ПОЦЕСС УПРАВЛЕНИЯ АКТИВАМИ ГЛАЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Директор по информационной безопасности ПАО ДОМ.РФ

Дмитрий Шарапов

ОТВЕТЬ НА ВОПРОС: ЧТО ТЫ ЗАЩИЩАЕШЬ?

Прежде чем что-то защищать, нужно ответить на один вопрос: Что ты защищаешь?

- Без понимания цифрового актива и его свойств невозможно проработать, выставить, применить и проконтролировать требования информационной безопасности.

ЧТО ТАКОЕ ЦИФРОВОЙ АКТИВ ?

- Цифровой актив — это средство, используемое для передачи, обработки и хранения какой-либо информации. Это может быть персональный компьютер, сервер, сетевое оборудование или даже камера.

КАК НАЧАТЬ УПРАВЛЯТЬ АКТИВАМИ ?

- Необходимо проработать стратегию по поиску и агрегации информации об активе и его свойствах в централизованной информационной системе, например в решении класса CMDB. Такие системы могут быть как коробочными, так и основанными на открытом исходном коде

НАХОДИМ ЦИФРОВЫЕ АКТИВЫ

АКТИВНЫЙ

Ключевой аспект, это выбор способа поиска цифровых активов

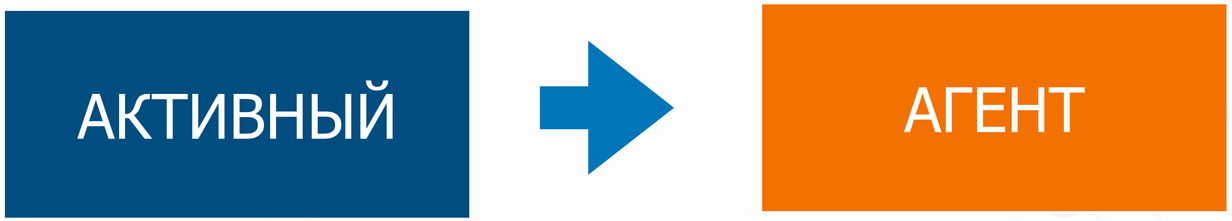
Возможности

- Поиск базовой информации

Недостатки

- сегментация
- распределенная инфраструктура
- скорость

УЛУЧШАЕМ ПОИСК ЦИФРОВЫХ АКТИВОВ



Возможности

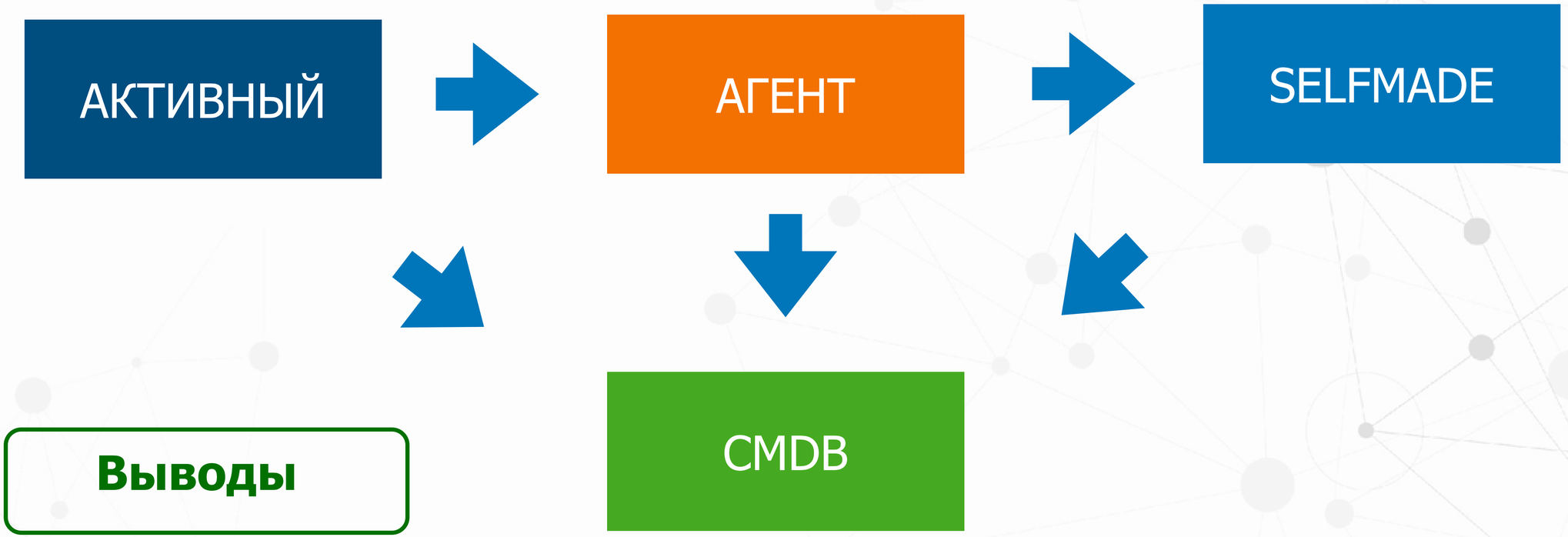
- Получение расширенной информации

НАЧИНАЕМ ПОНИМАТЬ КАК УПРАВЛЯТЬ АКТИВАМИ

Возможности

- Получение расширенной информации
- Получение информации для обогащения из внешних источников

