MAKVES
ТЕПЕРЬ ЧАСТЬ GARDA

КАК ЗАЩИТИТЬ ВАЖНЫЕ ДАННЫЕ. ПОДХОД MAKVES

Роман Подкопаев

НОВАЯ РЕАЛЬНОСТЬ = НОВЫЕ РИСКИ

Количество кибератак растет
Главная цель – нанести ущерб российским компаниям

Массовые утечки данных
Данные приходится защищать от внешних атак

Источник: Positive Technologies. Актуальные киберугроз: итоги 2022 года

ПРИЧИНЫ

Команды ИТ и ИБ перегружены работой и лишними уведомлениями

Отсутствует контроль работы с конфиденциальной информацией. Утечки данных фиксируются по факту пересечения периметра

Сложно понять, где хранится критичная для бизнеса информация и ее копии

ДАННЫЕ СТАНОВЯТСЯ УЯЗВИМЫМИ ДЛЯ КИБЕРАТАК И МОШЕННИЧЕСКИЙ ДЕЙСТВИЙ

РАСТЕТ НАГРУЗКА НА ИТ, СНИЖАЕТСЯ ПРОИЗВОДИТЕЛЬНОСТЬ

DCAP – НОВЫЙ ПОДХОД К ЗАЩИТЕ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

MAKVES теперь часть ГАРДА

ИТ-ИНФРАСТРУКТУРА И ИСТОЧНИКИ ДАННЫХ


Доменные службы


Серверы, СХД


Рабочие станции


Почтовые серверы


Облачные хранилища

РЕЗУЛЬТАТЫ

- ✓ СОКРАЩЕНИЕ ПОВЕРХНОСТИ КИБЕРАТАКИ
- ✓ КОМПЛАЕНС
- ✓ АВТОМАТИЗАЦИЯ РУТИНЫ
- ✓ ЗАЩИТА ИНФОРМАЦИИ

Возможности современных DCAP-систем

MAKVES теперь часть ГАРДА

АУДИТ ДОСТУПА
К ИНФОРМАЦИОННЫМ РЕСУРСАМ: ФАЙЛОВЫЕ ХРАНИЛИЩА, ПОЧТА, АРМ

УПРАВЛЕНИЕ ДОСТУПОМ
ИЗМЕНЕНИЕ ДОСТУПА К ФАЙЛАМ В ИНТЕРФЕЙСЕ СИСТЕМЫ. МОДЕЛИРОВАНИЕ ИЗМЕНЕНИЙ В ПЕСОЧНИЦЕ

UEBA
КОНТРОЛЬ ВСЕХ СУЩНОСТЕЙ СИСТЕМЫ И ИХ ВЗАИМОДЕЙСТВИЯ. ВЫЯВЛЕНИЕ АНОМАЛИЙ, ШИФРОВАЛЬЩИКОВ И DDoS

ПОИСК И КАТЕГОРИЗАЦИЯ
ФЗ-152, GDPR, PCI DSS, ГОСТ Р 57580.1-2017, СТО БР ИББС, ФСТЭК...

