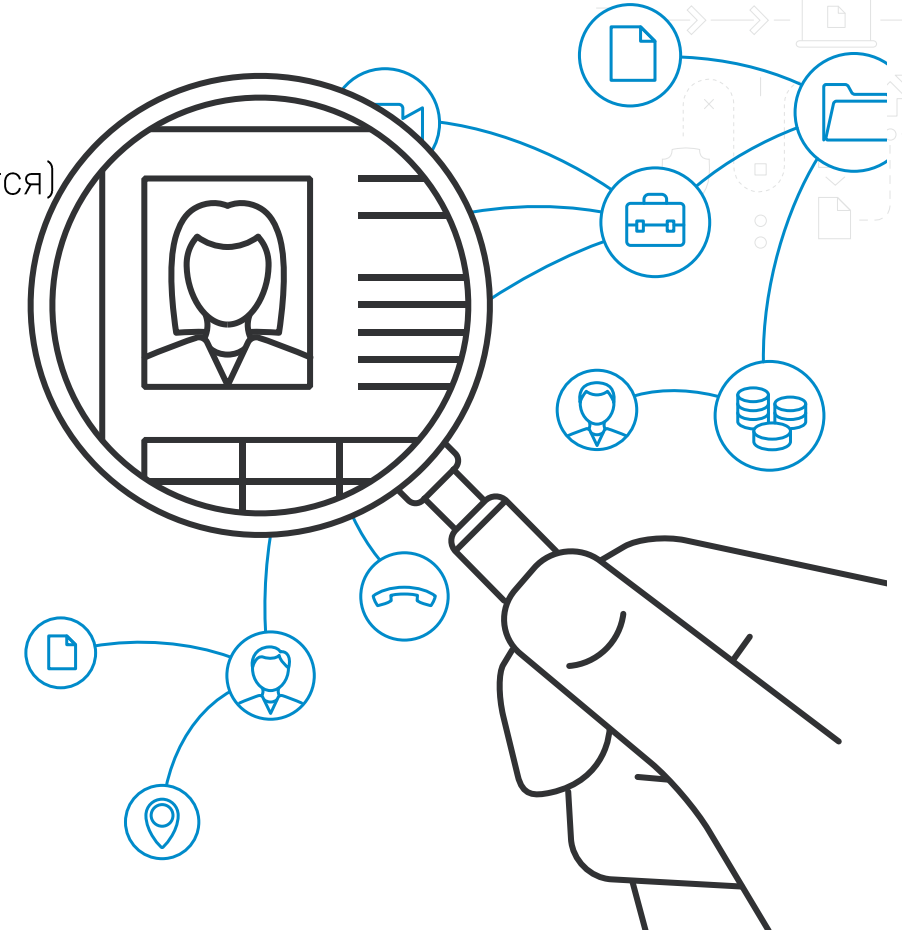
АУДИТ ТЕКУЩИХ РАЗРЕШЕНИЙ К ДАННЫМ

ГАРДА ФАЙЛЫ
ГАРДА ТЕХНОЛОГИИ

Наличие папок и файлов:

- Общедоступных (в т.ч. информация, которая в них содержится)
- С выключенным наследованием прав доступа
- С прямыми разрешениями
- С уникальными правами
- Со “сломанными” ACL

Возможность **сформировать отчёт**
(в наглядном и техническом формате)
по конкретному или по всем найденным рискам.



ПОМОЩЬ В РАССЛЕДОВАНИИ ИНЦИДЕНТА

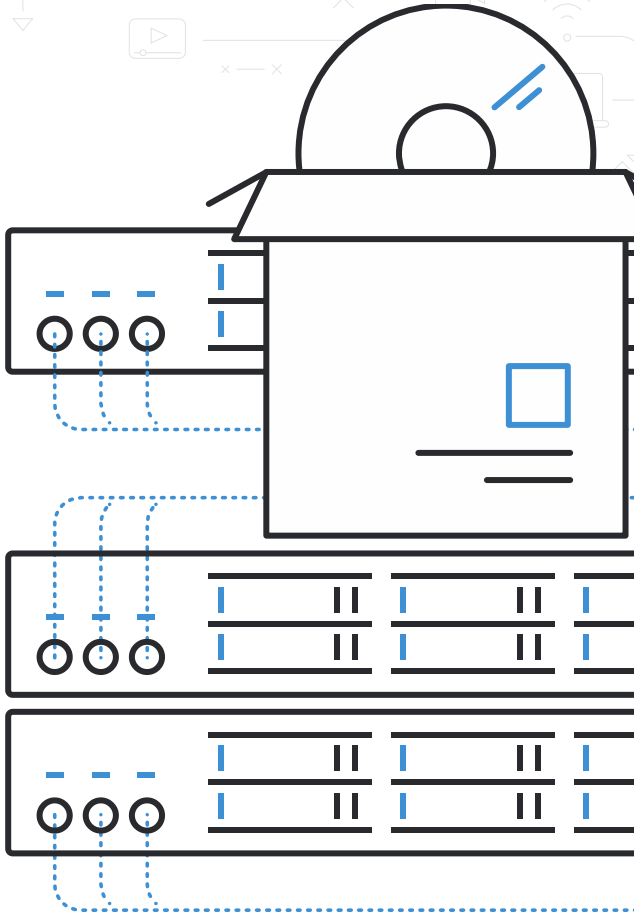
ГАРДА ФАЙЛЫ
ГАРДА ТЕХНОЛОГИИ

- Вся история обращений к файлу
- Все сотрудники, кто обращался к файлу, включая локальные обращения
- Частота и время обращений сотрудников к файлам
- Все дубликаты файла и полная картина работы с ними (информация, возможно, была получена не из наблюдаемого файла, а из его копии)
- Все файлы, доступ к которым имел сотрудник

АНОМАЛЬНАЯ АКТИВНОСТЬ НА ХРАНИЛИЩАХ

ГАРДА ФАЙЛЫ
ГАРДА ТЕХНОЛОГИИ

- Автоматическое в режиме, приближенном к реальному времени, обнаружение отклонений от нормальной активности
- Уведомление ответственных сотрудников
- Активное реагирование: запрет удаление / изменение файлов на указанное время “до выяснение ситуации”, блокировка учетной записи
- Графические отчеты об аномальной активности
- Аномальная активность на отдельно взятом хранилище или суммарно по всем хранилищам



ГАРДА - ЕДИНЫЙ КОМПЛЕКС УПРАВЛЕНИЯ ЦИКЛОМ БЕЗОПАСНОСТИ ДАННЫХ

ГАРДА ТЕХНОЛОГИИ

ГАРДА БД

СУБД

В информационных системах и бизнес-приложениях данные систематизированы и структурированы. Защита – системы DAM.

ГАРДА ПРЕДПРИЯТИЕ

КОММУНИКАЦИИ

Сотрудники передают корпоративные данные «за периметр» самыми разными путями – электронной почтой, мессенджерами, внешними носителями. Защита – системы DLP.

ГАРДА ФАЙЛЫ

СЕТЕВЫЕ ХРАНИЛИЩА

На компьютерах пользователей и в локальных сетевых хранилищах можно найти самые разные данные, включая черновики конфиденциальных документов, копии данных клиентов. Защита – системы DAG.

СПАСИБО ЗА ВНИМАНИЕ!

ГАРДА
ТЕХНОЛОГИИ

info@gardatech.ru
8 (831) 422 12 21
gardatech.ru