

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

с помощью ПО класса



НИКИТА ВЬЮГИН

МЕНЕДЖЕР ПРОЕКТОВ



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

DLP

SIEM

SOAR

DFIR



и другие



ПРОГРАММНОЕ
ОБЕСПЕЧЕНИЕ КЛАССА

DFIR

DFIR

DFIR

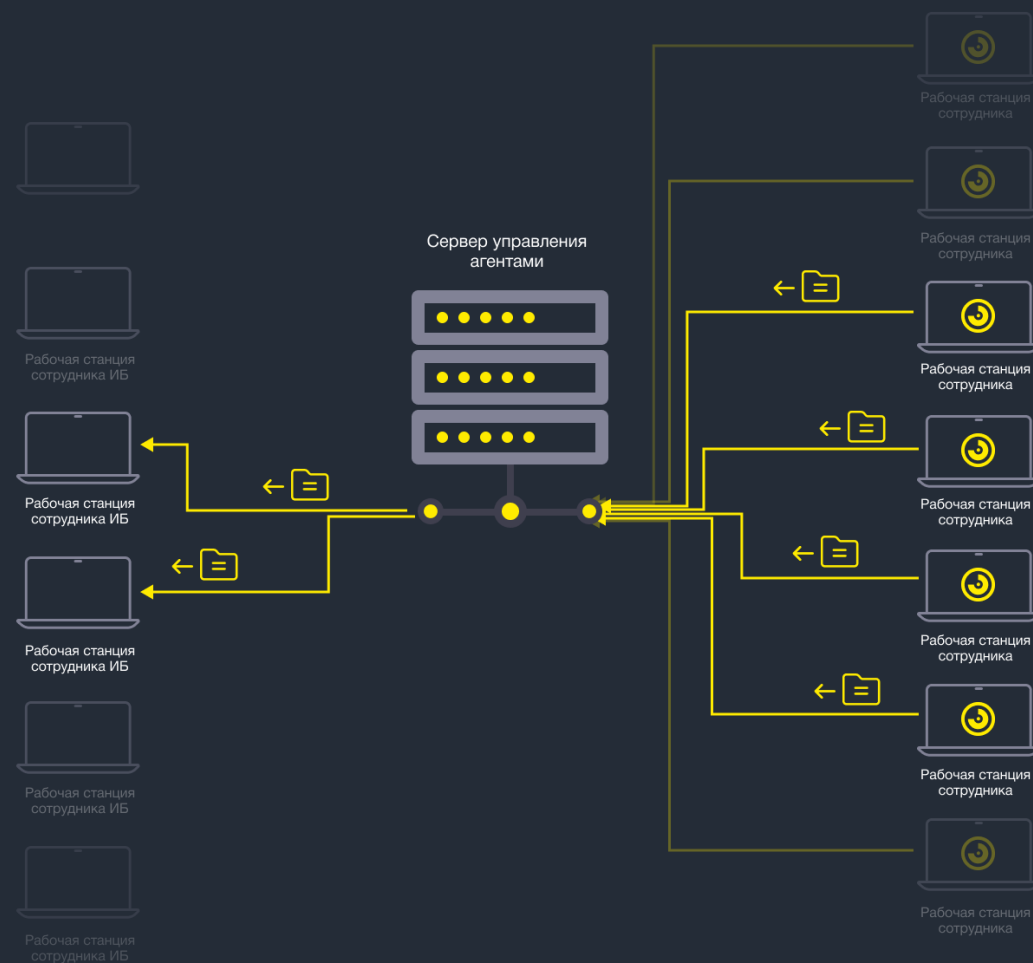
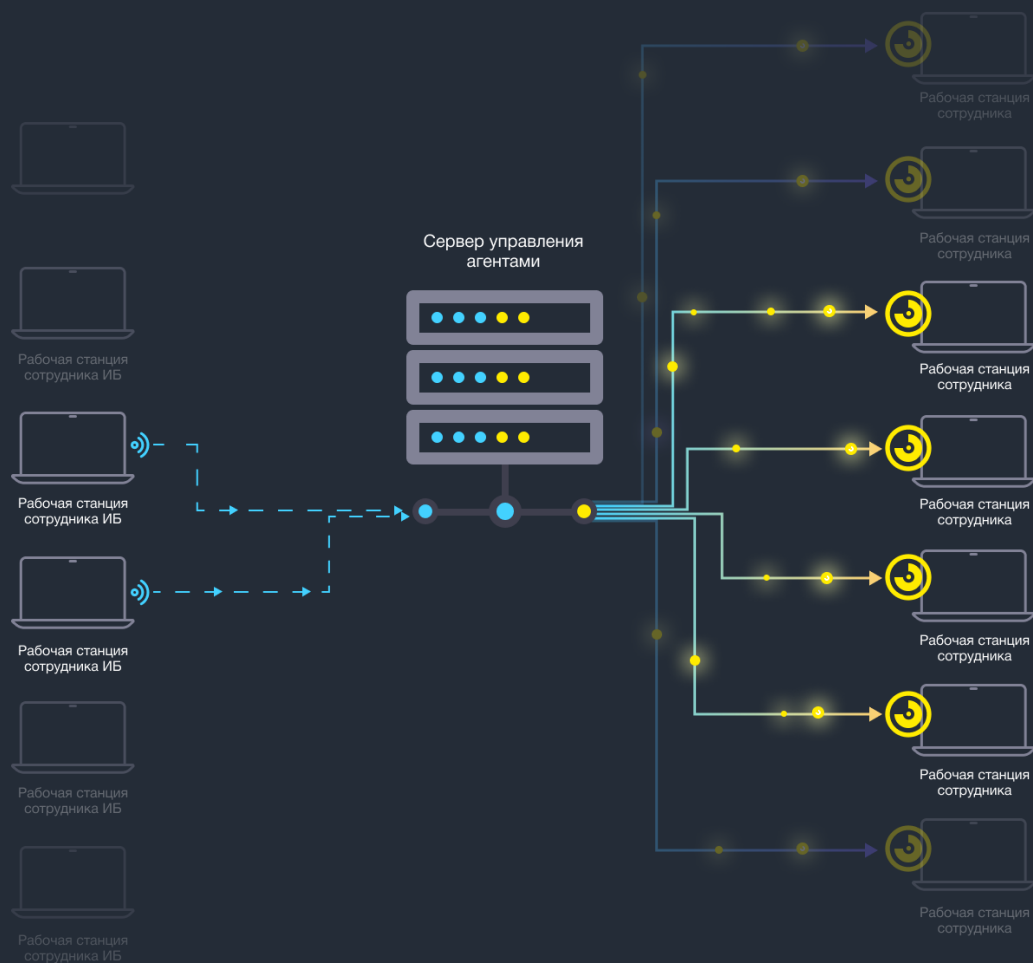
DFIR