АУДИТ ACTIVE DIRECTORY
+ LDAP, APACHE DIRECTORY, RED HAT DIRECTORY SERVER

АКТИВНАЯ РЕАКЦИЯ НА ИНЦИДЕНТ
БЛОКИРОВКА / СМЕНА ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ

КОНТРОЛЬ ДЕЙСТВИЙ
С ФАЙЛАМИ: МОДИФИКАЦИЯ, КОПИРОВАНИЕ, УДАЛЕНИЕ

АНАЛИЗ ДЕЙСТВИЙ
С УЧЕТНЫМИ ЗАПИСЯМИ И ГРУППАМИ ACTIVE DIRECTORY: ВКЛЮЧЕНИЕ / ОТКЛЮЧЕНИЕ, ИЗМЕНЕНИЕ ПРАВ

НАСТРАИВАЕМЫЕ ОТЧЕТЫ И ОПОВЕЩЕНИЯ
В КОНСОЛИ, НА E-MAIL, В МЕССЕНДЖЕРЫ

ОПРЕДЕЛЯЕТ ЭФФЕКТИВНЫХ ВЛАДЕЛЬЦЕВ ФАЙЛОВ
АКТИВНЫЕ ПОЛЬЗОВАТЕЛИ

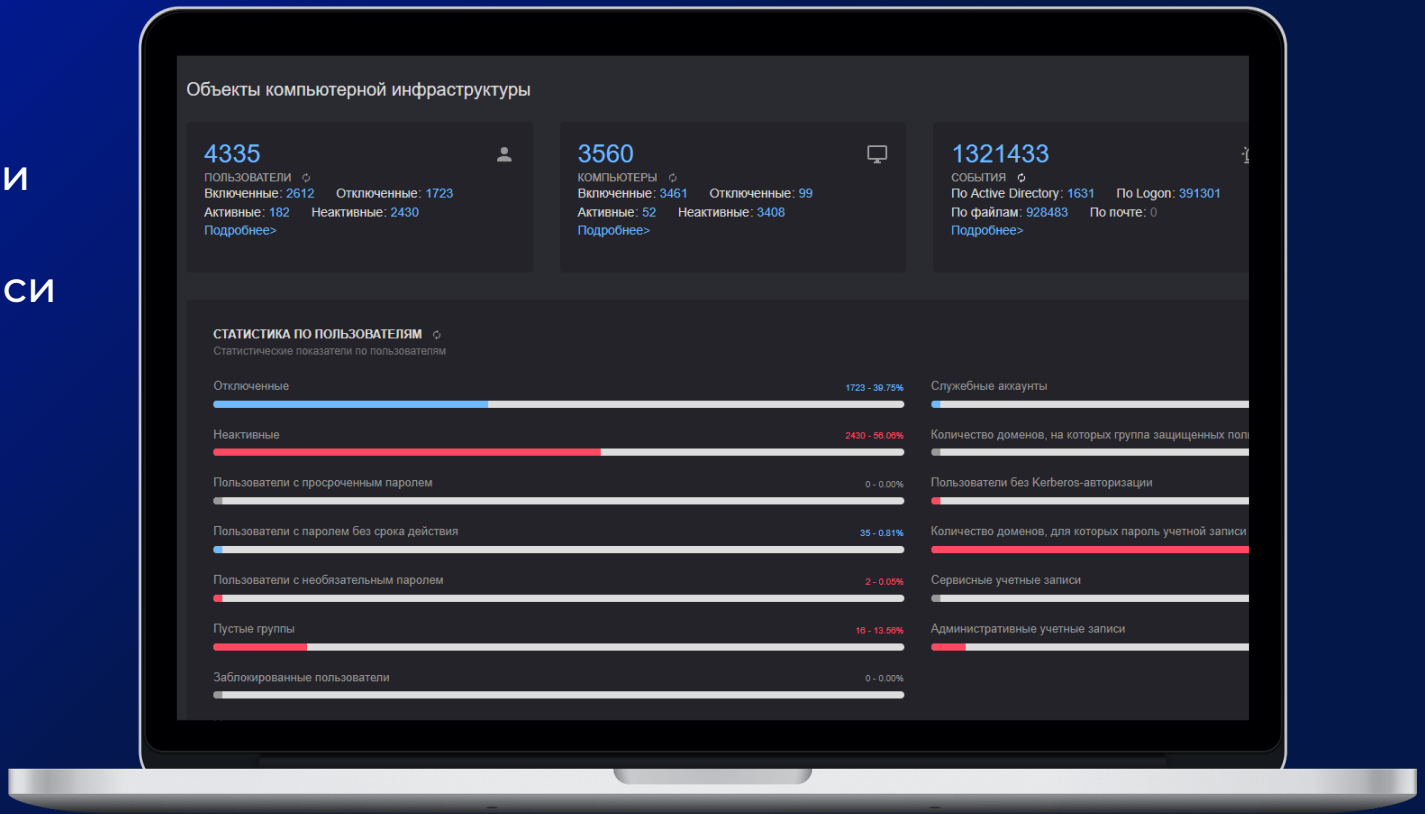
АНАЛИЗ СОБЫТИЙ
ВХОД, ВЫХОД, НЕВЕРНЫЙ ПАРОЛЬ И Т.Д.

