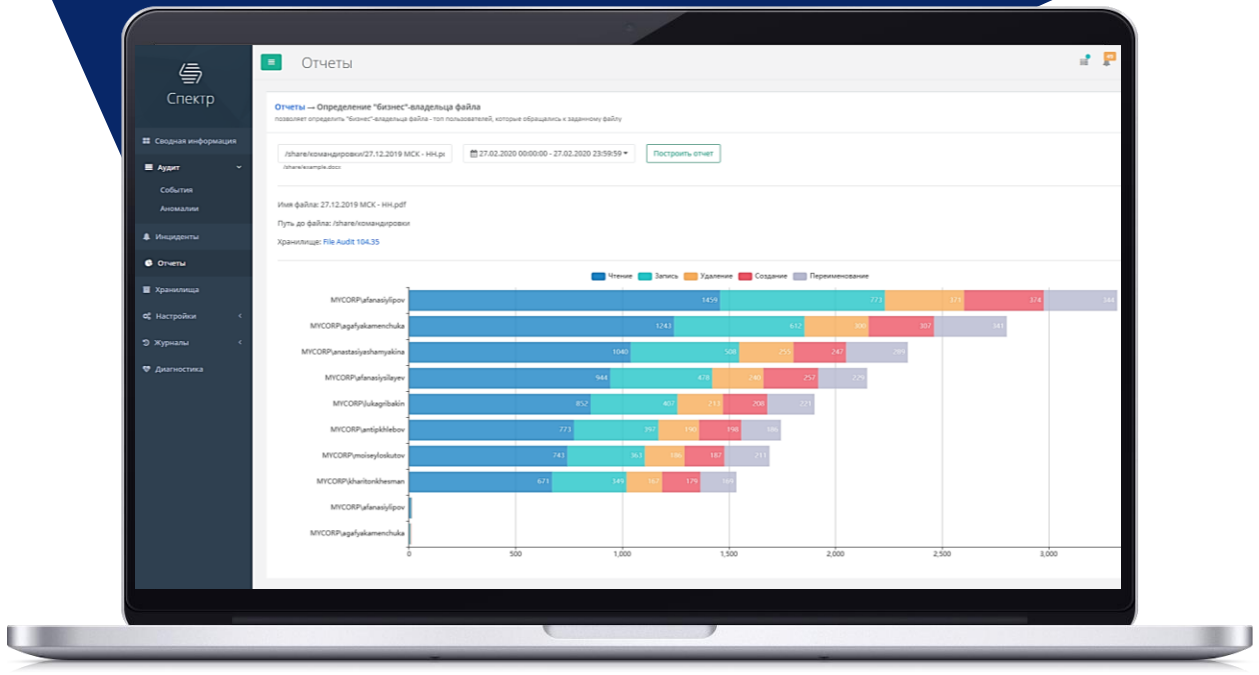
РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

CyberPeak

АУДИТ И УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА
К НЕСТРУКТУРИРОВАННЫМ ДАННЫМ

СПЕКТР

ЧТО ТАКОЕ «СПЕКТР»?



Система «СПЕКТР» — решение класса DAG (Data Access Governance) — полный контроль доступа сотрудников компании к файлам, находящимся на хранилищах неструктурированных данных (файловые сервера MS Windows, Linux, почтовые сервера, сервера MS SharePoint и др.).

Система позволяет осуществлять полную классификацию всех документов, помогая определить, где расположены наиболее ценные информационные активы, и управлять правами доступа к этим данным.

Технологии машинного обучения позволяют выявлять нетипичные активности сотрудников по отношению к данным, решая такие задачи как массовое удаление данных, аномальное изменение привилегий доступа, определение бизнес владельцев документов и другие.

Система «СПЕКТР» является полностью отечественной разработкой, не требующей лицензии на сторонние коммерческие продукты.

НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ – НАИБОЛЕЕ ДИНАМИЧНО РАСТУЩИЙ ОБЪЕМ ИНФОРМАЦИИ В КОМПАНИЯХ С ПРИРОСТОМ ~30% В ГОД

«СПЕКТР» РЕШАЕТ СЛЕДУЮЩИЕ ЗАДАЧИ

Защита от утечек информации хранящейся на файловых серверах

Аудит доступа к данным файловых хранилищ

Классификация и поиск чувствительных данных

Аудит всех прав доступа к данным

ЗАЧЕМ КОНТРОЛИРОВАТЬ ДОСТУП К НЕСТРУКТУРИРОВАННЫМ ДАННЫМ?

ВАЖНО ИМЕТЬ ОТВЕТЫ НА СЛЕДУЮЩИЕ ВОПРОСЫ

- У кого есть доступ к данным?
- Кто должен иметь доступ к данным?
- Где хранятся данные?
- Какие данные наиболее критичны?
- Кто, когда, к каким данным имел доступ?
- Какие данные не используются?
- Есть ли избыточные права доступа к данным?
- Кто является ответственным за тот или иной файл - каталог?

АРХИТЕКТУРА СИСТЕМЫ

ЦЕНТР УПРАВЛЕНИЯ СИСТЕМЫ «СПЕКТР»

СПЕКТР

Аудит доступа выполняется с помощью агентов

Классификация, получение структуры хранилищ и прав доступа происходит удаленно

КОЛЛЕКТОРЫ/ АГРЕГАТОРЫ

КОЛЛЕКТОРЫ/ АГРЕГАТОРЫ

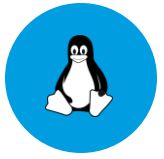
АГЕНТЫ «СПЕКТР»

Файловые хранилища MS Windows

MS Exchange

Серверы Sharepoint

Active Directory



Файловые хранилища Unix/Linux

ПРИНЦИП РАБОТЫ СИСТЕМЫ «СПЕКТР»

1

ПОЛУЧЕНИЕ СТРУКТУРЫ ХРАНИЛИЩ

«СПЕКТР» синхронизируется с защищаемыми хранилищами и получает полную структуру каталогов-файлов.

2

СИНХРОНИЗАЦИЯ С AD

Для получения всех пользователей, групп и прав доступа.

3

КЛАССИФИКАЦИЯ ДАННЫХ

Сканирование файловых серверов на предустановленные и настраиваемые пользователем категории данных. Выявление новых мест хранения и контроль обезличенности информации.

4

АУДИТ ДОСТУПА К ДАННЫМ

С использованием механизмов штатного аудита и/или агентского ПО. Ведется полный архив событий.

5

АНАЛИТИКА/ОТЧЕТЫ

Просмотр любых статистических срезов доступа к информации. Аналитика с выявлением отклонений от типичного поведения. Наглядные отчеты в различных форматах.

6

СИСТЕМА ОПОВЕЩЕНИЯ

В комплексе предусмотрены уведомления о событиях по e-mail, передача данных во внешние SIEM-системы.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ: ПРОСМОТР ПРАВ ПОЛЬЗОВАТЕЛЕЙ

ВОЗМОЖНОСТЬ ДВУНАПРАВЛЕННОГО ПРОСМОТРА ТЕКУЩИХ ПРАВ ДОСТУПА

У кого есть доступ к конкретным файлам – каталогам

К каким файлам-каталогам, какие права доступа есть у конкретного пользователя/группы

К каким данным есть доступ у общих групп (Everyone, и т.д.)

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ: АУДИТ ДОСТУПА К ДАННЫМ

АУДИТ ВСЕХ ОПЕРАЦИЙ С ДАННЫМИ ФАЙЛОВЫХ СЕРВЕРОВ, ОБЩИХ ПАПОК EXCHANGE, И.Т.Д.

