РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

с помощью ПО класса

MKO SYSTEMS

ДАНИЭЛЬ КЛЮЕВ

ЭКСПЕРТ В ОБЛАСТИ ИЗВЛЕЧЕНИЯ
И АНАЛИЗА ДАННЫХ
ИЗ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

DLP

SIEM

SOAR

DFIR

и другие

ПРОГРАММНОЕ
ОБЕСПЕЧЕНИЕ КЛАССА

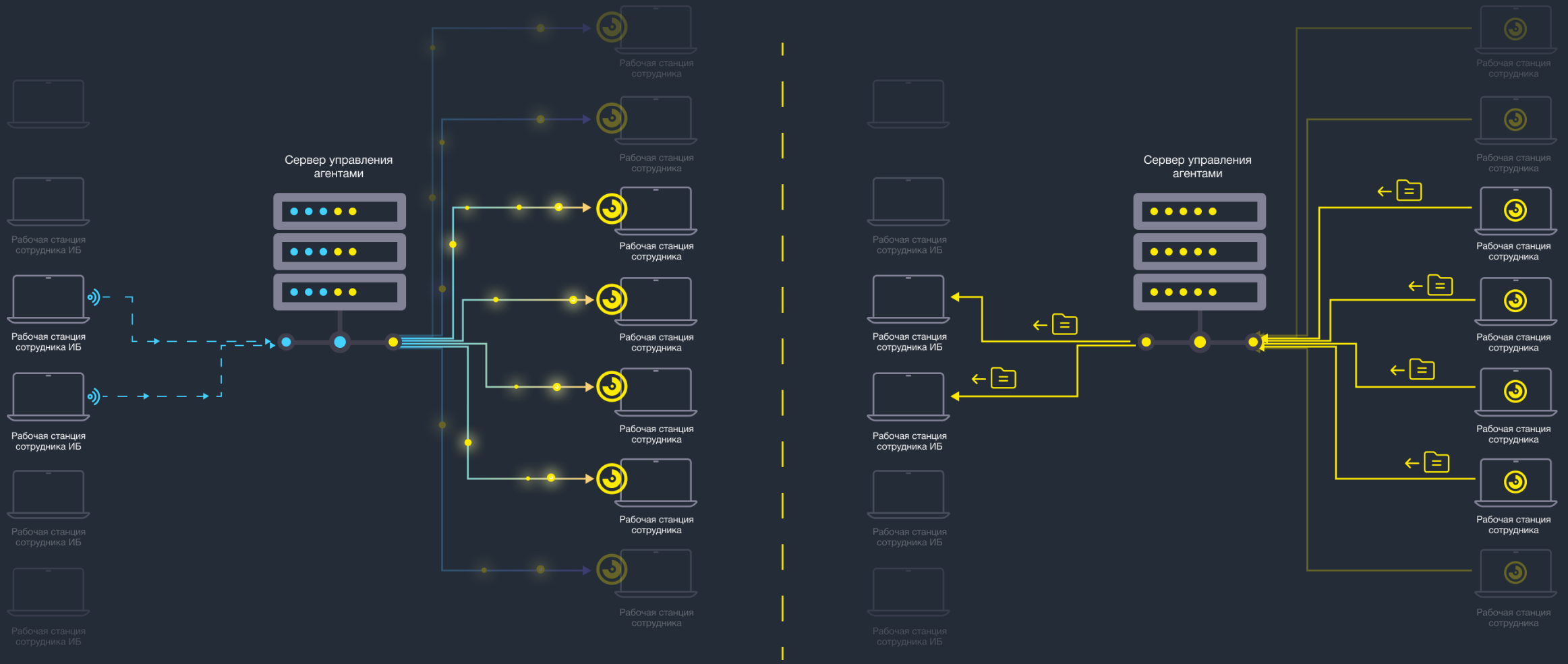
MK ENTERPRISE

- Дистанционное исследование рабочих станций на Windows, macOS, GNU/Linux
- Исследование группы рабочих станций на Windows
- Извлечение данных из устройств на базе Android и iOS
- Получение доступа к информации в облачных хранилищах
- Анализ коммуникаций владельца устройства или учетной записи
- Построение полной хронологии инцидента
- Изучение полной файловой базы объекта исследования
- Поиск данных внутри извлечения по заданным параметрам

ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ РАБОЧИХ СТАНЦИЙ

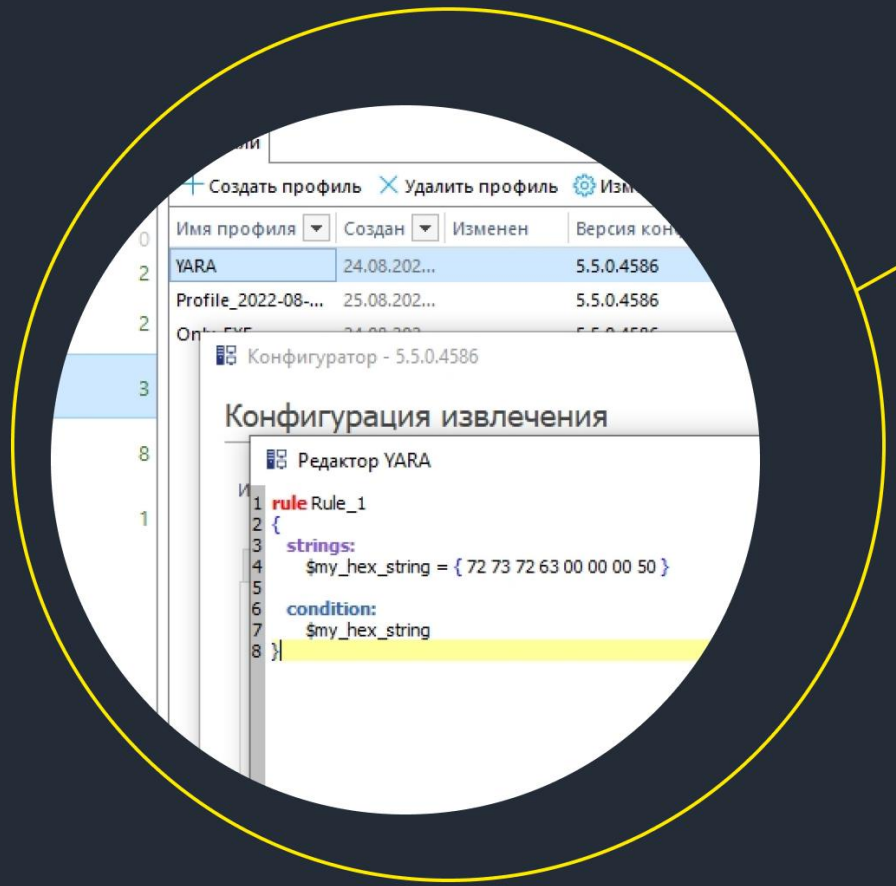
АГЕНТСКИЙ РЕЖИМ

- АГЕНТ



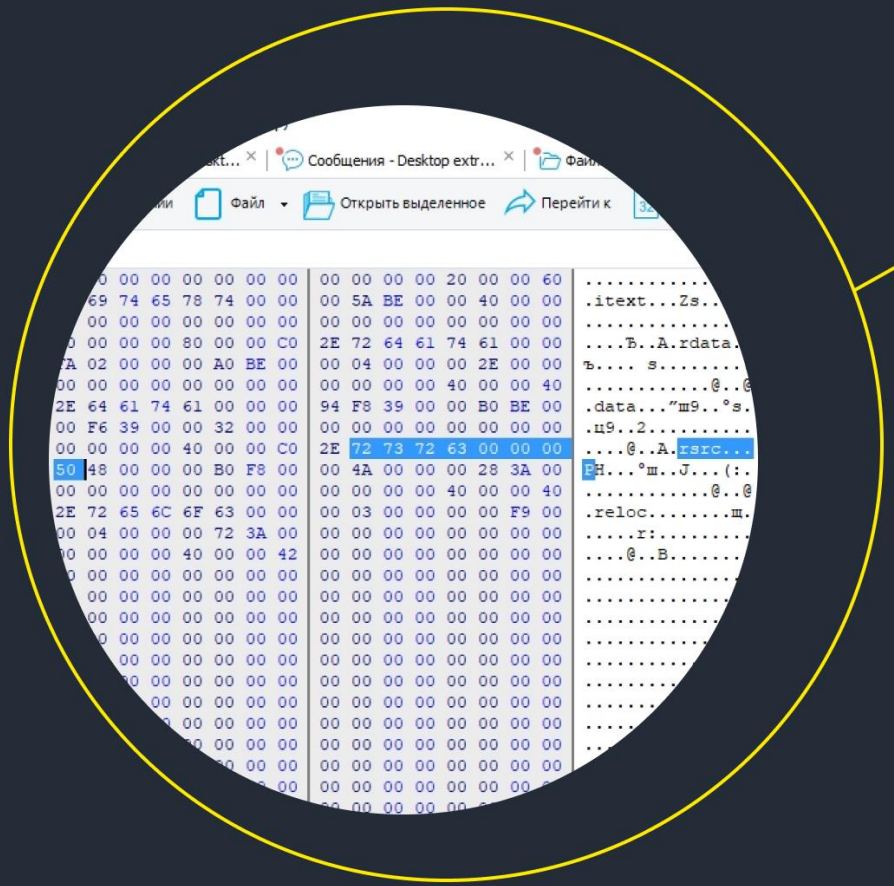
ПОИСК ПО СОДЕРЖИМОМУ

ПРАВИЛА YARA



ПОИСК ПО СОДЕРЖИМОМУ

ПРАВИЛА YARA



DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ЗАДАЧИ

- Проведение аудита
- Инициация расследования
- Предотвращение ущерба до его возникновения
- Оптимизация процесса реагирования на подобные инциденты

