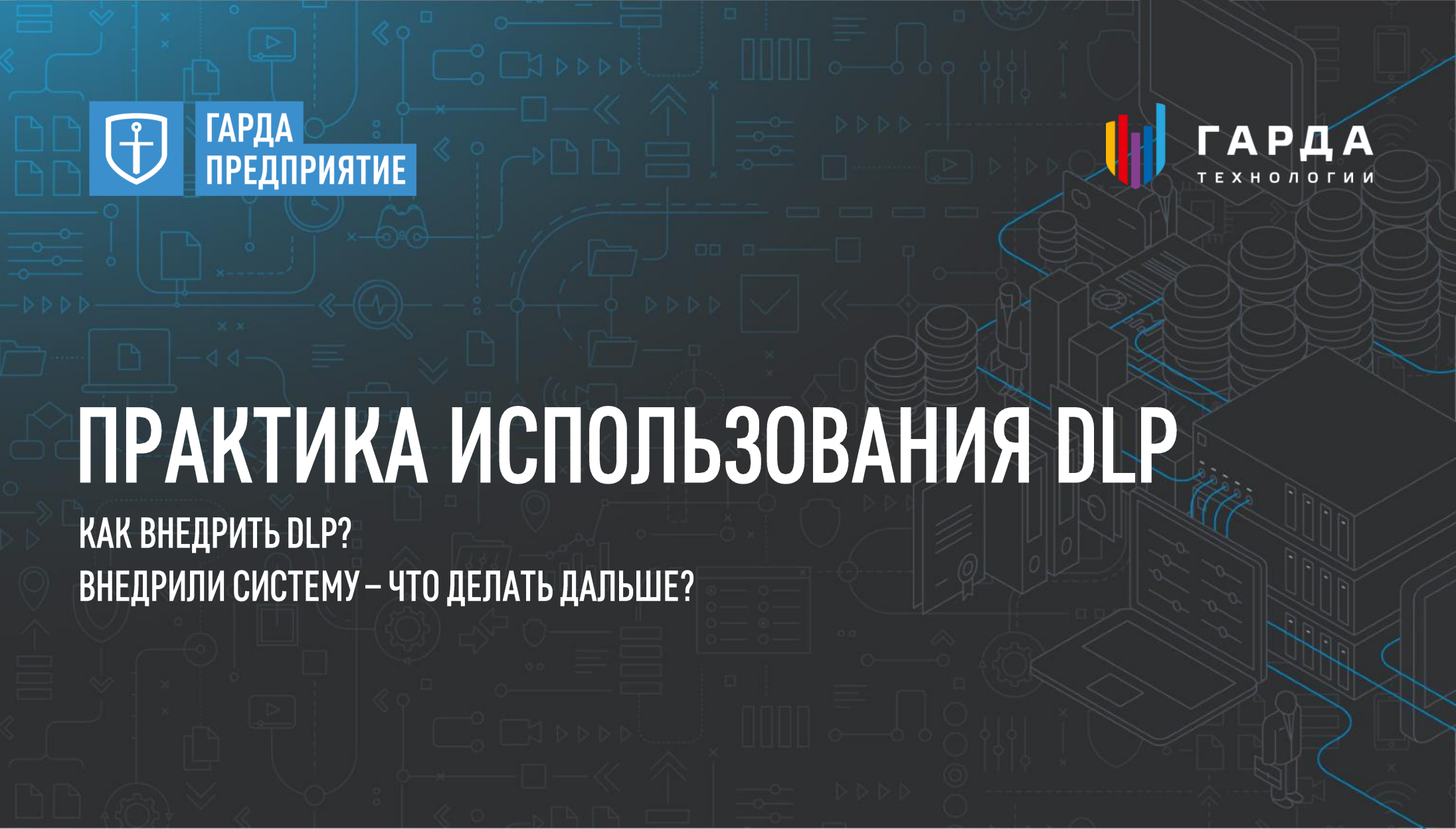
ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ПРАКТИКА ИСПОЛЬЗОВАНИЯ DLP

КАК ВНЕДРИТЬ DLP?

ВНЕДРИЛИ СИСТЕМУ – ЧТО ДЕЛАТЬ ДАЛЬШЕ?