DFIR

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



ПОИСК ПО СОДЕРЖИМОМУ ПРАВИЛА YARA

Создать профиль × Удалить профиль ⚙ Изм

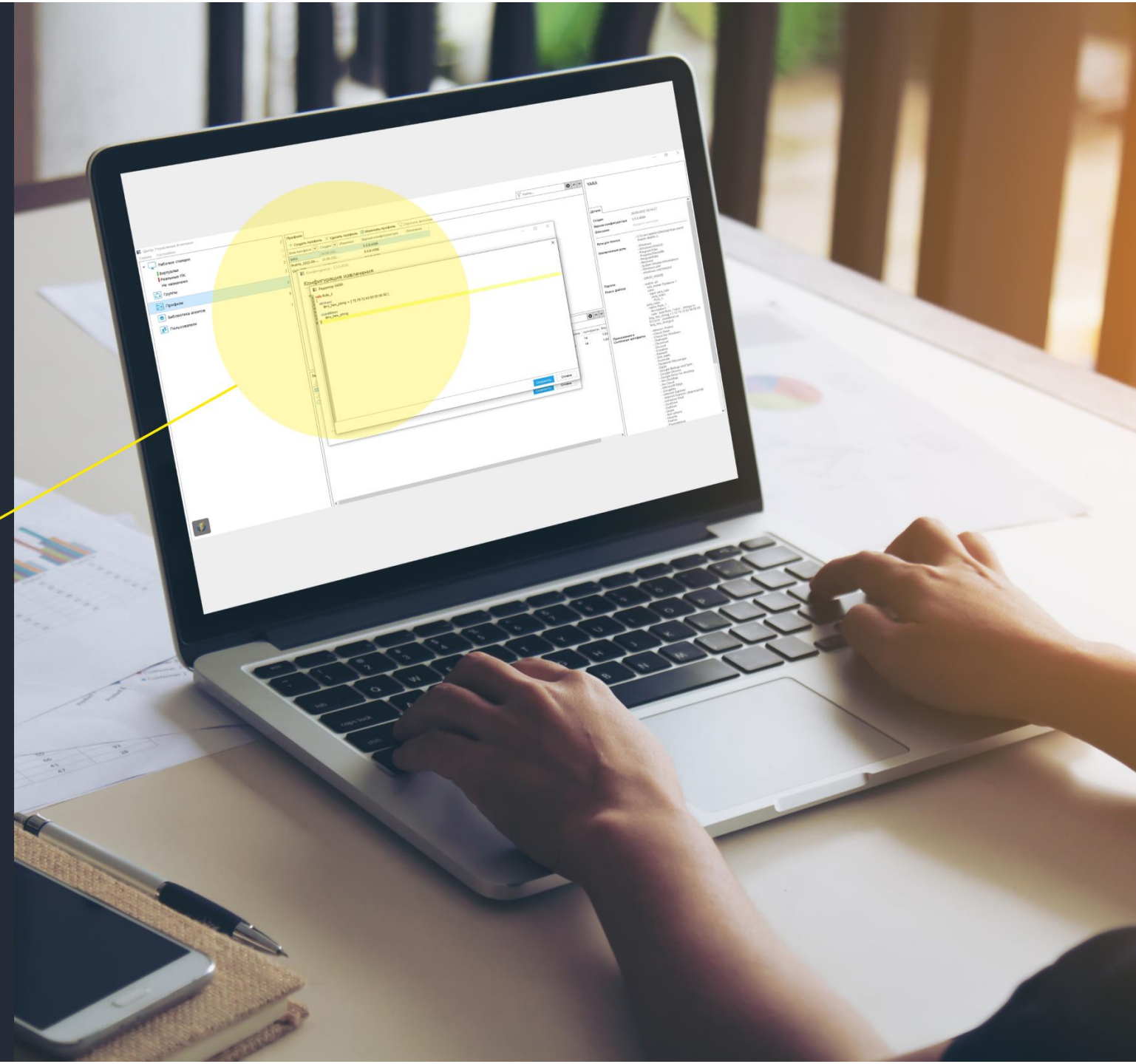
Имя профиля	Создан	Изменен	Версия кон
YARA	24.08.202...		5.5.0.4586
Profile_2022-08-...	25.08.202...		5.5.0.4586
Opt...	24.08.202...		5.5.0.4586