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ТИПЫ КЕЙСОВ

RANSOMWARE

MALWARE

ФИШИНГ

ИНСАЙДЕРСТВО

НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ АКТИВОВ

НАРУШЕНИЕ ВНУТРЕННЕЙ ПОЛИТИКИ

МОШЕННИЧЕСТВО

ПРОГРАММЫ-ВЫМОГАТЕЛИ

УВОЛЬНЕНИЕ СОТРУДНИКА

ЗАПРЕЩЕННЫЕ ПРИЛОЖЕНИЯ

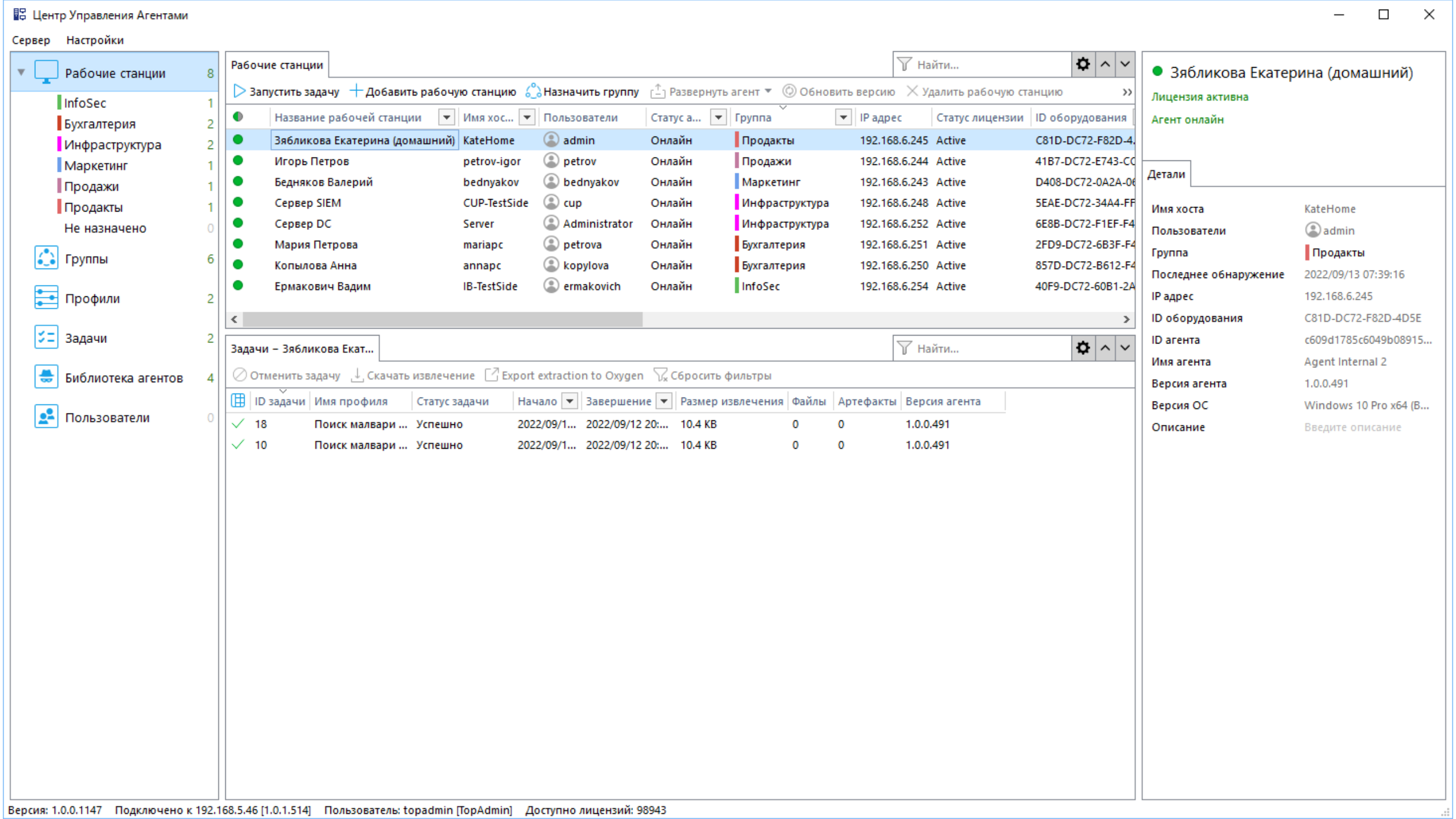
ХАРАССМЕНТ

и другое

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

MALWARE

- В ходе проведения аудита было выявлено вредоносное ПО
- Было инициировано расследование
- Выявлена точка входа
- Выявлены затронутые злоумышленником элементы сети и активность на них
- Инцидент предотвращен до возникновения ущерба


Центр Управления Агентами
Сервер
Настройки
Рабочие станции 8
InfoSec 1
Бухгалтерия 2
Инфраструктура 2
Маркетинг 1
Продажи 1
Продакты 1
Не назначено 0
Группы 6
Профили 2
Задачи 2
Библиотека агентов 4
Пользователи 0
Рабочие станции
Найти...
Запустить задачу
Добавить рабочую станцию
Назначить группу
Развернуть агент
Обновить версию
Удалить рабочую станцию
Название рабочей станции
Имя хос...
Пользователи
Статус а...
Группа
IP адрес
Статус лицензии
ID оборудования
Зябликова Екатерина (домашний) KateHome admin Онлайн Продакты 192.168.6.245 Active C81D-DC72-F82D-4...
Игорь Петров petrov-igor petrov Онлайн Продажи 192.168.6.244 Active 41B7-DC72-E743-C...
Бедняков Валерий bednyakov bednyakov Онлайн Маркетинг 192.168.6.243 Active D408-DC72-0A2A-0...
Сервер SIEM CUP-TestSide cup Онлайн Инфраструктура 192.168.6.248 Active 5EAE-DC72-34A4-FF...
Сервер DC Server Administrator Онлайн Инфраструктура 192.168.6.252 Active 6E8B-DC72-F1EF-F4...
Мария Петрова mariapc petrova Онлайн Бухгалтерия 192.168.6.251 Active 2FD9-DC72-6B3F-F4...
Копылова Анна annapc kopylova Онлайн Бухгалтерия 192.168.6.250 Active 857D-DC72-B612-F4...
Ермакович Вадим IB-TestSide ermakovich Онлайн InfoSec 192.168.6.254 Active 40F9-DC72-60B1-2A...
Задачи – Зябликова Екат...
Найти...
Отменить задачу
Скачать извлечение
Export extraction to Oxygen
Сбросить фильтры
ID задачи
Имя профиля
Статус задачи
Начало
Завершение
Размер извлечения
Файлы
Артефакты
Версия агента
18 Поиск малвари ... Успешно 2022/09/1... 2022/09/12 20:... 10.4 KB 0 0 1.0.0.491
10 Поиск малвари ... Успешно 2022/09/1... 2022/09/12 20:... 10.4 KB 0 0 1.0.0.491
Зябликова Екатерина (домашний)
Лицензия активна
Агент онлайн
Детали
Имя хоста KateHome
Пользователи admin
Группа Продакты
Последнее обнаружение 2022/09/13 07:39:16
IP адрес 192.168.6.245
ID оборудования C81D-DC72-F82D-4D5E
ID агента c609d1785c6049b08915...
Имя агента Agent Internal 2
Версия агента 1.0.0.491
Версия ОС Windows 10 Pro x64 (B...
Описание Введите описание
Версия: 1.0.0.1147 Подключено к 192.168.5.46 [1.0.1.514] Пользователь: topadmin [TopAdmin] Доступно лицензий: 98943

Центр Управления Агентами

Сервер Настройки

- Рабочие станции 8
  - IT 1
  - Бухгалтерия 2
  - Дизайн 1
  - Инфраструктура 2
  - Маркетинг 2
  - Продажи 0
  - Не назначено 0
- Группы 6
- Профили 0
- Библиотека агентов 2
- Пользователи 0

Профили

Найти...

Создать профиль | Удалить профиль | Изменить профиль | Сбросить фильтры

Нет данных для отображения

Нет данных

Версия: 1.0.0.898 Подключено к 192.168.5.41 [1.0.1.388] Пользователь: topadmin [TopAdmin] Licenses available: 98951

MK Enterprise (Лицензия Экспертный Центр)

Журнал событий - Deskto... | Важное - Desktop extractio...

Desktop extraction (4.odb)

Часовой пояс (UTC+03:00) Москва (Европа)
ОС Windows 10.0.17763
Номер инцидента Добавить номер инцидента
Номер вещдока Добавить номер вещдока

Статистика | Извлечение | Владелец | Общая информация | Устройство | Фото | Заметка

Общая информация
Платформа Windows 10.0.17763

Общие разделы 5

Приложения | Контакты | Отчёты | Снимки | Файлы 485

Системные артефакты 2

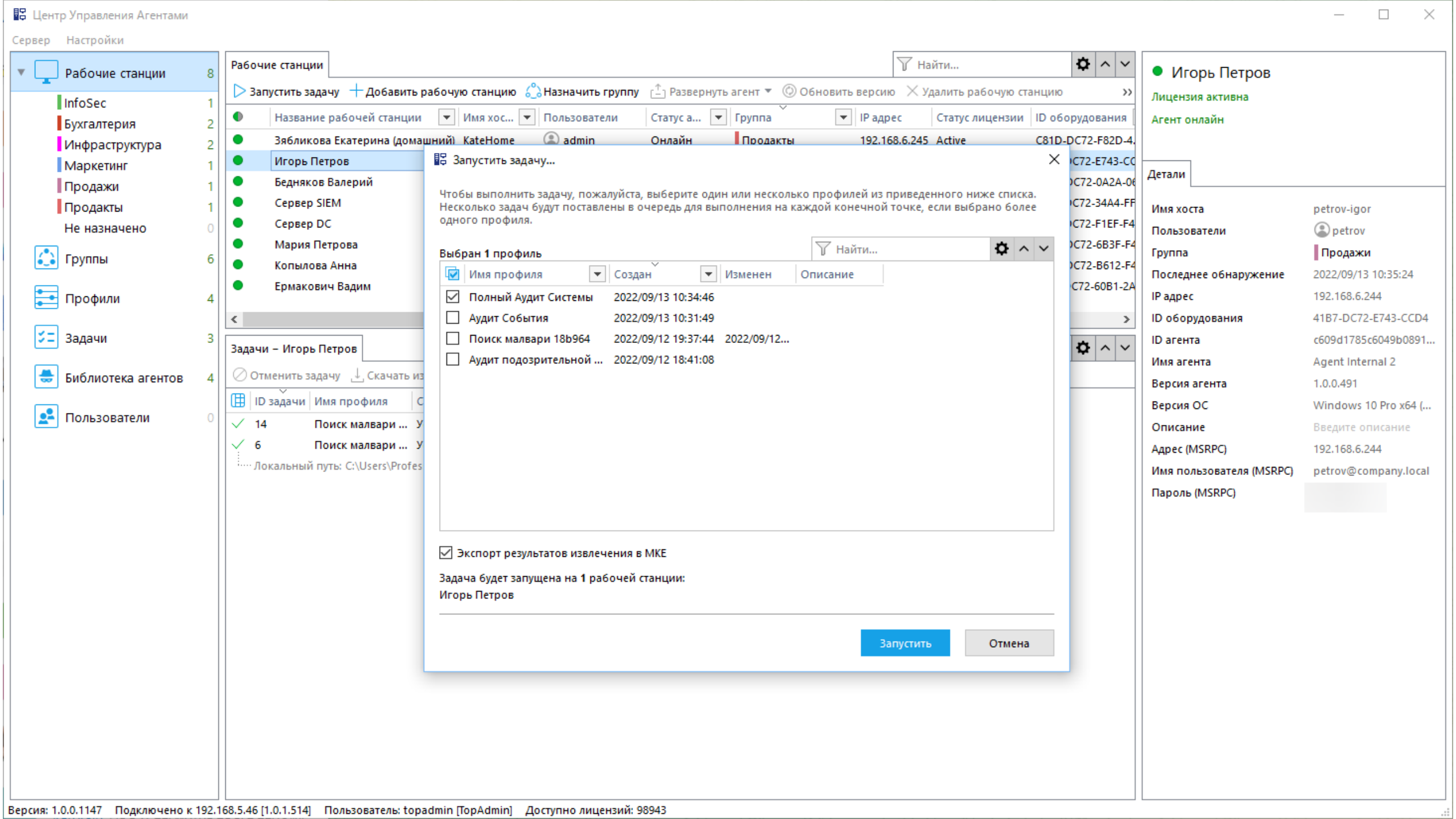
Autorun 140 | Журнал событий 270,425

Аналитика 6

Важное 4 | Граф связей | Лента событий 270,427 | Поиск | Распознавание текста | Статистика