УПРАВЛЯЕМ АКТИВАМИ



Выводы

- Почти научились управлять активами
- Требуется использовать комбинированный подход, где мы сочетаем понимание ИТ-Ландшафта и используем комплексный подход по сбору такой информации

ВАЖНО! АКТУАЛИЗИРОВАТЬ СВЕДЕНИЯ

- Система, где хранится итоговая информация, должна учитывать актуальность данных — иначе она быстро превратится в свалку устаревших сведений

КТО ДОЛЖЕН УПРАВЛЯТЬ ЭТИМИ ПРОЦЕССАМИ ?

- В разных организациях по разному, это может быть совместными усилиями ИТ(CMBD) и ИБ(Активные сканеры)

Риски

- уровень доверия

УРОВЕНЬ ДОВЕРИЯ ЦИФРОВОГО АКТИВА

- При выстраивании комбинированного подхода к сбору информации о свойствах цифрового актива, чем больше источников мы можем сопоставить между собой, тем выше достоверность полученных данных. Например, баннерная проверка ресурса даёт лишь ограниченное представление о типе актива, тогда как дополнительные методы — аудитное сканирование или получение данных от агентов — позволяют существенно повысить уровень доверия.

- Уровень доверия цифрового актива это один из ключевых аспектов, чем выше уровень доверия к цифровому активу, тем надежнее будет проверка в части контроля категории цифровых активов по применению требований информационной безопасности.

КАТЕГОРИРОВАНИЕ

- Когда мы научились управлять процессом по поиску и описанию цифровых активов мы должны определить по каждому набору цифровых активов их категории, например, мультимедиа, принтеры, камеры, сетевое оборудование, серверное оборудование, рабочие ПК и так далее

Важно ?

- при моделировании угроз и экспертной оценке со стороны внутренней команды мы формируем не единые типовые требования для всех категорий (что может быть дорого), а индивидуальные требования под каждую конкретную категорию активов

ПРИОРИТЕЗАЦИЯ

- Например: внешний периметр, автоматизированные системы критической информационной инфраструктуры, ИСПДн и так далее
- Где то мы будем принимать решения о приоритетах по внедрению требований на внешнем контуре, а где то будем принимать решения по регуляторным требованиям

Важно !

- невозможно сразу реализовать все свои идеи, требования и мероприятия, а также обеспечить всесторонний контроль.
- необходимо поэтапное внедрение мер и практик информационной безопасности в отношении различных цифровых активов (категорий)

КОНТРОЛЬ

- Требования были проработаны и применены, но можем ли мы быть уверены, что завтра они будут выполняться в полном объеме? Например, может появиться новый узел, измениться версия операционной системы или установиться дополнительное прикладное программное обеспечение и т. п.
- Необходимо реализовать автоматизированные решения, способные консолидировать требования информационной безопасности по заданным категориям и на регулярной автоматизированной основе проверять соответствие цифровых активов этим требованиям (включая контроль изменений их свойств). Такие решения могут быть как коробочными, так и основанными на открытом исходном коде.

Важно !

- ИТ-Инфраструктура это большой организм, которые постоянно изменяется, активы появляются, убывают или изменяют свой вид.

ГЛУБИНА

- Глубина контроля отдельный цифровых активов позволит повысить уровень защищенности, чем больше метрик мы можем контролировать (например, антивирус запущен, антивирус получил последние обновления, запуск сканирований, версии и тп.)

Важно !

- это позволит нам настроить триггеры, на основании которых мы сможем увидеть отклонения, например, антивирус выключен, давно не подключался к серверу обновлений, это позволит на постоянной основе выявлять отклонения или как раз те изменения про которые мы говорили в ИТ-Инфраструктуре.

ISO МОДЕЛЬ УПРАВЛЕНИЯ АКТИВАМИ

- Планирование (стратегия)
- Описание цифрового актива
- Подготовка платформы для сбора информации
- Внедрение практик сбора данных об активах
- Категоризация активов
- Приоритезация (подход «едим слона по частям»)
- Контроль соответствия
- Глубинный анализ (стремимся получить максимум метрик)
- Alert → замыкание цикла

СПАСИБО ЗА ВНИМАНИЕ!