Аудит ведется в режиме реального времени

Возможно получать данные как с использованием агентского ПО, так и без него

Сохранение всех результатов аудита для ретроспективного анализа

Гибкие возможности фильтрации, сортировки, настройки представления

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ: СТАТИСТИЧЕСКИЙ АНАЛИЗ АКТИВНОСТИ

ПРОСМОТР АНАЛИТИЧЕСКИХ СРЕЗОВ АКТИВНОСТИ ПО ДОСТУПУ К ДАННЫМ

Выявление наиболее и наименее используемых файлов

Просмотр самых активных пользователей в части чтения, записи, удаления и других операций с данными

Выявление «владельцев» данных на основе статистики обращений

Просмотр возможен по любому пользователю, группе, файлу или файловому серверу

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ: КЛАССИФИКАЦИЯ ДАННЫХ

ОПРЕДЕЛЕНИЕ МЕСТОНАХОЖДЕНИЯ КРИТИЧНОЙ ИНФОРМАЦИИ, ПОИСК ПО ШАБЛОНАМ, ПОМОЩЬ В СООТВЕТСТВИИ PCI DSS, GDPR, 152 ФЗ И ДР.

Позволяет сканировать данные файловых серверов*

Предустановленные категории позволяют находить файлы с ПДН, финансовой информацией, карточными данными и другими категориями

Проверка файлов происходит в ночное время на сервере «СПЕКТР» и не нагружает защищаемые системы

* Опционально доступно сохранение содержимого сканируемых файлов для последующих поисков

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ: ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА

ВСТРОЕННЫЕ СРЕДСТВА АНАЛИТИКИ ПОЗВОЛЯЮТ ВЫЯВЛЯТЬ ОТКЛОНЕНИЯ ОТ ОБЫЧНЫХ СЦЕНАРИЕВ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ С ДАННЫМИ ФАЙЛОВЫХ ХРАНИЛИЩ

Построение профилей поведения по каждому сотруднику/учетной записи для каждого файлового хранилища

Выявление статистических аномалий и отклонений, включая:

- доступ к ранее неиспользуемым данным
- аномальное число обращений к файлам
- массовые выгрузки – удаление файлов
- выявление неиспользуемых, и наоборот самых используемых файлов

Работает по принципу машинного обучения и не требует ручной настройки профилей пользователей

ТЕХНИЧЕСКИЕ ВОЗМОЖНОСТИ

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ

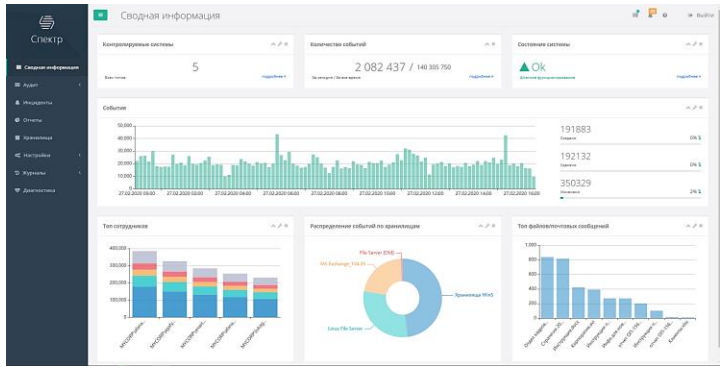
- Файловые сервера MS Windows
- Файловые сервера Linux
- MS Exchange
- NetApp
- MS Sharepoint
- и другие