↑ Показать извлечения ↑

Версия: 1.4.0.159 Всего извлечений: 199

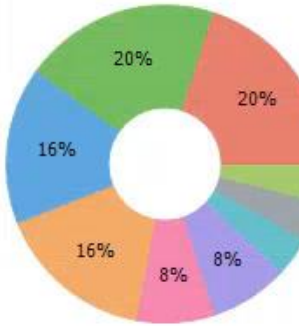

Центр Управления Агентами
Сервер
Настройки
Рабочие станции 8
InfoSec 1
Бухгалтерия 2
Инфраструктура 2
Маркетинг 1
Продажи 1
Продакты 1
Не назначено 0
Группы 6
Профили 4
Задачи 3
Библиотека агентов 4
Пользователи 0
Рабочие станции
Найти...
Запустить задачу
Добавить рабочую станцию
Назначить группу
Развернуть агент
Обновить версию
Удалить рабочую станцию
Название рабочей станции
Имя хос...
Пользователи
Статус а...
Группа
IP адрес
Статус лицензии
ID оборудования
Зябликова Екатерина (домашний)
KateHome
admin
Онлайн
Продакты
192.168.6.245
Active
C81D-DC72-F82D-4...
Игорь Петров
Бедняков Валерий
Сервер SIEM
Сервер DC
Мария Петрова
Копылова Анна
Ермакович Вадим
Задачи – Игорь Петров
Отменить задачу
Скачать из
ID задачи
Имя профиля
14
Поиск малвари ...
6
Поиск малвари ...
Локальный путь: C:\Users\Profes
Запустить задачу...
Чтобы выполнить задачу, пожалуйста, выберите один или несколько профилей из приведенного ниже списка. Несколько задач будут поставлены в очередь для выполнения на каждой конечной точке, если выбрано более одного профиля.
Выбран 1 профиль
Найти...
Имя профиля
Создан
Изменен
Описание
Полный Аудит Системы
2022/09/13 10:34:46
Аудит События
2022/09/13 10:31:49
Поиск малвари 18b964
2022/09/12 19:37:44
2022/09/12...
Аудит подозрительной ...
2022/09/12 18:41:08
Экспорт результатов извлечения в MKE
Задача будет запущена на 1 рабочей станции:
Игорь Петров
Запустить
Отмена
Игорь Петров
Лицензия активна
Агент онлайн
Детали
Имя хоста
petrov-igor
Пользователи
petrov
Группа
Продажи
Последнее обнаружение
2022/09/13 10:35:24
IP адрес
192.168.6.244
ID оборудования
41B7-DC72-E743-CCD4
ID агента
c609d1785c6049b0891...
Имя агента
Agent Internal 2
Версия агента
1.0.0.491
Версия ОС
Windows 10 Pro x64 (...
Описание
Введите описание
Адрес (MSRPC)
192.168.6.244
Имя пользователя (MSRPC)
petrov@company.local
Пароль (MSRPC)
Версия: 1.0.0.1147
Подключено к 192.168.5.46 [1.0.1.514]
Пользователь: topadmin [TopAdmin]
Доступно лицензий: 98943

Полное исследование / Игорь Петров

Часовой пояс (UTC+03:00) Москва (Европа)
ОС Windows 10.0.19044
Номер инцидента Добавить номер инцидента
Номер вещдока Добавить номер вещдока

Статистика | Извлечение | Владелец | Общая информация | Устройство | Фото | Заметка

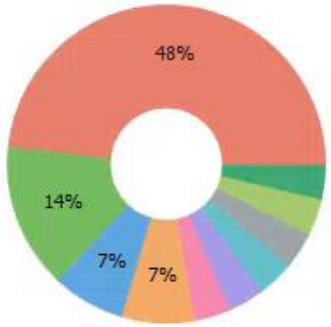
Топ 10 контактов



5 (20.00%) Анна Копылова
5 (20.00%) Мария Петрова
4 (16.00%) Komolin Andrew
4 (16.00%) Ермакович Вадим Викторович
2 (8.00%) Игорь Петров petrov@feel-o...
2 (8.00%) Анна Копылова
1 (4.00%) Магика
1 (4.00%) Andrew Komolin
1 (4.00%) Петрова Мария Львовна

Перейти в Контакты

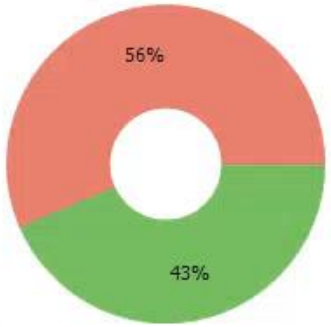
Топ 10 групп



13 (48.15%) Рабочий чат Чувство Стиля
4 (14.81%) petrov@feel-of-style.ru,erm...
2 (7.41%) petrov@feel-of-style.ru,ko...
2 (7.41%) petrov@feel-of-style.ru,ko...
1 (3.70%) petrov@feel-of-style.ru,ko...
1 (3.70%) Игорь Петров petrov@feel-...
1 (3.70%) Игорь Петров petrov@feel-...
1 (3.70%) petrov@feel-of-style.ru,kop...
1 (3.70%) petrov@feel-of-style.ru,kop...
1 (3.70%) petrov@feel-of-style.ru,kop...

Перейти в Контакты

Топ 10 приложений



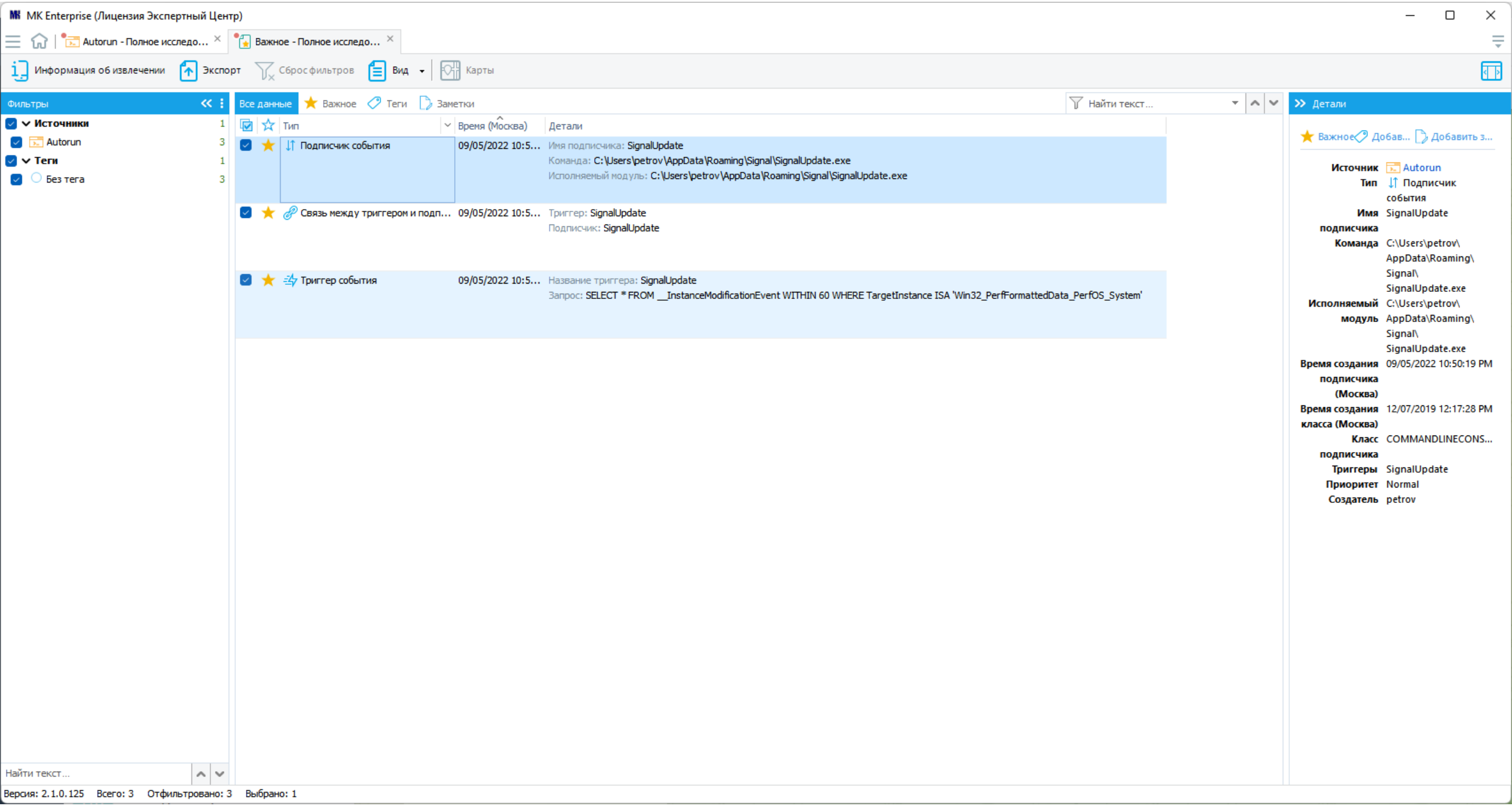
22 (56.41%)
17 (43.59%)

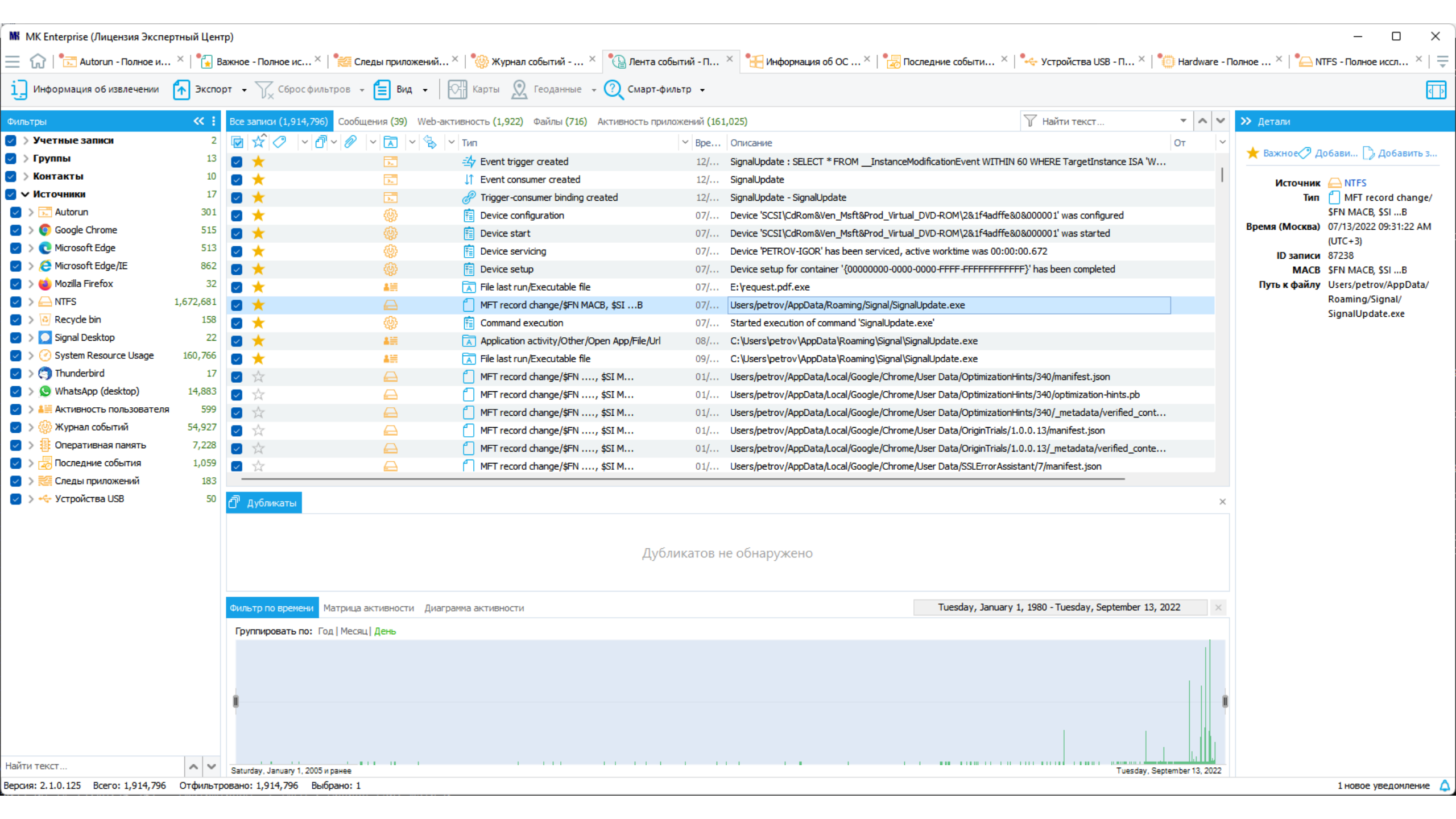
Общие разделы 8

Приложения 10
Аккаунты и пароли 9
Контакты 34
Отчёты
Поисковые запросы 14
Снимки
Сообщения 39
Файлы 48,331

