Деметра Холдинг

DLP или DCAP?

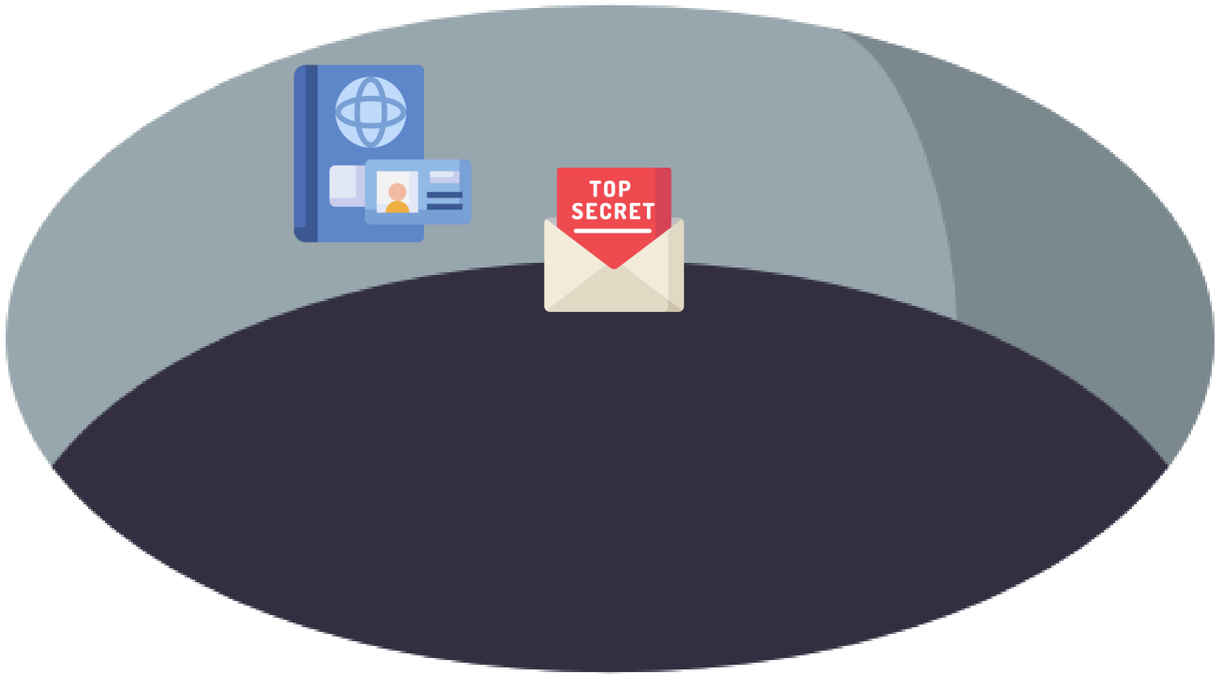
Практика применения решений в контексте различных векторов атак

Искандар Косимов,
Начальник управления информационной безопасности
ООО «УК Деметра-Холдинг»

