Безопасность и анализ конечных точек

Предпосылки

- Массовый переход на удаленный режим работы
- Неготовность многих организаций к массовым удаленным подключениям пользователей
- Повышенное внимание злоумышленников к личным и корпоративным устройствам в домашних и публичных сетях
- Отсутствующая или крайне слабая защита домашних и публичных сетей

Защищаемые активы

- Личные и корпоративные ПК пользователей
- Сервисы организаций
- Каналы связи
- Мобильные устройства пользователей

Защита корпоративных устройств.

- Проверки рабочей станции на соответствие политикам
- Дополнительная антивирусная защита
- Контроль устройств для мобильных и ноутбуков
- Усиление политик межсетевого экранирования, имплементация ролевой модели доступа к ресурсам

Защита корпоративных устройств

- VPN-клиенты (Check Point, Fortinet, Palo Alto)
- Агенты защиты конечных точек (Check Point SandBlast Agent, Fortinet FortiClient, Palo Alto Global Protect Agent)
- MDM/EMM (MobileIron)
- Усиление политик межсетевого экранирования, имплементация ролевой модели доступа к ресурсам (сервисы Softline и Инфосекьюрити)

Агенты защиты конечных точек

- Конечные точки часто являются целью первоначальных атак. Одно недавнее исследование показало, что 30% нарушений связаны с установкой вредоносного ПО на конечных точках. FortiClient усиливает безопасность конечных точек за счет интегрированной видимости, контроля и упреждающей защиты. Имея возможность обнаруживать, отслеживать и оценивать риски конечных точек, можно гарантировать соответствие требованиям безопасности конечных точек, снижать и ликвидировать риски. FortiClient активно защищает от продвинутых атак.

- Для эффективного отслеживания поведения устройств и своевременной идентификации потенциальных рисков необходим контроль доступа к сети. Упреждающая (*предсказывающий; опережающий, антиципирующий, предупредительный, предваряющий, предвосхищающий, предупреждающий*) стратегия безопасности конечных точек показывает свою эффективность в организациях всех размеров.

Отслеживание состояния и управление конечными точками

Функции сбора телеметрических данных конечных точек, сканирования на наличие уязвимостей и динамического управления доступом повышают эффективность системы безопасности в целом.

Упреждающая защита конечных точек

Система безопасности использует функции защиты от вредоносного ПО на базе технологии машинного обучения, защиты от эксплойтов, Web Filtering, межсетевой экран защиты приложений и интегрированную «песочницу» для противодействия атакам на конечные точки.

Защита конечных точек в современных условиях

- Несмотря на повсеместное распространение облачных технологий и тенденции к размытию периметров безопасности, важность защиты локальных конечных точек корпоративной сети ощущается сегодня всё так же остро, как и десять лет назад. Ведь в итоге именно эти рабочие станции и серверы являются целью злоумышленников, той площадкой, на которую они «приземляются» в ходе атаки. При этом ключевым бастионом безопасности, защищающим конечные точки от киберугроз, долгое время был (а в ряде случаев и остаётся) классический антивирус, использующий сигнатурный анализ. Как должны измениться подходы к защите конечных точек, чем отличаются современные антивирусы от своих предшественников и что нужно сделать, чтобы построить эффективную систему безопасности рабочих станций.
- Основной инструмент, который используется для защиты рабочей станции, — это сигнатурный анализ вредоносного кода. Изначально для этих целей применялся обычный антивирус, однако с появлением источников данных, способных его обойти, возникла необходимость дополнительных инструментов — комплексных решений для защиты рабочей станции.
- Говоря о защите конечных точек, можно выделить следующие категории угроз: вредоносные файлы; эксплойты; скрипты, использующие функциональные возможности легитимных инструментов операционной системы; фишинг; мобильные угрозы; инсайдеры и ошибки пользователей.

Комплексная защита конечных точек и реагирование

- **Останавливает вредоносные программы и вымогатели -** Ловушки предотвращают запуск вредоносных исполняемых файлов, библиотек DLL и файлов Office с помощью нескольких методов предотвращения, уменьшая поверхность атаки и повышая точность предотвращения вредоносных программ.
- **Обеспечивает защиту на основе поведения -** Сложные атаки, в которых используются несколько легальных приложений и процессов, встречаются чаще, их трудно обнаружить, и для их сопоставления требуется наглядность. Traps обнаруживает и прекращает атаки путем отслеживания вредоносного поведения в последовательности событий и прекращают атаку при обнаружении.
- **Блокирует эксплойты и атаки без файлов -** Вместо того, чтобы фокусироваться на отдельных атаках, Traps блокирует методы эксплойтов, которые используют атаки. Делая это на каждом этапе попытки эксплойта, Traps прерывает жизненный цикл атаки и делает угрозы неэффективными