Системные артефакты 13

Partitions
Hardware
Информация об ОС
Autorun
Журнал событий
NTFS


MK Enterprise (Лицензия Экспертный Центр)
Autorun - Полное исследо...
Важное - Полное исследо...
Информация об извлечении
Экспорт
Сброс фильтров
Вид
Карты
Фильтры
Источники 1
Autorun 3
Теги 1
Без тега 3
Все данные
Важное
Теги
Заметки
Найти текст...
Тип
Время (Москва)
Детали
Подписчик события
09/05/2022 10:5...
Имя подписчика: SignalUpdate
Команда: C:\Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe
Исполняемый модуль: C:\Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe
Связь между триггером и подп...
09/05/2022 10:5...
Триггер: SignalUpdate
Подписчик: SignalUpdate
Триггер события
09/05/2022 10:5...
Название триггера: SignalUpdate
Запрос: SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'
Детали
Важное
Добав...
Добавить з...
Источник Autorun
Тип Подписчик события
Имя подписчика SignalUpdate
Команда C:\Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe
Исполняемый модуль C:\Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe
Время создания подписчика (Москва) 09/05/2022 10:50:19 PM
Время создания класса (Москва) 12/07/2019 12:17:28 PM
Класс подписчика COMMANDLINECONS...
Триггеры SignalUpdate
Приоритет Normal
Создатель petrov
Найти текст...
Версия: 2.1.0.125
Всего: 3
Отфильтровано: 3
Выбрано: 1


MK Enterprise (Лицензия Экспертный Центр)
Autorun - Полное и...
Важное - Полное ис...
Следы приложений...
Журнал событий - ...
Лента событий - П...
Информация об ОС ...
Последние событи...
Устройства USB - П...
Hardware - Полное ...
NTFS - Полное иссл...
Информация об извлечении
Экспорт
Сброс фильтров
Вид
Карты
Геоданные
Смарт-фильтр
Фильтры
Учетные записи 2
Группы 13
Контакты 10
Источники 17
Autorun 301
Google Chrome 515
Microsoft Edge 513
Microsoft Edge/IE 862
Mozilla Firefox 32
NTFS 1,672,681
Recycle bin 158
Signal Desktop 22
System Resource Usage 160,766
Thunderbird 17
WhatsApp (desktop) 14,883
Активность пользователя 599
Журнал событий 54,927
Оперативная память 7,228
Последние события 1,059
Следы приложений 183
Устройства USB 50
Найти текст...
Все записи (1,914,796)
Сообщения (39)
Web-активность (1,922)
Файлы (716)
Активность приложений (161,025)
Найти текст...
Тип
Вре...
Описание
От
Event trigger created 12/... SignalUpdate : SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'W...
Event consumer created 12/... SignalUpdate
Trigger-consumer binding created 12/... SignalUpdate - SignalUpdate
Device configuration 07/... Device 'SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001' was configured
Device start 07/... Device 'SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001' was started
Device servicing 07/... Device 'PETROV-IGOR' has been serviced, active worktime was 00:00:00.672
Device setup 07/... Device setup for container '{00000000-0000-0000-FFFF-FFFFFFFFFFFF}' has been completed
File last run/Executable file 07/... E:\request.pdf.exe
MFT record change/$FN MACB, $SI ...B 07/... Users/petrov/AppData/Roaming/Signal/SignalUpdate.exe
Command execution 07/... Started execution of command 'SignalUpdate.exe'
Application activity/Other/Open App/File/Url 08/... C:\Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe
File last run/Executable file 09/... C:\Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe
MFT record change/$FN ...., $SI M... 01/... Users/petrov/AppData/Local/Google/Chrome/User Data/OptimizationHints/340/manifest.json
MFT record change/$FN ...., $SI M... 01/... Users/petrov/AppData/Local/Google/Chrome/User Data/OptimizationHints/340/optimization-hints.pb
MFT record change/$FN ...., $SI M... 01/... Users/petrov/AppData/Local/Google/Chrome/User Data/OptimizationHints/340/_metadata/verified_cont...
MFT record change/$FN ...., $SI M... 01/... Users/petrov/AppData/Local/Google/Chrome/User Data/OriginTrials/1.0.0.13/manifest.json
MFT record change/$FN ...., $SI M... 01/... Users/petrov/AppData/Local/Google/Chrome/User Data/OriginTrials/1.0.0.13/_metadata/verified_conte...
MFT record change/$FN ...., $SI M... 01/... Users/petrov/AppData/Local/Google/Chrome/User Data/SSLErrorAssistant/7/manifest.json
Дубликаты
Дубликатов не обнаружено
Фильтр по времени
Матрица активности
Диаграмма активности
Tuesday, January 1, 1980 - Tuesday, September 13, 2022
Группировать по: Год | Месяц | День
Saturday, January 1, 2005 и ранее
Tuesday, September 13, 2022
Детали
Важное
Добави...
Добавить з...
Источник NTFS
Тип MFT record change/ $FN MACB, $SI ...B
Время (Москва) 07/13/2022 09:31:22 AM (UTC+3)
ID записи 87238
MACB $FN MACB, $SI ...B
Путь к файлу Users/petrov/AppData/Roaming/Signal/SignalUpdate.exe
Версия: 2.1.0.125
Всего: 1,914,796
Отфильтровано: 1,914,796
Выбрано: 1
1 новое уведомление

Полное исследование / Игорь Петров

Часовой пояс (UTC+03:00) Москва (Европа)
ОС Windows 10.0.19044
Номер инцидента Добавить номер инцидента
Номер вещдока Добавить номер вещдока

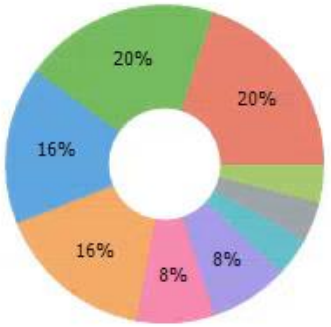
Статистика | Извлечение | Владелец | Общая информация | Устройство | Фото | Заметка

Последние коммуникации

Мария Петрова	04/19/2022 04:37:43 PM
Рабочий чат Чувство ...	04/19/2022 12:18:39 PM
Andrew Komolin	04/19/2022 12:18:39 PM
Магика	04/19/2022 12:12:44 PM
petrov@feel-of-style.ru...	04/06/2022 11:54:56 AM
Komolin Andrew	04/06/2022 11:54:56 AM
petrov@feel-of-style.ru...	04/06/2022 08:53:22 AM
Анна Копылова	04/05/2022 08:29:42 AM
petrov@feel-of-style.ru...	04/04/2022 09:24:29 AM
Игорь Петров petrov@...	04/04/2022 09:14:07 AM

Перейти в Контакты

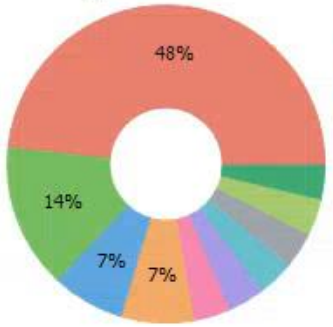
Топ 10 контактов



5 (20.00%)	Анна Копылова
5 (20.00%)	Мария Петрова
4 (16.00%)	Komolin Andrew
4 (16.00%)	Ермакович Вадим Викторович
2 (8.00%)	Игорь Петров petrov@feel-o...
2 (8.00%)	Анна Копылова
1 (4.00%)	Магика
1 (4.00%)	Andrew Komolin
1 (4.00%)	Петрова Мария Львовна

Перейти в Контакты

Топ 10 групп



13 (48.15%)	Рабочий чат Чувство Стиля
4 (14.81%)	petrov@feel-of-style.ru,erm...
2 (7.41%)	petrov@feel-of-style.ru,ko...
2 (7.41%)	petrov@feel-of-style.ru,ko...
1 (3.70%)	petrov@feel-of-style.ru,ko...
1 (3.70%)	Игорь Петров petrov@feel-...
1 (3.70%)	Игорь Петров petrov@feel-...
1 (3.70%)	petrov@feel-of-style.ru,kop...
1 (3.70%)	petrov@feel-of-style.ru,kop...
1 (3.70%)	petrov@feel-of-style.ru,kop...

Перейти в Контакты

Общие разделы 8

- Приложения 10
- Аккаунты и пароли 9
- Контакты 34
- Отчёты
- Поисковые запросы 14
- Снимки
- Сообщения 39
- Файлы 48,331

Системные артефакты 13

- Partitions 5
- Hardware 509
- Информация об ОС 11,328
- Autorun 507
- Журнал событий 54,928
- NTFS 667,889/156,690

MK Enterprise (Лицензия Экспертный Центр)

Оперативная память - По... | Важное - Полное исследо...

Информация об извлечении | Экспорт | Сброс фильтров | Вид | Карты

Фильтры

- Источники 1
  - Оперативная память 5
- Теги 1
  - Без тега 5

Найти текст...

Все данные | Важное | Теги | Заметки

Найти текст...

Тип	Детали
Network connection/Established	Локальный адрес: 192.168.6.244 Удаленный адрес: 87.242.105.205 Локальный порт: 61640 Удаленный порт: 443
Process created	Имя файла: svchost.exe
Process created	Имя файла: OpenWith.exe
Файловый дескриптор	Имя: \Device\HarddiskVolume3\Users\petrov\Desktop
Файловый дескриптор	Имя: \Device\HarddiskVolume3\Users\petrov\Desktop\Базы клиентов\Клиентская ...