ОПТИМИЗАЦИЯ ХРАНИЛИЩ
ВЫЯВЛЯЕТ НЕДЕЛОВЫЕ ФАЙЛЫ И ДУБЛИКАТЫ


MAKVES
ТЕПЕРЬ ЧАСТЬ ГАРДА
DCAP
ПРАКТИКА ПРИМЕНЕНИЯ

Атака на Active Directory

- Конфигурации домена
- Учетные записи

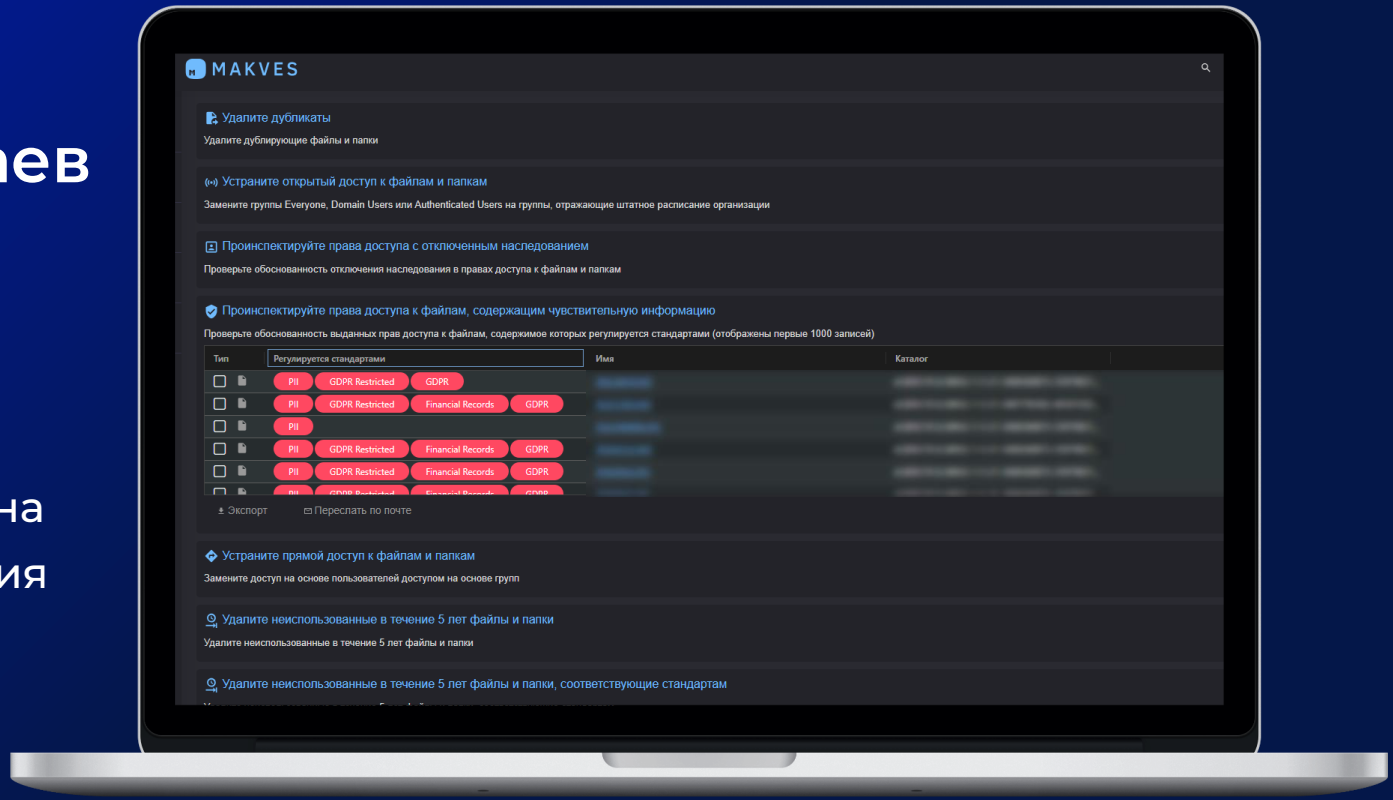


Конфиденциальная информация в общем доступе

MAKVES ТЕПЕРЬ ЧАСТЬ ГАРДА

Нарушения в 100% случаев

- Персональные данные
- Коммерческая тайна
- Банковская тайна
- Мед. информация



MAKVES теперь часть ГАРДА

Защита данных от киберугроз

1 Проверяйте, что хранится в сетевых папках и на ПК

2 Классифицируйте данные (152-ФЗ, ФСТЭК, GDPR, коммерческая тайна...)

3 Изучайте действия пользователей с ценными файлами и права доступа

MAKVES
ТЕПЕРЬ ЧАСТЬ ГАРДА

ПОЛУЧИТЕ БЕСПЛАТНЫЙ ОТЧЕТ О РИСКАХ В ИТ:

- БРОШЕННЫЕ УЧЕТНЫЕ ЗАПИСИ
- ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ОБЩЕМ ДОСТУПЕ
- ПОЛЬЗОВАТЕЛИ БЕЗ ПАРОЛЯ / ПАРОЛИ БЕЗ СРОКА ДЕЙСТВИЯ
- НЕЗАЩИЩЕННЫЕ КОПИИ ВАЖНЫХ ДОКУМЕНТОВ
- НЕНАСЛЕДУЕМЫЕ/ ПРЯМЫЕ ПРАВА
- ДОСТУП К ЧУЖОЙ ПОЧТЕ