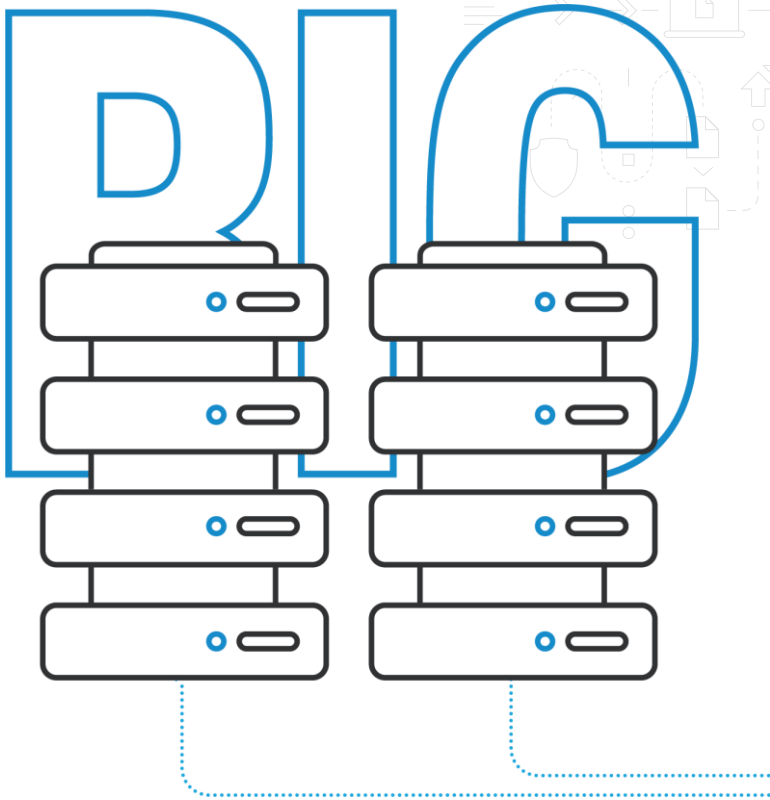


ХРАНЕНИЕ ДАННЫХ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ПРЕДПРИЯТИЕ — ОДНА ИЗ ПЕРВЫХ DLP-СИСТЕМ, СПРОЕКТИРОВАННЫХ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ BIG DATA



Подсистема хранения — эксклюзивная разработка Гарда Технологии, созданная для решения актуальных проблем обычных DLP-систем и обеспечивает:

BIG DATA

- Хранение широкого спектра данных, обрабатываемых в компании – сведения об инцидентах, маркеры информационных потоков, факты совершения коммуникаций между объектами наблюдения и т.д.
- Высокую скорость доступа к данным – их анализ, и быстрый поиск;
- Низкую стоимость хранения по сравнению со схожими решениями.

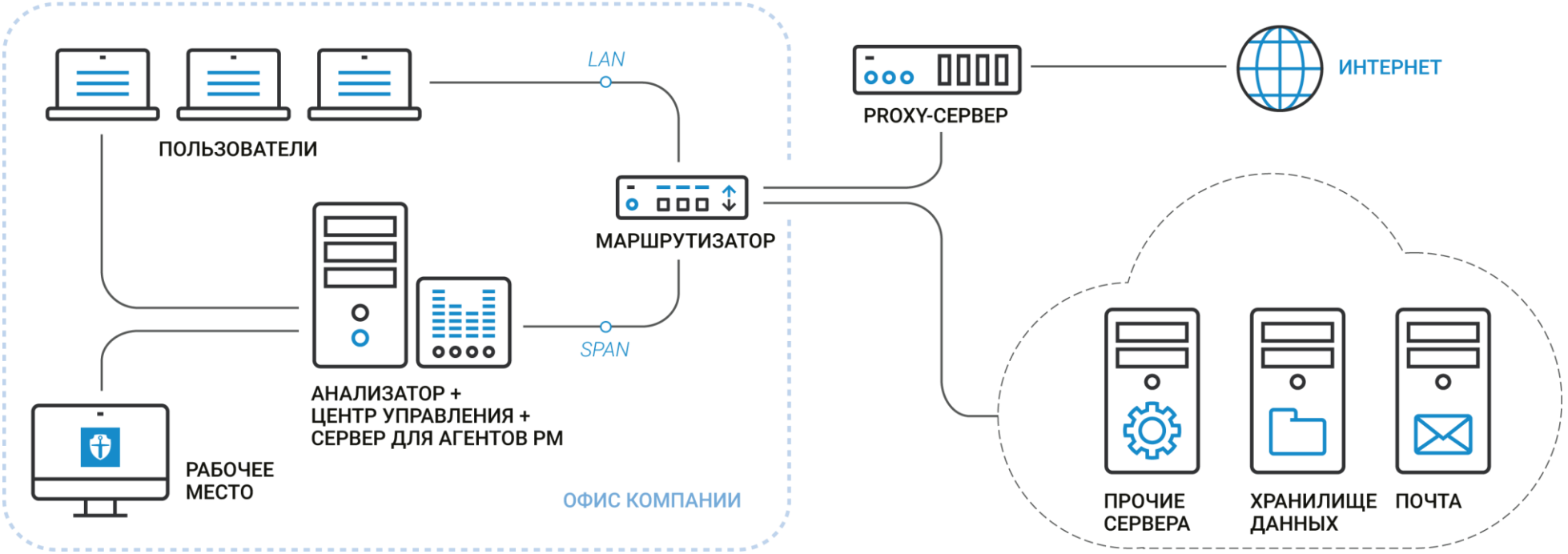
Данные поступают в комплекс из различных источников (сетевой трафик, почтовые серверы, рабочие места и др.) и хранятся в собственной базе для дальнейшего анализа.