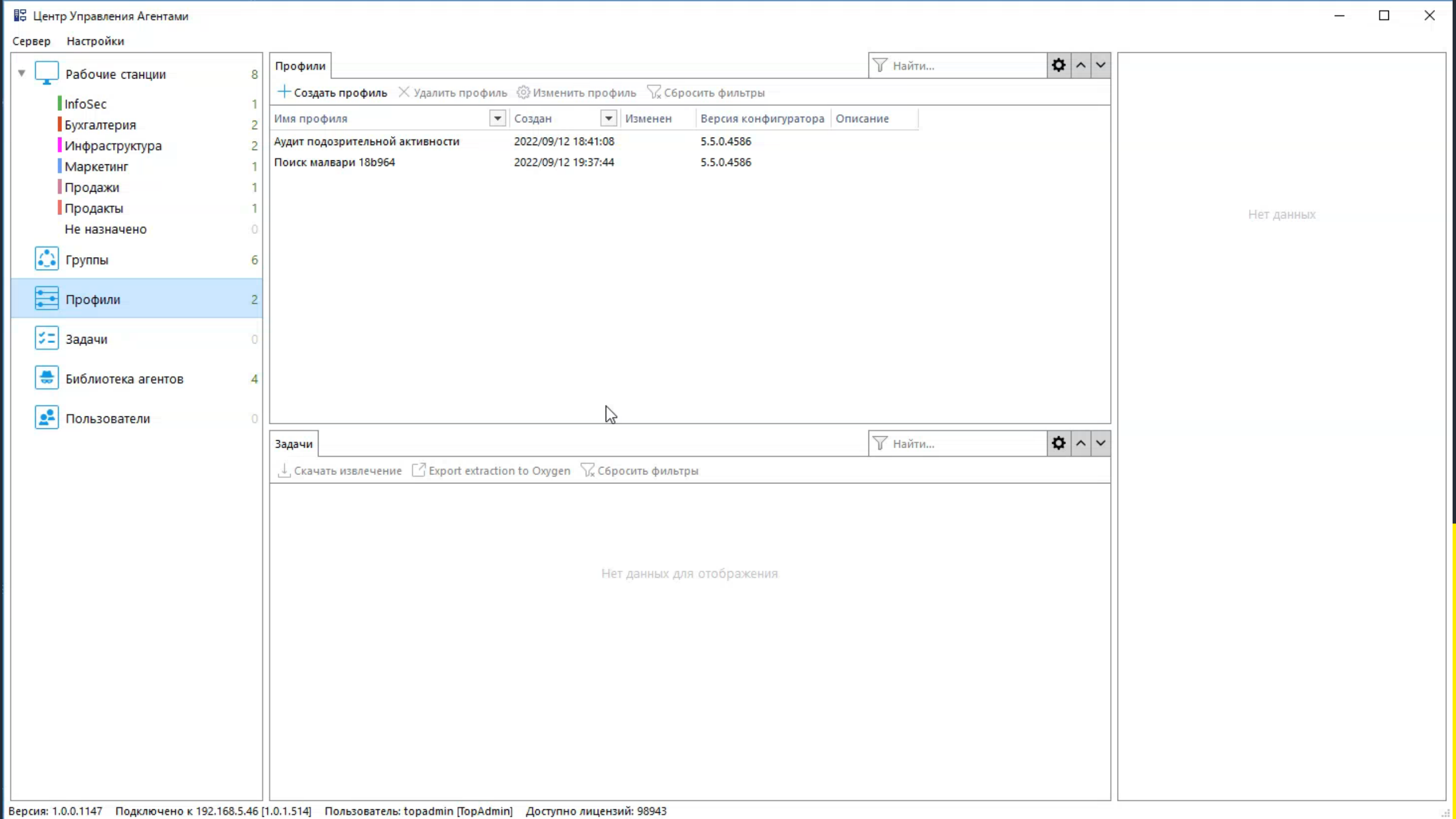
Детали

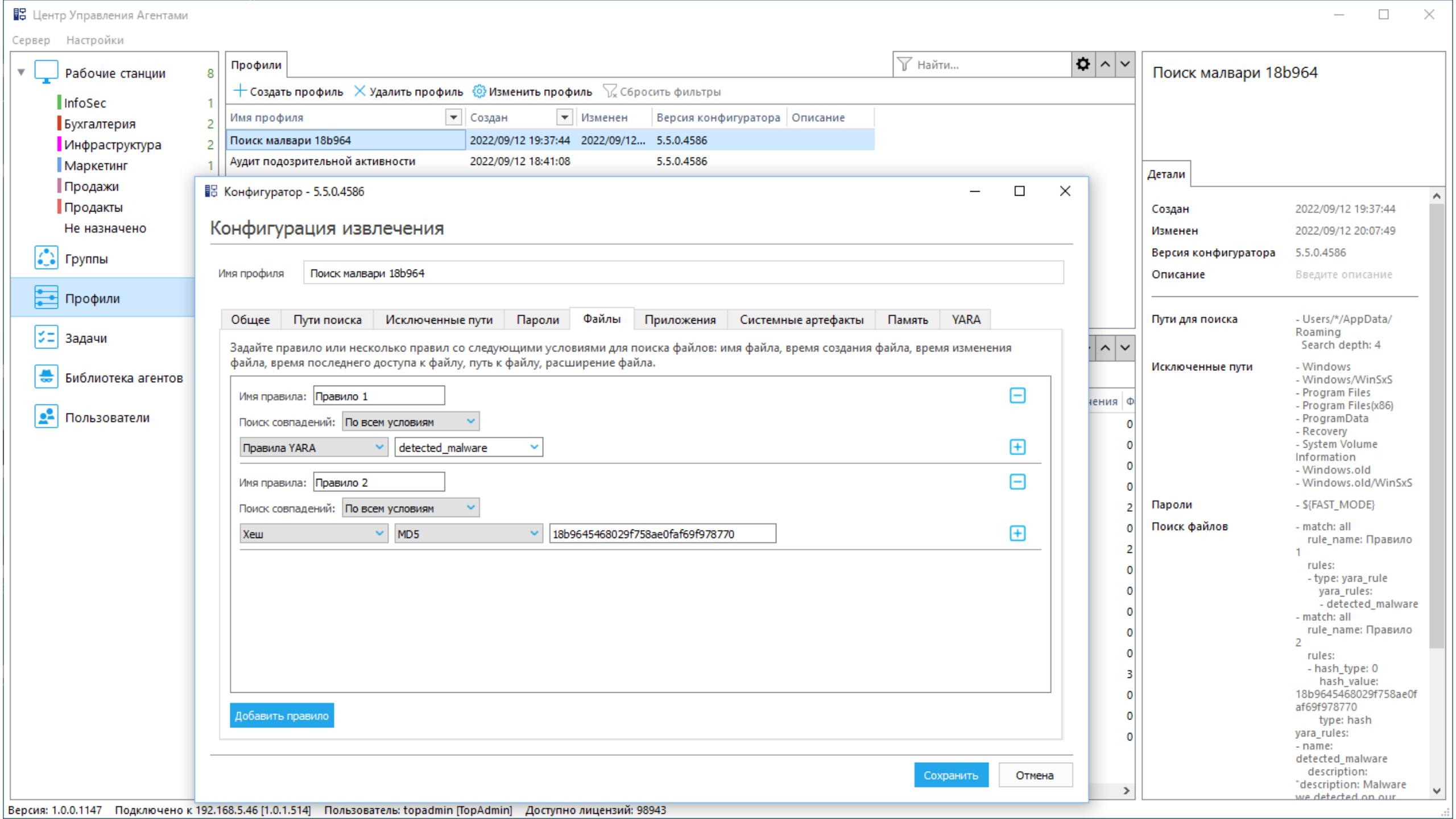
Важное | Добавить тег | Добавить заметку

Источник Оперативная память
Тип Файловый дескриптор
Имя \Device\HarddiskVolume3\Users\petrov\Desktop\Базы клиентов\Клиентская база 2022 год.xlsx
ID процесса 12404
Флаги доступа 1048705
Дескриптор 13976

Версия: 2.1.0.125 Всего: 5 Отфильтровано: 5 Выбрано: 1

```
Field0
Field1
zonedTimeFromTimeImpl
zonedTimeFromAdjTimeImpl
name
bCryptGenRandom
queryProcessCycleTime
queryUnbiasedInterruptTime
queryIdleProcessorCycleTime
coresCount
hIntel
ValueError
base64.nim
decode
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
@) at location
@` (ord
@Invalid base64 format character `
?456789:;<=
 !"#$%&'()*+,-./0123
ValueError
strformat.nim
parseStandardFormatSpecifier
formatValue
@strformat.nim(320, 9) `v < 26`
@invalid type in format string for number, expected one  of 'x', 'X', 'b', 'd', 'o' but got:
@invalid format string, cannot parse:
@[!] fdlEDOgpCumVBVeGRrtSINPD FAILED to resume thread:
@[*] fdlEDOgpCumVBVeGRrtSINPD resumed thread successfully.
@[!] gYuOiGRPCKWTubonbibfqXsQ FAILED to add routine to APC queue:
@[*] gYuOiGRPCKWTubonbibfqXsQ added routine to APC queue successfully.
@EwVvGShaCzirXMHwOvZEmnSc FAILED to modify permissions:
@[*] EwVvGShaCzirXMHwOvZEmnSc modified permissions successfully.
@[!] AtONTUzajEuwaOGNqdPpHNQa FAILED to write decoded payload to allocated memory:
@[*] AtONTUzajEuwaOGNqdPpHNQa wrote decoded payload to allocated memory successfully.
@[!] FAikJPxLwcDkQGTYlgJXDkwG FAILED to allocate memory in created process, exiting:
@[*] FAikJPxLwcDkQGTYlgJXDkwG allocated memory in the created process sucessfully.
@[*] Started process with PID:
@calc
@bcmode.nim(503, 9) `len(input) <= len(output)`
@GsIUCZ2QrF2ad+yWaKIpwg==
@JEpsjbbnvsedRxLAaqFxQxLQpHbngKTv
@n+XQi38M7lshABSTjGeu5QaU7Jvq4vqiHP9AP/yPhWKa8nb8BTHEptcVhWbF8iWFt2I9zn1PEdYycX6U7MZa3IxeJ6ymNpZdmuUHshmfplbc48StyKGqZjrtl+S6LoIzeIAzHA56AKS1nPhUyjKSZ6eMFD8WssI5bdntp2mRmTSqLoObWW4CPKWjCAfAAUzLkfVyMjg92Ef
StZBG/nWVpeAiAP4shMkuUHiNcX5e9ZlH5mXrK3ql+9G/DAvbqeA6EXNfJgw7FhIeBQtOxdG3O2aaXaZyP2nE6nHpxXxyVduUbQBT4O1eL7c9JyKYPBaG8qdZyzOHEXrlwqNRg+/+6fWlKnEeQefKoQ912VsbI6Olh6rmkc9PCa9hiNOLitgPAVRNM948nQOXzrPQyZsIOIr
IJzzbRCaf1YJwxaorQTZoC7Bbw6n9NlOLGGuiZn4styqugIeKtqpL3DM5jSNRMSwYrNwSOkNIHhTOR9qWBf6SJj1REM1CZZErBn4nvVaNLT7xx1vb2vNYLEBAu37UM9tB/TO5yB5jLGqA+Jn2KzOVwZX8EYbUrEuw+GKktd5OcIs5s4TipoS5Bn4ik1sAwr8Jc1iu4lVH3Kv
u1AhOmUGAKNlwTnYGnBqbVfhVazHnCF4w7HJ+nqiKPDq51BDcLhe6K5wvnaUsljOGVPFVFdYVKFTAqnA/m0d8opzoo+dGcwmdn8rf6wdRf8t0ekOy2c+un5r6YdFNoducTS7ztfT7Ok/XMIjQ1ehPE6MrDqQKuTopT9ubVaCvZEHV27ZY/bksiX7t3+2M4PqXCOgZ65OC3VU
+RZ+P4YY4g/8Se7BCgNFEv2ezJTqybAzhOTNlmQQ5f3wrT5/NfknfCdr8YybyOjMqrI2OaNabG1v51Q1OCrnwO7xBYWg4DRl+GIk3K3yKGTMap9JeUFcbiR0h71K42i9j/Cyf5N1yaDagk/cKuaOPOeWh4886MOaZuw65xYusQSYOLcgq6JM15RKFs8WIfBssw+QP6NY4qyM
zHsp8fN4J3s0VcfEWbOHIDNrOnz6nmfSmJrod1mH9pIcfvOnYt3C6qXjqMDtxe8mHYBPB4jrYttfppE4MICuyIhLaAC9A3TN87ZKxcyQPMiobUgBC4azf1+Yvhp5+7xnGCUxUn7ljdD1T4zmzeP3XBSQPtb1Y3xApOs2jXkvnJQLfx5w7mrtEOtZO9vak5VPwNaKgnO6KRjI
Pt2LwrDLpj88TVTbCmcVHOoHTqBmYN3TH365oWVivD7DpsELXO7al/Lr7KVElIWvLK1hdvDC7vuT6oPa4J7BaBe18k3LdXumoXoQMfN7CjTT27mJt4HXKgPlFXLCUme5EArmhU9bw7rFoBmSyjZ+3a8wOguCmzd9Eurq/63nQYTVQGnP/V/AWVfA4iibOsdlbQ/3dO1bimh/
3IOYuZbjO/+yTdEIMQBBSuEhtSSA3XrAWMditJFX1kECLubNAQ5fLLFAEZ1BgP9as460aujoztOEf60Vgly4aHr/8tLKUir2sFe2bEQALWerN1eHxJGYIxVtSDNk+oPTX7bPCJuC8NgIaQ8vZkR6+9nBeNfP9Zdet3BqhD8dn7TKeLgxfSIt6YgkvgtG03ZfhpUIiA5kl4S6
aoxZMCWQY86gTfrXUME/v+T5yL/VXflY3bQZvK5RCamZkcvb8XWbBSzZr74FUCeaJyKL5bN3V5r839Vb866xGzjWHfZiDbXLcwNiEbNAxvAAZby/eopDVn2Vf/PG8/mBeO2i2SW8/uDIiMuLj3DyKw8Mxwc+qRQNOUtvU2W4VqPk16rD39nbXOtYBNfg+pRjjVWNdt4DKLyO
9EZS4jaZ6Tj0OZk84zw+lJtyFVrSkQ/NWC36XTWq17+Zhh6pL/MWBQj7dDJc9yXoC7FKQjq2RjbZcwoQZFlBwkd+BJVr/ukUqkxFyBw+jLuM2SByjcht/GPi3y2OUsaMSeic7GxTmLahJ881nfCt9RacIASweXyiVYmO/kjoZGG2cqTWtefTX7RYlAN84mLeiDxZUtCJ+Myi
CuM/ob1fCXoblbfLrbA7ePa5N+/EGxKNzVgniUGxQTxDJUVsLo4qSw71G7uO85gP2uFKyEXrMUXZk44T2j8flsxDlEhdiF7jLeCROOXWy2gdlQlEMie6MPTd5swqyBOvQ3AkOoKpFkg/U8o3zHeM8H6ZCDO3Zw+Gr4txu0Qhhmw/Agi6uRY9djZdFPo/ONpSczn X9KEnm/c1
Kt6NqhCS/iKU44MW5tcQOkMOjZNdMbfUaH/H2uk+fbODhqWYBbOUaysx2UIleu85mf4eBMO3NHJrSIezKmMUUO6wIr4gUbrVTgWVbDhlm7zrCV845cfnHHOdvMe2i5dULMn7scwOMk/wa63uSy9dDG4NOZuBviV/OceIa+nDdAoNb7a8sgPnQOQRfTd8Z+RQ3EhvIsbD+2cC
WP/rmHEYTbXb4A/NFYahwSiLaeP8Qi9G8DUQ9ISPWqJr7GPm+FzdgpF8mOImx6kGsPrF6S1Ops/CyqAdmIOJUWZO99+asDezqGnMj3sDhYOVNNbrcMcIOy3upLOjN8HbpOgQ/fA6QCA2cSzjA5kEmkbQvjQIaDgJjfTBltmrt5wdekmhVWvA9Bsj/QjlEUxpLquFDJbj6rBn
pIL9Wvy6RPLRiBBKfRwlCbpVb43tUO9067FsZ12dbeF4fsCzafydJHjqPjnwvtPWyg9NBbGDsbPmehukP8QCoAwKKNRmCIzIcUDK+BXwUTzhDeNuqzYuAdcvyky6wJMXDOe/r3kGwiXaB5b15y1L2w1X4EwodlIQxbnctv1xajqwv5JEYiA/NMFUU2ps7DNeY5KGmxTk8Iug
DCPGcHePrbEkD+KYp1sWKUZmV/WgYghU8lIqQ47MgO9B/kkjGdWf84WNUcmfKO4lObobVbxltDV8v5ltkFUNvVHKPOJ9NerKWGLaoofa2I+ZufSdxZdN2VRajmTTDFwWeA6YXL92OZSMhusWF5d/RCNxG/4tgemTBMFHwciKEmo3wf4NJGOWDNAkwmPKWLCu1MVyzB8T49C9
T1esPGdPdi6tZ88O7cYkaiJ9Wa7yepyZBMTfP66usT5/xIcwSltV1B1x9kGNpMf3egH26ea5iPN+SwcVDS7OkfHEZq7tGPaTko56g14t6r0bdYKkV2jiPUqUGHjd4c4+U6jQAAeZwv2PdtsIlBUvdo4Rvk9ncfJv91j1JMi5b8zfpDgyj4OiiUHmZ7Z9gIcyY2OREpTqo+20
qC4S9B8FDE45UB1zMuSptWvqNbAwHsLQGHvrdvUis1BVYA+8VW+EAErfaG2/a+vEt7uEL8QUJGHxM1T/I4o8VtvNC/IfHqiWzIu2utxL4vf3kEwdeKGJfBQrz04icDp8ZKxYmhZLv9MNvwhGZhBKkIUKB1vwvJ6aH+G9NV4xqf11Z2mTcUiT7DxEmighNMvSJ81+Rqul4ucr
```


