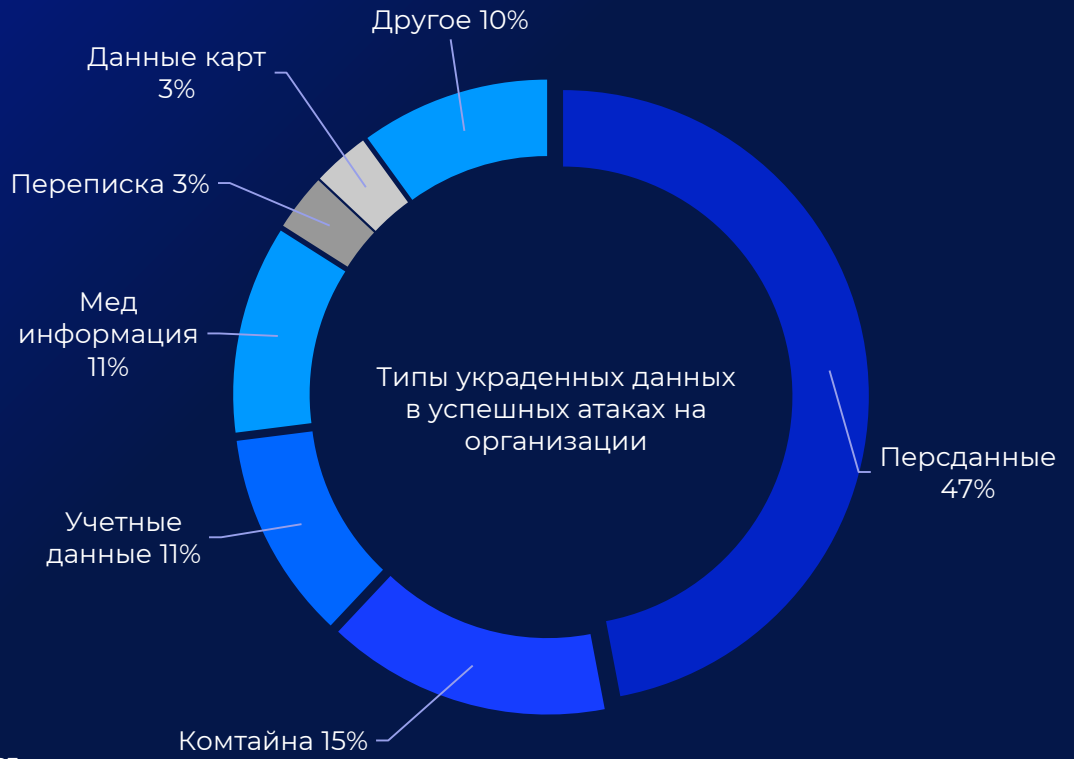
ПОСЛЕДСТВИЯ АТАК

Утечка конфиденциальной информации – 56%

Нарушение деятельности - 36%



Q3, 2023

Источник: Positive Technologies. Актуальные киберугрозы Q3 2023

ПРИЧИНЫ

Утечки данных фиксируются по факту пересечения периметра

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

Отсутствует контроль работы с конфиденциальной информацией

ДАННЫЕ СТАНОВЯТСЯ УЯЗВИМЫМИ ДЛЯ КИБЕРАТАК И МОШЕННИЧЕСКИЙ ДЕЙСТВИЙ

РАСТЕТ НАГРУЗКА НА ИТ, СНИЖАЕТСЯ ПРОИЗВОДИТЕЛЬНОСТЬ

DCAP - ПОДХОД К ЗАЩИТЕ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

ИТ-ИНФРАСТРУКТУРА И ИСТОЧНИКИ ДАННЫХ

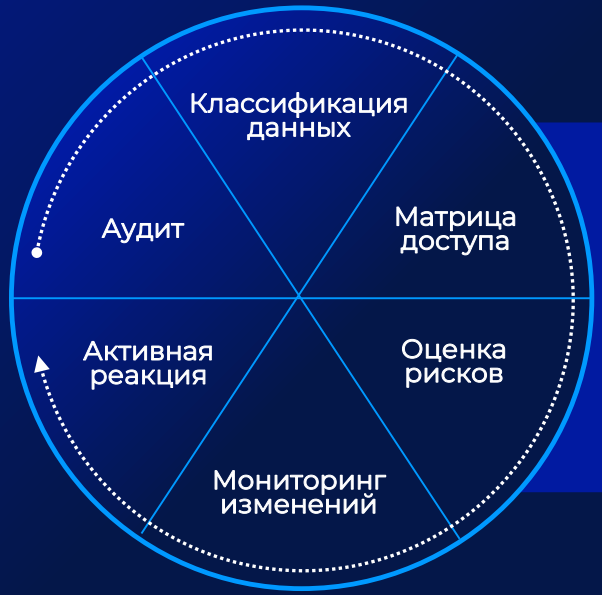
Доменные службы

Серверы, СХД

Рабочие станции

Почтовые серверы

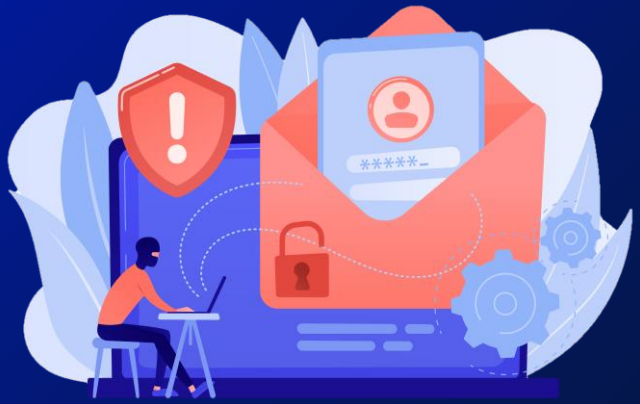