СХЕМА ВНЕДРЕНИЯ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

Вся **функциональность системы**, включая управление агентами рабочих мест, работу с https, перехват и анализ трафика, хранение данных, поставляется на 1U/2U или 4U сервере, в зависимости от количества рабочих мест и требуемого периода хранения.



КОНТРОЛЬ РАБОЧИХ МЕСТ

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ПОДДЕРЖКА ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ УСТАНОВКИ АГЕНТА ГПР

WINDOWS

- Windows XP SP3
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2008, 2012

LINUX

- Astra Linux Special Edition версии 1.6 и выше
- Astra Linux Common Edition версии 1.9 и выше
- Ubuntu версии 16 и выше

MAC OS

Версии 10.13 и выше

КОНТРОЛЬ РАБОЧИХ МЕСТ

ОБЕСПЕЧЬТЕ КОМПЛЕКСНЫЙ МОНИТОРИНГ КОМПЬЮТЕРОВ «ГАРДА ПРЕДПРИЯТИЕ» 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 (Соц.сети, веб-почта и др. 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

ВНЕДРЕНИЕ DLP ≠ УСТАНОВКА

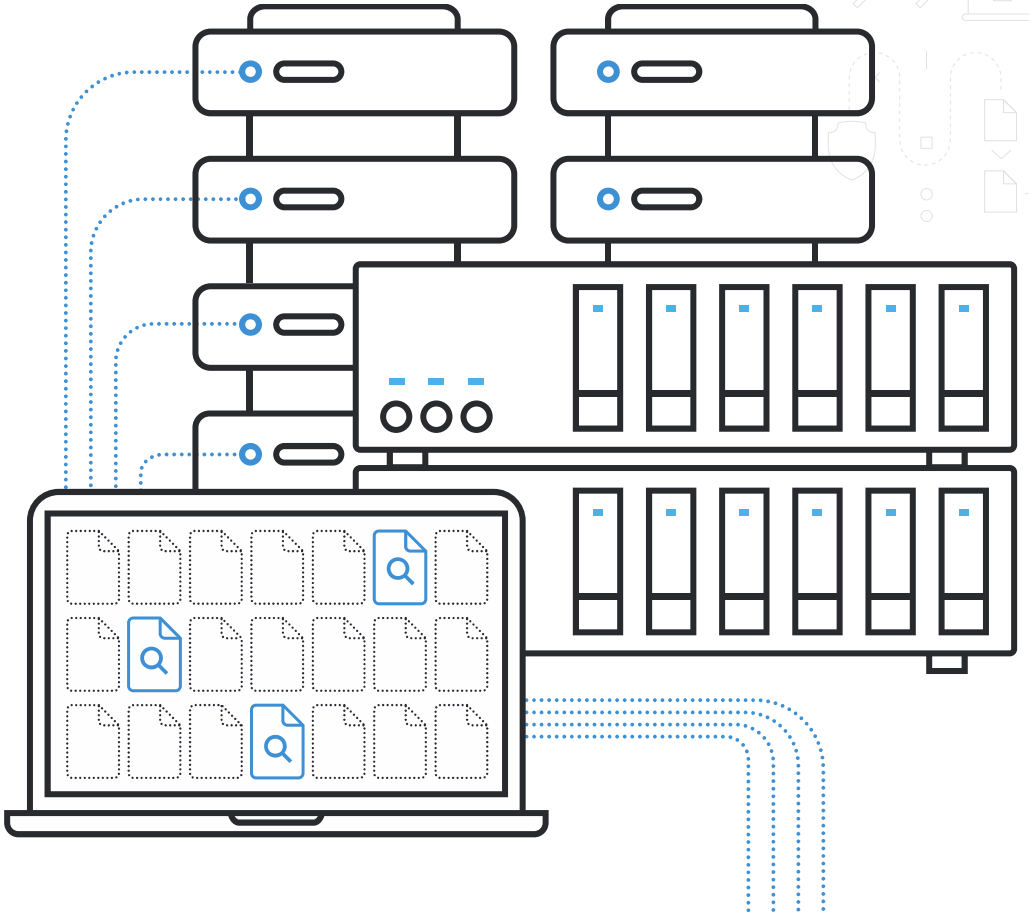
ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