Центр Управления Агентами
Сервер
Настройки
Рабочие станции 8
InfoSec 1
Бухгалтерия 2
Инфраструктура 2
Маркетинг 1
Продажи 1
Продакты 1
Не назначено 0
Группы 6
Профили 2
Задачи 0
Библиотека агентов 4
Пользователи 0
Профили
Найти...
Создать профиль
Удалить профиль
Изменить профиль
Сбросить фильтры
Имя профиля
Создан
Изменен
Версия конфигуратора
Описание
Аудит подозрительной активности
2022/09/12 18:41:08
5.5.0.4586
Поиск малвари 18b964
2022/09/12 19:37:44
5.5.0.4586
Нет данных
Задачи
Найти...
Скачать извлечение
Export extraction to Oxygen
Сбросить фильтры
Нет данных для отображения
Версия: 1.0.0.1147
Подключено к 192.168.5.46 [1.0.1.514]
Пользователь: topadmin [TopAdmin]
Доступно лицензий: 98943


Центр Управления Агентами
Сервер
Настройки
Рабочие станции 8
InfoSec 1
Бухгалтерия 2
Инфраструктура 2
Маркетинг 1
Продажи
Продакты
Не назначено
Группы
Профили
Задачи
Библиотека агентов
Пользователи
Профили
Найти...
Создать профиль
Удалить профиль
Изменить профиль
Сбросить фильтры
Имя профиля
Создан
Изменен
Версия конфигуратора
Описание
Поиск малвари 18b964
2022/09/12 19:37:44
2022/09/12...
5.5.0.4586
Аудит подозрительной активности
2022/09/12 18:41:08
5.5.0.4586
Поиск малвари 18b964
Детали
Создан 2022/09/12 19:37:44
Изменен 2022/09/12 20:07:49
Версия конфигуратора 5.5.0.4586
Описание Введите описание
Пути для поиска - Users/*/AppData/Roaming Search depth: 4
Исключенные пути - Windows - Windows/WinSxS - Program Files - Program Files(x86) - ProgramData - Recovery - System Volume Information - Windows.old - Windows.old/WinSxS
Пароли - ${FAST_MODE}
Поиск файлов - match: all rule_name: Правило 1 rules: - type: yara_rule yara_rules: - detected_malware - match: all rule_name: Правило 2 rules: - hash_type: 0 hash_value: 18b9645468029f758ae0faf69f978770 type: hash yara_rules: - name: detected_malware description: "description: Malware we detected on our
Конфигуратор - 5.5.0.4586
Конфигурация извлечения
Имя профиля
Поиск малвари 18b964
Общее
Пути поиска
Исключенные пути
Пароли
Файлы
Приложения
Системные артефакты
Память
YARA
Задайте правило или несколько правил со следующими условиями для поиска файлов: имя файла, время создания файла, время изменения файла, время последнего доступа к файлу, путь к файлу, расширение файла.
Имя правила: Правило 1
Поиск совпадений: По всем условиям
Правила YARA
detected_malware
Имя правила: Правило 2
Поиск совпадений: По всем условиям
Хеш
MD5
18b9645468029f758ae0faf69f978770
Добавить правило
Сохранить
Отмена
Версия: 1.0.0.1147
Подключено к 192.168.5.46 [1.0.1.514]
Пользователь: topadmin [TopAdmin]
Доступно лицензий: 98943

Центр Управления Агентами

Сервер Настройки

- Рабочие станции 8
  - InfoSec 1
  - Бухгалтерия 2
  - Инфраструктура 2
  - Маркетинг 1
  - Продажи 1
  - Продакты 1
  - Не назначено 0
- Группы 6
- Профили 2
- Задачи 0
- Библиотека агентов 4
- Пользователи 0

Рабочие станции

Найти...

Запустить задачу | Добавить рабочую станцию | Назначить группу | Развернуть агент | Обновить версию

Название рабочей станции	Имя хос...	Пользователи	Статус агента	Группа	IP
Сервер SIEM	CUP-TestSide	cup	Онлайн	Инфраструктура	1
Мария Петрова	mariapc	petrova	Онлайн	Бухгалтерия	1
Сервер DC	Server	Administrator	Онлайн	Инфраструктура	1
Игорь Петров	petrov-igor	petrov	Онлайн	Продажи	1
Ермакович Вадим	IB-TestSide	ermakovich	Онлайн	InfoSec	1
Бедняков Валерий	bednyakov	bednyakov	Онлайн	Маркетинг	1
Копылова Анна	annapc	kopylova	Онлайн	Бухгалтерия	1
Зябликова Екатерина (домашний)	KateHome	admin	Онлайн	Продакты	1

Задачи

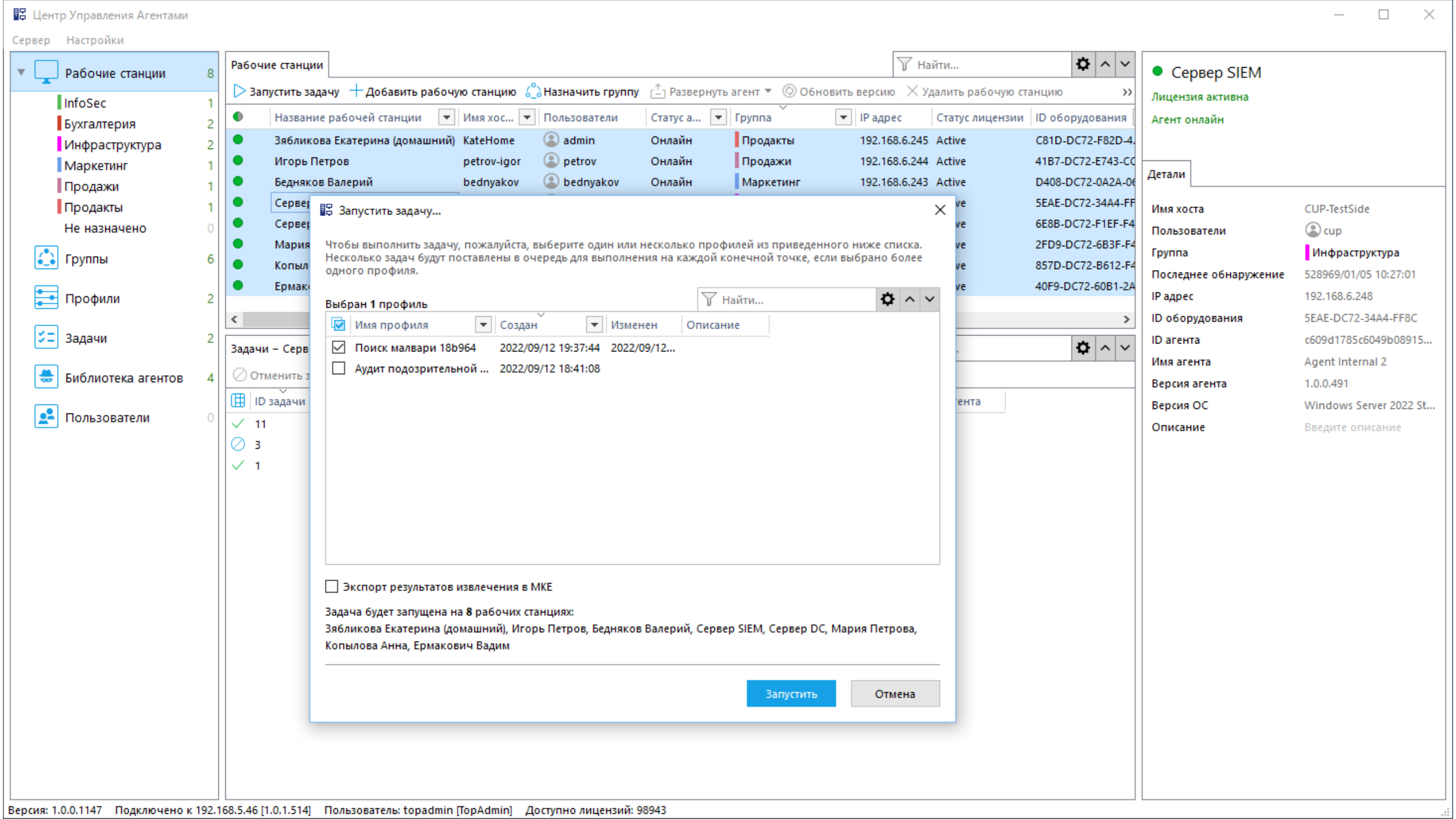
Найти...