Облачные хранилища



- ✓ СОКРАЩЕНИЕ ПОВЕРХНОСТИ АТАКИ
- ✓ КОМПЛАЕНС
- ✓ ЗАЩИТА ИНФОРМАЦИИ

MAKVES
ТЕПЕРЬ ЧАСТЬ ГАРДА

Техническая атака на учетную запись пользователя



DCAP

Аудит

- «ЗАБЫТЫЕ» УЧЕТНЫЕ ЗАПИСИ
- ПРОСРОЧЕННЫЕ ПАРОЛИ
- СЕРВИСНЫЕ УЧЕТНЫЕ ЗАПИСИ
- РЕАЛЬНЫЕ ПРАВА ДОСТУПА

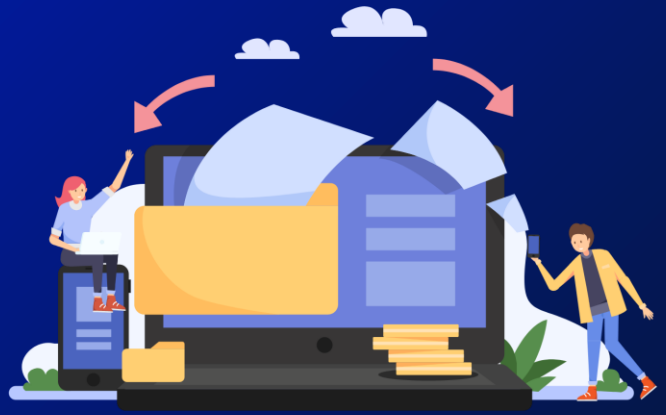
Мониторинг

- ПОПЫТКИ ПОДКЛЮЧЕНИЯ
- АНОМАЛЬНАЯ АКТИВНОСТЬ:

СОБЫТИЯ, ФАЙЛЫ, ПОЛЬЗОВАТЕЛИ, ПК

MAKVES теперь часть ГАРДА

Конфиденциальная информация в общем доступе



DCAP

- ГДЕ ХРАНИТСЯ ИНФОРМАЦИЯ И ЕЕ КОПИИ
- В КАКОМ КОЛИЧЕСТВЕ
- КТО ИМЕЕТ К НЕЙ ДОСТУП
- КТО АКТИВНЫЙ ПОЛЬЗОВАТЕЛЬ

Нарушения в 100% случаев

MAKVES теперь часть ГАРДА

Как защитить данные от атак?

1. Контроль файловых хранилищ
2. Контроль учетных записей
3. Регулярный аудит