- **Координирует действияс сетью и облаком -** Тесная интеграция между сетью, конечной точкой и облаком позволяет постоянно улучшать состояние безопасности и обеспечивает многоуровневую защиту от атак нулевого дня. Всякий раз, когда брандмауэр видит новую вредоносную программу или конечная точка обнаруживает новую угрозу, средства защиты становятся доступными в течение нескольких минут для всех других брандмауэров и конечных точек следующего поколения, на которых выполняется Traps без каких-либо усилий со стороны администратора, будь то в час или в три часа ночи
- **Обнаружение и реагирование на сложные атаки -** Traps использует озеро данных Cortex ™ для хранения всех захваченных событиях и инцидентах, что обеспечивает бесшовную интеграцию с Cortex XDR для расследования и реагирования на инциденты. Cortex XDR, облачное приложение для обнаружения и реагирования, которое позволяет SecOps останавливать сложные атаки и адаптировать защиту в режиме реального времени. Сочетая богатые данные о сети, конечных точках и облаке с аналитикой, Cortex XDR дает:
  - Автоматическое определение основной причины, чтобы ускорить сортировку и реакцию на инцидент
  - Сокращение времени и опыта, требуемого от сортировки до поиска угроз.
  - Отвечать на угрозы быстрее и адаптировать защиту на основе полученных знаний, делая следующий ответ еще быстрее

Управление уязвимостями

ИТ-инфраструктура динамична и ее надо постоянно контролировать (появление новых узлов, портов…). Уязвимости же присущи любой сети и любому ее компоненту. Поддержание приемлемого уровня информационной безопасности в условиях, когда каждый день появляются десятки новых способов обхода мер безопасности, реализуется внедрением практик управления уязвимостями (Vulnerability Management)

Какие задачи позволяет решить

- ✔ Управление уязвимостями
- ✔ Инвентаризация и классификация активов
- ✔ Найти уязвимость
- ✔ Ошибки в конфигурациях
- ✔ Приоритезация найденных уязвимостей и проблем с конфигурациями

Управление конфигурациями

- Самые многочисленные недостатки ИБ в инфраструктуре – некорректные настройки систем. При большом количестве ресурсов в сети задачи по управлению их настройками безопасности практически невозможно решить без применения специальных средств. SCM-решения позволяют управлять соответствием требований международных и национальных стандартов, лучших практик, внутренним политикам организации.

Какие задачи позволяет решить

- ✔ Оценка ресурсов на соответствие техническим требованиям
- ✔ Контроль соответствия

