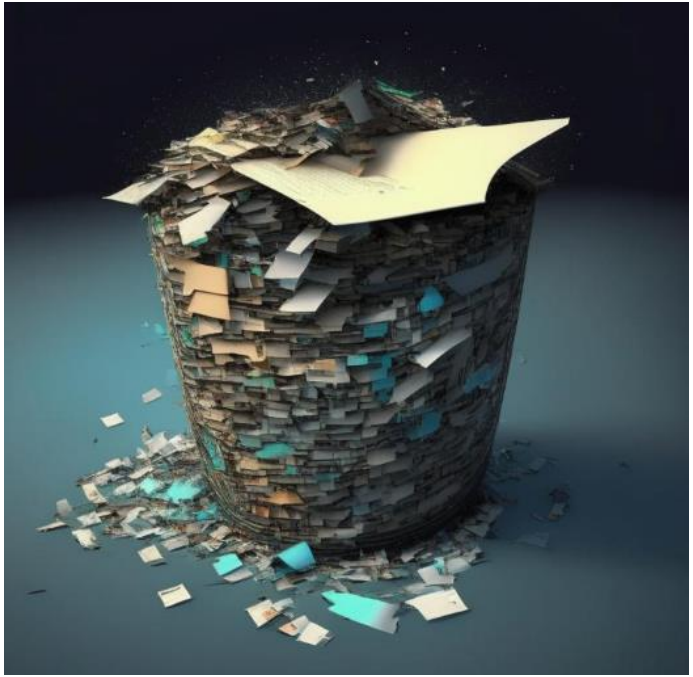
АО «ДИАЛОГНАУКА»
DCAP
ПОДХОД К ЗАЩИТЕ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ

Кузнецов Николай, руководитель направления ОТР, АО «ДиалогНаука»

2023

Неструктурированные данные

- До 80% корпоративных данных являются неструктурированными и хранятся на файловых ресурсах;
- До 60% таких данных – бесполезны: копии, неиспользуемые данные, медиафайлы;
- До 40% составляет ежегодный прирост объема неструктурированных данных;
- Отсутствие решений аудита прав доступа к таким данным



О DCAP

- Data-Centric Audit and Protection (DCAP) – подход к управлению безопасностью данных
- DCAP фокусируется на неструктурированном контенте и его содержимом

- Основной функционал DCAP:
  - обнаружение и классификация данных, хранящихся на общедоступных ресурсах;
  - аудит и управление доступом к таким данным;
  - аналитика поведения пользователей;
  - мониторинг и аудит изменений данных и разрешений.

Возможности DCAP

Аудит доступа к данным файловых хранилищ

Классификация и поиск чувствительных данных, в том числе, по требованиям регуляторов РФ, GDPR

UEBA
Построение профилей сотрудников/хранилищ, выявление аномалий

Аудит всех прав доступа к данным

Детектирование изображений паспортов, ВУ, СНИЛС, кредитных карт на основе нейронных сетей

Активная реакция на инцидент/аномалию. Остановит вирус шифровальщик блокировкой пользователя/хранилища

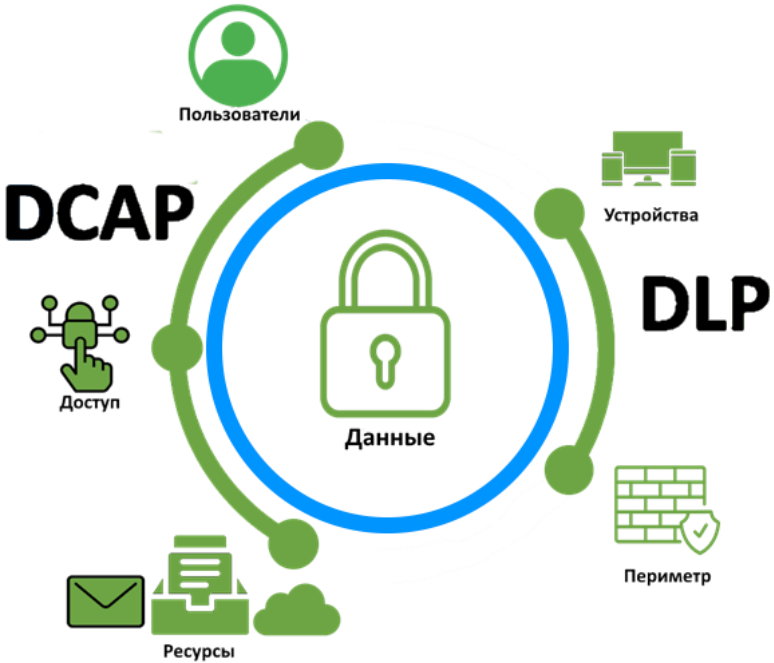
Аудит Active Directory и обнаружение связанных с этим аномалий и инцидентов

Мгновенный поиск информации хранящейся на файловых серверах

Автоматическое выявление рисков связанных с выдачей прав и аномальной активностью

Почему DPL недостаточно?

- DLP предназначена для контроля за перемещением файлов на конечных узлах
- DLP не обеспечивает классификацию документов на файловых ресурсах, порталах MS SharePoint, почтовых серверах, базах знаний организаций (к примеру, Confluence)
- DLP не обладает возможностью выстраивания прав доступа сотрудников к документам, расположенным на общедоступных ресурсах компаний
- Отсутствие контроля за операциями по отношению к учетным записям, группам безопасности, и любым другим объектам, расположенным в AD
- DLP не позволяет выявлять аномальную активность пользователей на файловых ресурсах



А может SIEM + штатный аудит?

Невозможность проведения аудита в режиме, близком к реальному времени

Нельзя классифицировать данные

Отсутствие активной реакции на инциденты

Отсутствие возможности по двунаправленному отображению прав доступа

Отсутствие возможности по распознаванию графических документов

Отсутствие возможности глобальной индексации данных

Трудоемкость настройки поведенческой аналитики

СПАСИБО ЗА ВНИМАНИЕ!

ПО ВСЕМ ВОПРОСАМ ОБРАЩАЙТЕСЬ НА EMAIL:

marketing@dialognauka.ru