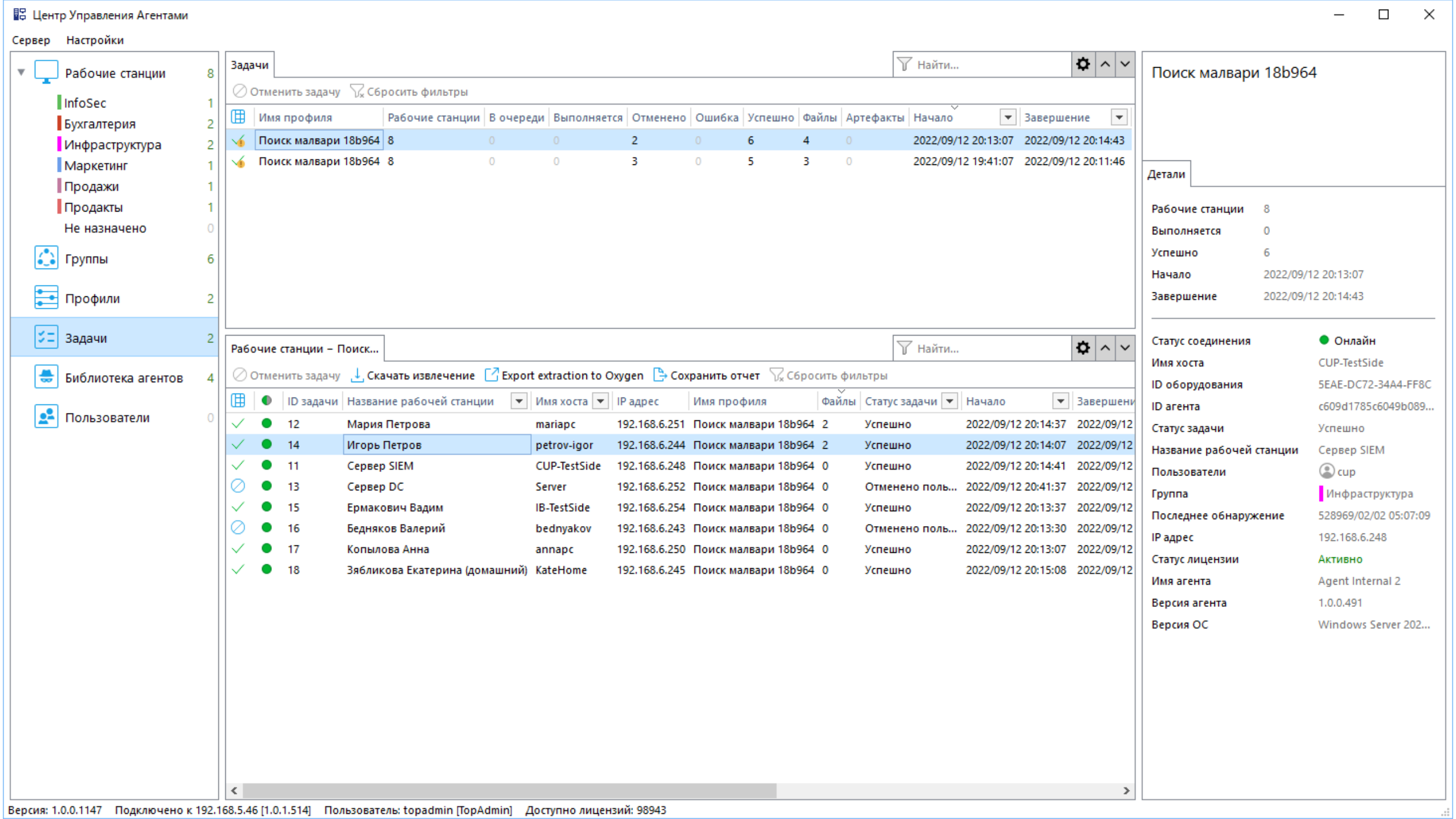
Отменить задачу | Скачать извлечение | Export extraction to Oxygen | Сбросить фильтры

Нет данных для отображения

Нет данных

Версия: 1.0.0.1147 Подключено к 192.168.5.46 [1.0.1.514] Пользователь: topadmin [TopAdmin] Доступно лицензий: 98943


Центр Управления Агентами
Сервер
Настройки
Рабочие станции 8
InfoSec 1
Бухгалтерия 2
Инфраструктура 2
Маркетинг 1
Продажи 1
Продакты 1
Не назначено 0
Группы 6
Профили 2
Задачи 2
Библиотека агентов 4
Пользователи 0
Рабочие станции
Найти...
Запустить задачу
Добавить рабочую станцию
Назначить группу
Развернуть агент
Обновить версию
Удалить рабочую станцию
Название рабочей станции
Имя хос...
Пользователи
Статус а...
Группа
IP адрес
Статус лицензии
ID оборудования
Зябликова Екатерина (домашний) KateHome admin Онлайн Продакты 192.168.6.245 Active C81D-DC72-F82D-4...
Игорь Петров petrov-igor petrov Онлайн Продажи 192.168.6.244 Active 41B7-DC72-E743-C0
Бедняков Валерий bednyakov bednyakov Онлайн Маркетинг 192.168.6.243 Active D408-DC72-0A2A-06
Сервер 5EAE-DC72-34A4-FF
Сервер 6E8B-DC72-F1EF-F4
Мария 2FD9-DC72-6B3F-F4
Копыл 857D-DC72-B612-F4
Ермак 40F9-DC72-60B1-2A
Задачи – Серв
Отменить з
ID задачи
11
3
1
Запустить задачу...
Чтобы выполнить задачу, пожалуйста, выберите один или несколько профилей из приведенного ниже списка. Несколько задач будут поставлены в очередь для выполнения на каждой конечной точке, если выбрано более одного профиля.
Выбран 1 профиль
Найти...
Имя профиля
Создан
Изменен
Описание
Поиск малвари 18b964 2022/09/12 19:37:44 2022/09/12...
Аудит подозрительной ... 2022/09/12 18:41:08
Экспорт результатов извлечения в MKE
Задача будет запущена на 8 рабочих станциях:
Зябликова Екатерина (домашний), Игорь Петров, Бедняков Валерий, Сервер SIEM, Сервер DC, Мария Петрова, Копылова Анна, Ермакович Вадим
Запустить
Отмена
Сервер SIEM
Лицензия активна
Агент онлайн
Детали
Имя хоста CUP-TestSide
Пользователи cup
Группа Инфраструктура
Последнее обнаружение 528969/01/05 10:27:01
IP адрес 192.168.6.248
ID оборудования 5EAE-DC72-34A4-FF8C
ID агента c609d1785c6049b08915...
Имя агента Agent Internal 2
Версия агента 1.0.0.491
Версия ОС Windows Server 2022 St...
Описание Введите описание
Версия: 1.0.0.1147 Подключено к 192.168.5.46 [1.0.1.514] Пользователь: topadmin [TopAdmin] Доступно лицензий: 98943


Центр Управления Агентами
Сервер
Настройки
Рабочие станции 8
InfoSec 1
Бухгалтерия 2
Инфраструктура 2
Маркетинг 1
Продажи 1
Продакты 1
Не назначено 0
Группы 6
Профили 2
Задачи 2
Библиотека агентов 4
Пользователи 0
Задачи
Найти...
Отменить задачу
Сбросить фильтры
Имя профиля | Рабочие станции | В очереди | Выполняется | Отменено | Ошибка | Успешно | Файлы | Артефакты | Начало | Завершение
Поиск малвари 18b964 | 8 | 0 | 0 | 2 | 0 | 6 | 4 | 0 | 2022/09/12 20:13:07 | 2022/09/12 20:14:43
Поиск малвари 18b964 | 8 | 0 | 0 | 3 | 0 | 5 | 3 | 0 | 2022/09/12 19:41:07 | 2022/09/12 20:11:46
Рабочие станции – Поиск...
Найти...
Отменить задачу
Скачать извлечение
Export extraction to Oxygen
Сохранить отчет
Сбросить фильтры
ID задачи | Название рабочей станции | Имя хоста | IP адрес | Имя профиля | Файлы | Статус задачи | Начало | Завершени
12 | Мария Петрова | mariapc | 192.168.6.251 | Поиск малвари 18b964 | 2 | Успешно | 2022/09/12 20:14:37 | 2022/09/12
14 | Игорь Петров | petrov-igor | 192.168.6.244 | Поиск малвари 18b964 | 2 | Успешно | 2022/09/12 20:14:07 | 2022/09/12
11 | Сервер SIEM | CUP-TestSide | 192.168.6.248 | Поиск малвари 18b964 | 0 | Успешно | 2022/09/12 20:14:41 | 2022/09/12
13 | Сервер DC | Server | 192.168.6.252 | Поиск малвари 18b964 | 0 | Отменено поль... | 2022/09/12 20:41:37 | 2022/09/12
15 | Ермакович Вадим | IB-TestSide | 192.168.6.254 | Поиск малвари 18b964 | 0 | Успешно | 2022/09/12 20:13:37 | 2022/09/12
16 | Бедняков Валерий | bednyakov | 192.168.6.243 | Поиск малвари 18b964 | 0 | Отменено поль... | 2022/09/12 20:13:30 | 2022/09/12
17 | Копылова Анна | annapc | 192.168.6.250 | Поиск малвари 18b964 | 0 | Успешно | 2022/09/12 20:13:07 | 2022/09/12
18 | Зябликова Екатерина (домашний) | KateHome | 192.168.6.245 | Поиск малвари 18b964 | 0 | Успешно | 2022/09/12 20:15:08 | 2022/09/12
Поиск малвари 18b964
Детали
Рабочие станции 8
Выполняется 0
Успешно 6
Начало 2022/09/12 20:13:07
Завершение 2022/09/12 20:14:43
Статус соединения Онлайн
Имя хоста CUP-TestSide
ID оборудования 5EAE-DC72-34A4-FF8C
ID агента c609d1785c6049b089...
Статус задачи Успешно
Название рабочей станции Сервер SIEM
Пользователи cup
Группа Инфраструктура
Последнее обнаружение 528969/02/02 05:07:09
IP адрес 192.168.6.248
Статус лицензии Активно
Имя агента Agent Internal 2
Версия агента 1.0.0.491
Версия ОС Windows Server 202...
Версия: 1.0.0.1147 Подключено к 192.168.5.46 [1.0.1.514] Пользователь: topadmin [TopAdmin] Доступно лицензий: 98943

Центр Управления Агентами

Сервер Настройки

- Рабочие станции 8
  - InfoSec 1
  - Бухгалтерия 2
  - Инфраструктура 2
  - Маркетинг 1
  - Продажи 1
  - Продакты 1
  - Не назначено 0
- Группы 6
- Профили 2
- Задачи 2
- Библиотека агентов 4
- Пользователи 0

Задачи

Найти...