МНОГИЕ ВНЕДРЕНИЯ DLP СИСТЕМ «ЗАСТРЕВАЮТ» НА СТАДИИ ВНЕДРЕНИЯ И ДОЛГОЕ ВРЕМЯ ПРОСТАИВАЮТ И НЕ ПРИНОСЯТ НИКАКОЙ ПОЛЬЗЫ.

Причины:

- Нет понимания что нужно настроить
- Нет понимания защищаемой информации
- Предустановленные политики работают не так как хотелось
- Не все инциденты можно описать политиками
- Большое количество исключений из правил



ИНСТРУМЕНТЫ DLP

ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

ОСНОВНЫЕ:

- Анализ по ключевым словам
- Цифровые отпечатки документов
- Словари
- Регулярные выражения
- Каналы передачи

ДОПОЛНИТЕЛЬНЫЕ:

- Детектирование форматов файлов
- Скриншоты и клавиатурный ввод
- Отправители\получатели
- Статистические отчёты

Так же важно уметь пользоваться их комбинацией.

КОСВЕННЫЕ ПРИЗНАКИ ИНЦИДЕНТОВ

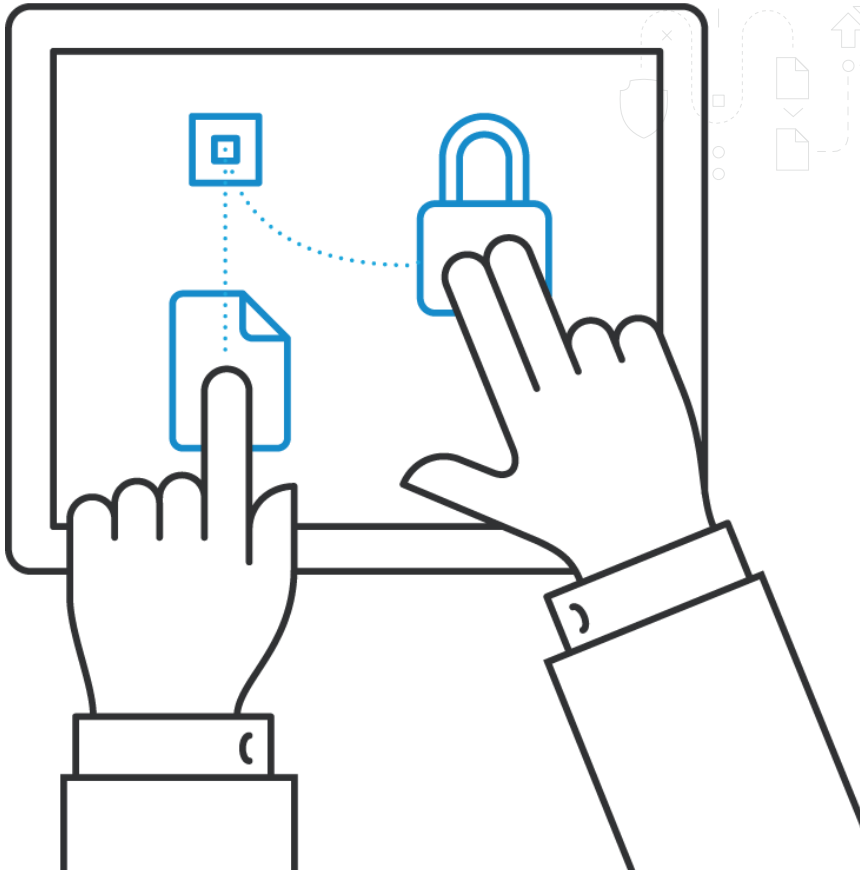
ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

СЛЕДУЕТ ОТЛИЧАТЬ САМИ ИНЦИДЕНТЫ И КОСВЕННЫЕ ПРИЗНАКИ ИНЦИДЕНТОВ.

Часть инцидентов может быть обнаружена только по косвенным признакам.

Соответственно, данные инциденты требуют дополнительного анализа и не могут быть выявлены исключительно автоматизированными средствами.



ГАРДА ПРЕДПРИЯТИЕ

ГАРДА ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!

БЛОК ВОПРОСОВ И ОТВЕТОВ.