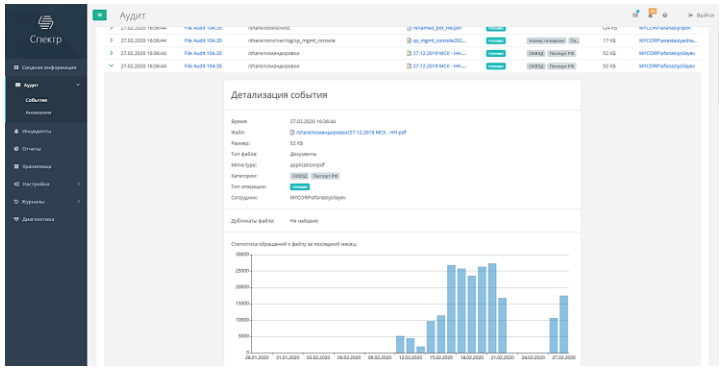
ПРОИЗВОДИТЕЛЬНОСТЬ

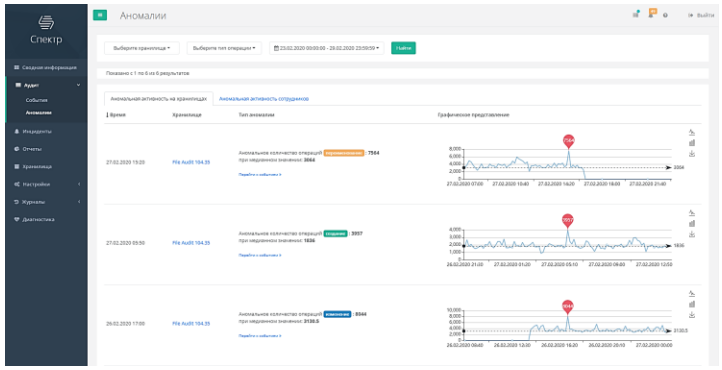
- Обработка событий аудита до 10 000 в секунду на один сервер
- Хранение данных (классификация, аудит)
- До 40 ТВ на один сервер
- Ретроспективный поиск по всем результатам аудита за секунды

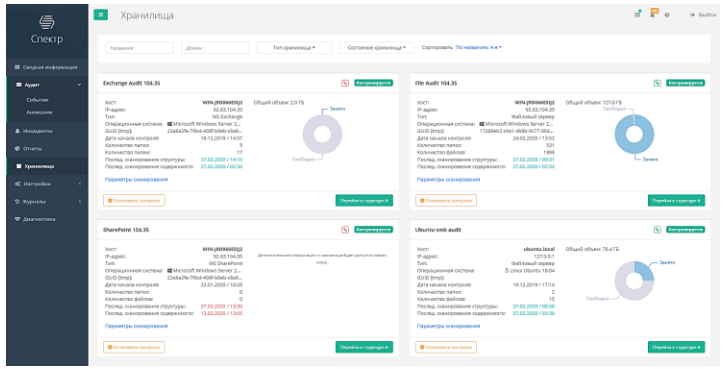
МАСШТАБИРУЕМОСТЬ

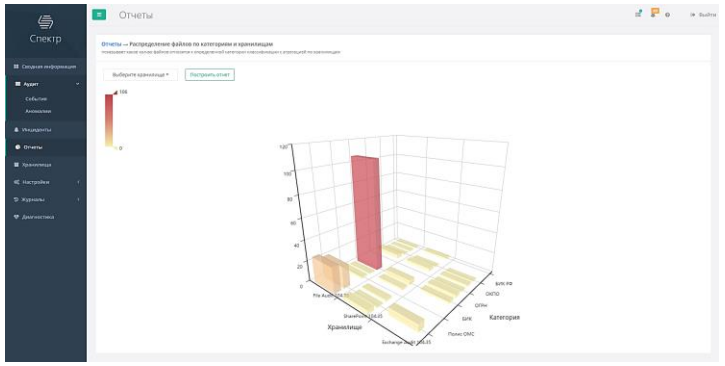
- Возможность построения георасределенной системы с единым интерфейсом управления
- Горизонтальное масштабирование системы для:
  - увеличения производительности
  - повышения отказоустойчивости


Спектр
Сводная информация
Контролируемые системы
5
Количество событий
2 082 437 / 140 305 750
Состояние системы
Ok
События
191883
192132
350329
Топ сотрудников
Распределение событий по хранилищам
Топ файлов/почтовых сообщений


Спектр
Аудит
Детализация события


Спектр
Аномалии


Спектр
Хранилища
Exchange Audit 104.35
File Audit 104.35
SharePoint 104.35
Ubuntu smb audit


Спектр
Отчеты
Хранилища
Категория


Спектр
Отчеты

УЗНАЙТЕ ВСЁ О ВАШИХ ДАННЫХ И ЗАЩИТИТЕ ИХ

КОНТАКТЫ

СПЕКТР

Москва,
ул. Донской 5-й проезд,
д. 21 Б, помещение 1

Нижний Новгород,
ул. Академика Сахарова,
д. 115 корп. 2, помещение 1

+7 (495) 135 05 35

info@cyberpeak.ru

https://cyberpeak.ru