Отменить задачу | Сбросить фильтры

Имя профиля	Рабочие станции	В очереди	Выполняется	Отменено	Ошибка	Успешно	Файлы	Артефакты	Начало	Завершение
Поиск малвари 18b964	8	0	0	2	0	6	4	0	2022/09/12 20:13:07	2022/09/12 20:14:43
Поиск малвари 18b964	8	0	0	3	0	5	3	0	2022/09/12 19:41:07	2022/09/12 20:11:46

Задачи – Сервер SIEM

Найти...

Отменить задачу | Скачать извлечение | Export extraction to Oxygen | Сохранить отчет | Сбросить фильтры

ID задачи	Название рабочей станции	Имя хоста	IP адрес	Имя профиля	Файлы	Статус задачи	Начало	Завершени
12	Мария Петрова	mariapc	192.168.6.251	Поиск малвари 18b964	2	Успешно	2022/09/12 20:14:37	2022/09/12
14	Игорь Петров	petrov-igor	192.168.6.244	Поиск малвари 18b964	2	Успешно	2022/09/12 20:14:07	2022/09/12
11	Сервер SIEM	CUP-TestSide	192.168.6.248	Поиск малвари 18b964	0	Успешно	2022/09/12 20:14:41	2022/09/12
13	Сервер DC	Server	192.168.6.252	Поиск малвари 18b964	0	Отменено поль...	2022/09/12 20:41:37	2022/09/12
15	Ермакович Вадим	IB-TestSide	192.168.6.254	Поиск малвари 18b964	0	Успешно	2022/09/12 20:13:37	2022/09/12
16	Бедняков Валерий	bednyakov	192.168.6.243	Поиск малвари 18b964	0	Отменено поль...	2022/09/12 20:13:30	2022/09/12
17	Копылова Анна	annapc	192.168.6.250	Поиск малвари 18b964	0	Успешно	2022/09/12 20:13:07	2022/09/12
18	Зябликова Екатерина (домашний)	KateHome	192.168.6.245	Поиск малвари 18b964	0	Успешно	2022/09/12 20:15:08	2022/09/12

Поиск малвари 18b964

Детали

Рабочие станции	8
Выполняется	0
Успешно	6
Начало	2022/09/12 20:13:07
Завершение	2022/09/12 20:14:43

Статус соединения	Онлайн
Имя хоста	CUP-TestSide
ID оборудования	5EAE-DC72-34A4-FF8C
ID агента	c609d1785c6049b089...
Статус задачи	Успешно
Название рабочей станции	Сервер SIEM
Пользователи	cup
Группа	Инфраструктура
Последнее обнаружение	2022/09/13 08:15:28
IP адрес	192.168.6.248
Статус лицензии	Активно
Имя агента	Agent Internal 2
Версия агента	1.0.0.491
Версия ОС	Windows Server 202...

Версия: 1.0.0.1147 Подключено к 192.168.5.46 [1.0.1.514] Пользователь: topadmin [TopAdmin] Доступно лицензий: 98943

Все данные | Файлы | Контакты | Чаты | Лента событий | Граф связей

Найти текст...

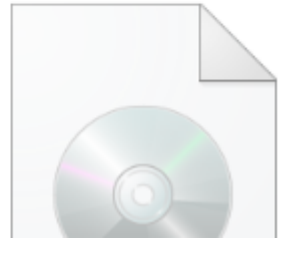
Правила поиска	YARA правила	Файл	Полный путь	Размер файла	Время создания (Москва)	Время пос
Правило 1	detected_malware	request.pdf.iso	C:/Users/petrov/Downloads/Telegram Desktop/request.pdf.iso	524 Кб	2022/07/13 09:22:56 (UTC+3)	2022/07/1
Правило 1	detected_malware	SignalUpdate.exe	C:/Users/petrov/AppData/Roaming/Signal/SignalUpdate.exe	161 Кб	2022/07/13 09:31:22 (UTC+3)	2022/07/1

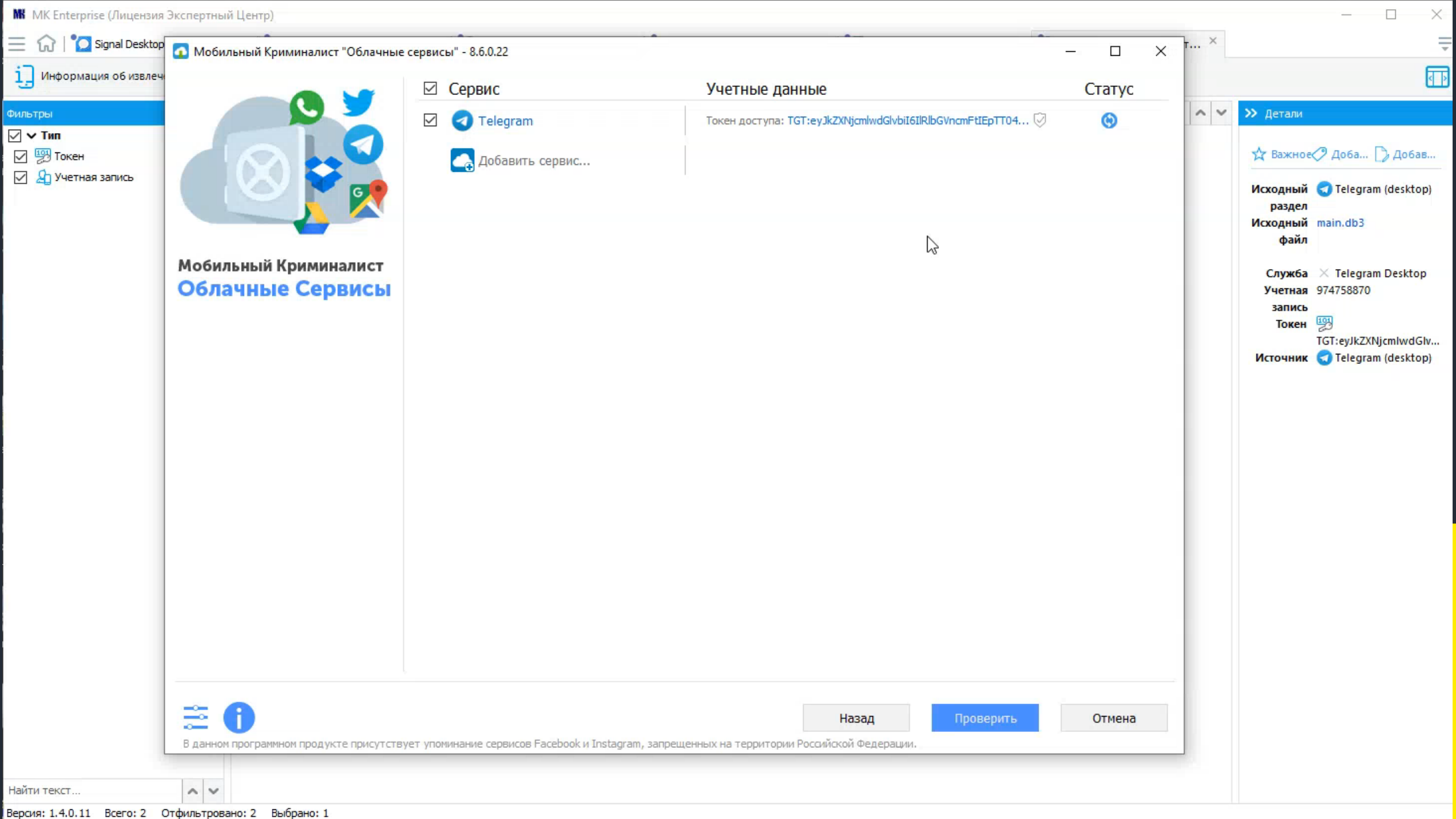
Правило 1

Детали

Важное | Добав... | Добавит...

Исходный файл	FilesData.db3
Размер исходного файла	28.0 KB
Исходная таблица	files_list
Правила поиска	Правило 1
YARA правила	detected_malware
Файл	request.pdf.iso
Полный путь	C:/Users/petrov/Downloads/Telegram Desktop/request.pdf.iso
Размер файла	524 Кб
Время создания (Москва)	2022/07/13 09:22:56 (UTC+3)
Время последнего изменения (Москва)	2022/07/13 09:22:56 (UTC+3)
Время последнего доступа (Москва)	2022/07/13 09:24:19 (UTC+3)




MK Enterprise (Лицензия Экспертный Центр)
Signal Desktop
Информация об извлеч
Фильтры
Тип
Токен
Учетная запись
Мобильный Криминалист "Облачные сервисы" - 8.6.0.22
Мобильный Криминалист
Облачные Сервисы
Сервис
Учетные данные
Статус
Telegram
Токен доступа: TGT:eyJkZXNjcmlwdGlvbiI6IlRlbGVncmFtIEpTT04...
Добавить сервис...
Назад
Проверить
Отмена
В данном программном продукте присутствует упоминание сервисов Facebook и Instagram, запрещенных на территории Российской Федерации.
Детали
Важное
Доба...
Добав...
Исходный раздел
Telegram (desktop)
Исходный файл
main.db3
Служба
Telegram Desktop
Учетная запись
974758870
Токен
TGT:eyJkZXNjcmlwdGlv...
Источник
Telegram (desktop)
Найти текст...
Версия: 1.4.0.11
Всего: 2
Отфильтровано: 2
Выбрано: 1

MK Enterprise (Лицензия Экспертный Центр)

Signal Desktop - Петров По...

Домашний экран

Мобильный Криминалист "Облачные сервисы" - 8.6.0.22

Мобильный Криминалист
Облачные Сервисы

Извлечение завершено!

Данные успешно извлечены из облака

Id извлечения: 99A1AB45DF9F4E71BEE40205E146F8D5
Владелец учетной записи: Petrov
Длительность извлечения: 00:00:28
Общий размер: 851 KB

Облачные сервисы

Telegram - +79259168152

Итоги извлечения

- Сообщения - 10
- Контакты - 559
- Авторизационные сессии - 3
- Изображения - 0
- Видео - 0
- Аудио - 0
- Другие файлы - 1
- Стикеры - 0

Далее | Отмена

В данном программном продукте присутствует упоминание сервисов Facebook и Instagram, запрещенных на территории Российской Федерации.

Карты памяти/МТР извлечения

Импорт резервных копий

Версия: 1.4.0.11

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ИТОГ

- Проведение аудита
- Инициация расследования
- Предотвращение ущерба до его возникновения
- Оптимизация процесса реагирования на подобные инциденты

СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО
СПАСИБО

КОНТАКТЫ:

+7 (495) 909-92-78

clients@mko-systems.ru

mko-systems.ru