  динамика изменений

  сравнение различных состояний ресурсов
- ✔ Инструментарий для настройки

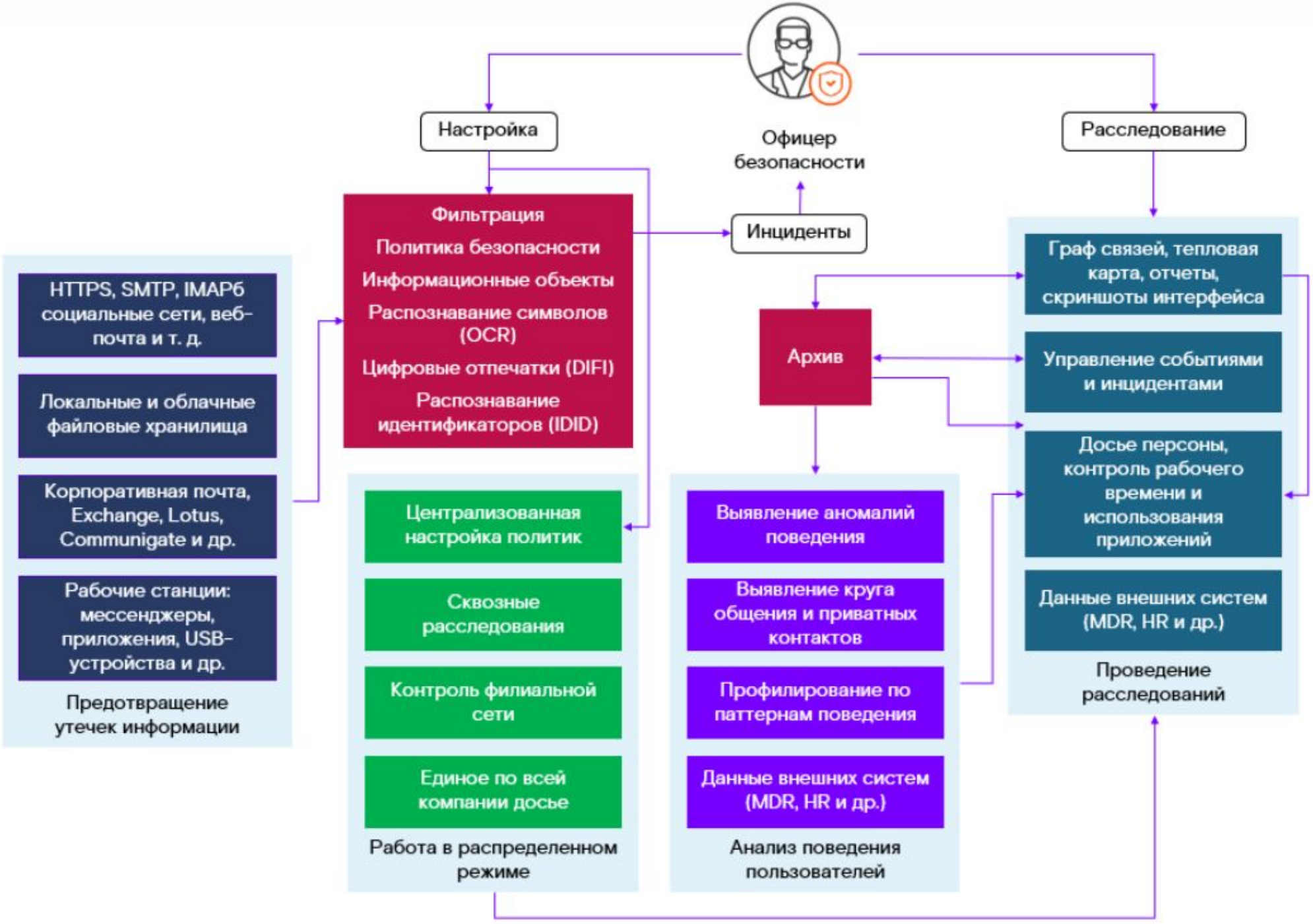
  настройка ресурсов непосредственно из интерфейса

Защищенный мессенджер

Использование популярных мессенджеров (WhatsApp, Telegram…) для обмена чувствительной информацией несет существенные риски, они не являются гарантом того, что данные будут в полной безопасности. Вся информация в этом случае будет храниться на удалённых серверах, откуда может быть извлечена третьими лицами или спецслужбами. Для обеспечения гарантированного уровня безопасности применяются корпоративные защищенные мессенджеры с размещением всей информации в инфраструктуре заказника, либо в защищен

- Задачи, решаемые при внедрении Rendall - это защищённый корпоративный мессенджер, созданный для защиты корпоративной коммуникации в ключевых отделах компаний. Rendall может быть установлен на серверах компании под её полным контролем, не хранит информацию на конечных устройствах пользователей, использует лучшие и проверенные алгоритмы сквозного шифрования. Rendall позволяет Заказчику полностью контролировать корпоративную информацию и соответствует рекомендациям ISO27002 по управлению информационной безопасностью.
- Безопасная коммуникация в кругу руководителей и уполномоченных сотрудников;
- Оперативное и безопасное управление бизнес-процессами
- Обеспечение надежной защиты оперативной информации, передаваемой в компании и контроль над ее распространением
- Введение единого корпоративного стандарта защищенной коммуникации.ному облаке.

Актуальные векторы атак


Настройка
Офицер безопасности
Расследование
Фильтрация
Политика безопасности
Информационные объекты
Распознавание символов (OCR)
Цифровые отпечатки (DIFI)
Распознавание идентификаторов (IDID)
Инциденты
HTTPS, SMTP, IMAPб социальные сети, веб-почта и т. д.
Локальные и облачные файловые хранилища
Корпоративная почта, Exchange, Lotus, Communigate и др.
Рабочие станции: мессенджеры, приложения, USB-устройства и др.
Предотвращение утечек информации
Архив
Граф связей, тепловая карта, отчеты, скриншоты интерфейса
Управление событиями и инцидентами
Досье персоны, контроль рабочего времени и использования приложений
Данные внешних систем (MDR, HR и др.)
Проведение расследований
Централизованная настройка политик
Сквозные расследования
Контроль филиальной сети
Единое по всей компании досье
Работа в распределенном режиме
Выявление аномалий поведения
Выявление круга общения и приватных контактов
Профилирование по паттернам поведения
Данные внешних систем (MDR, HR и др.)
Анализ поведения пользователей