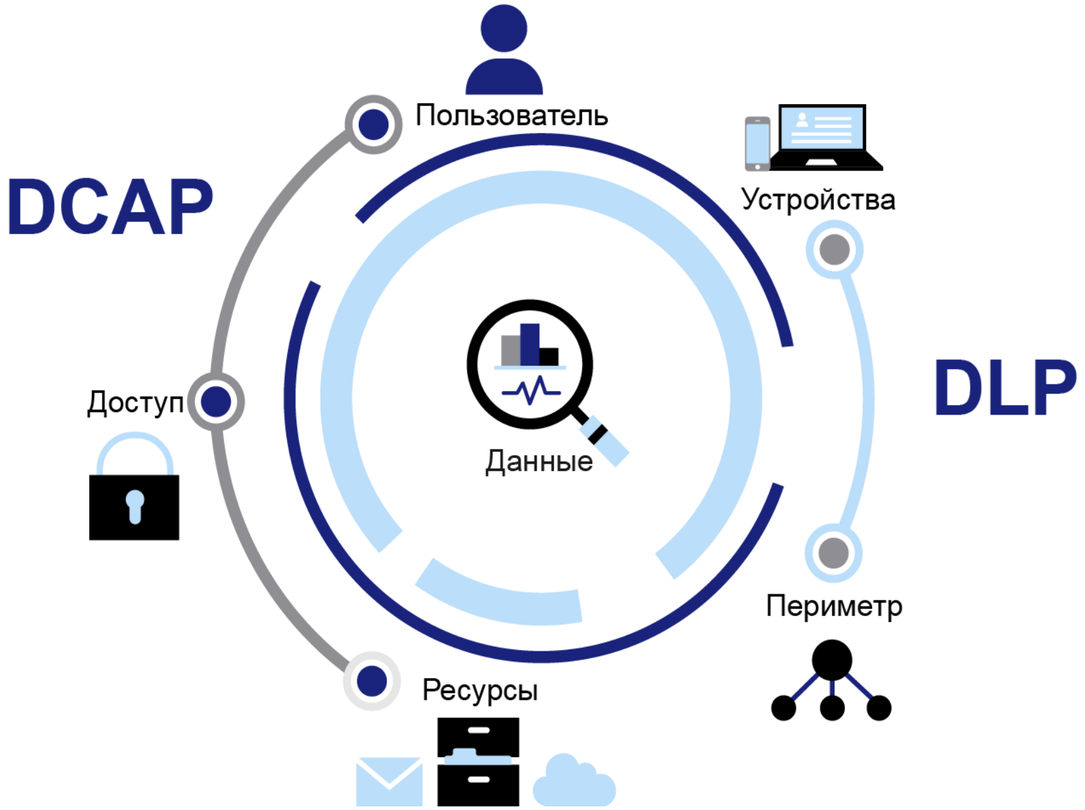
IT

инфраструктура

Data Breach



DCAP или DLP?


Пользователь
Устройства
DCAP
DLP
Доступ
Данные
Периметр
Ресурсы

ПРАКТИКА ПРИМЕНЕНИЯ

Техническая атака на учетную запись пользователя

DCAP

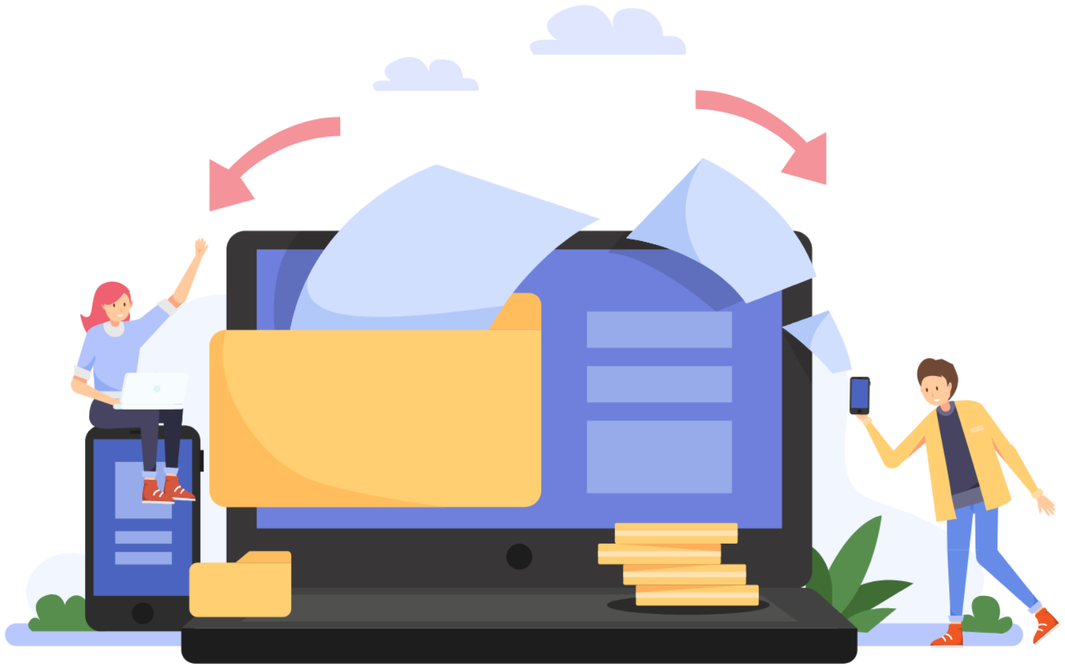
Аудит

- «Забытые» учетные записи
- Просроченные пароли
- Сервисные учетные записи
- Реальные права доступа

Мониторинг

- Попытки подключения
- Аномальная активность:
- **События, файлы, пользователи, ПК**

Доверенный инсайдер



DLP

- Контроль информационных потоков
- Анализ
  (на кого обратить внимание)
- Фиксация действий
  с конфиденциальной информацией
  в момент нарушения

DCAP

- Где хранится информация и ее копии
- В каком количестве
- Кто имеет к ней доступ
- Кто активный пользователь

DCAP+DLP

1 **Аудит и классификация**

2 **Контроль доступа**

3 **Защита от внутренних и внешних угроз**

Деметра Холдинг

Контакты:

+7 (926) 420-31-42

iskandar.kosimov@dholding.ru