Конфигуратор - 5.5.0.4586

Конфигурация извлечения

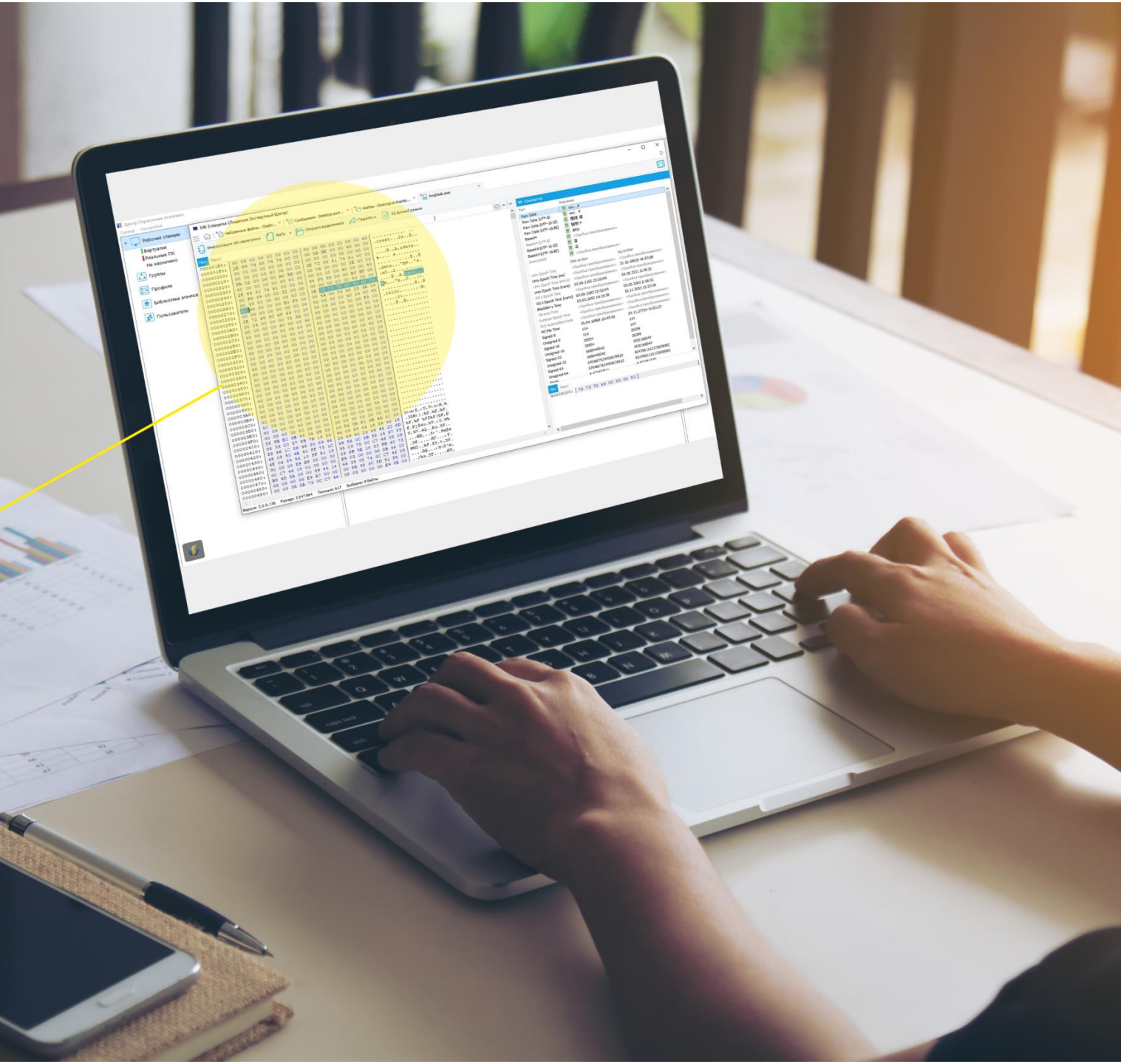
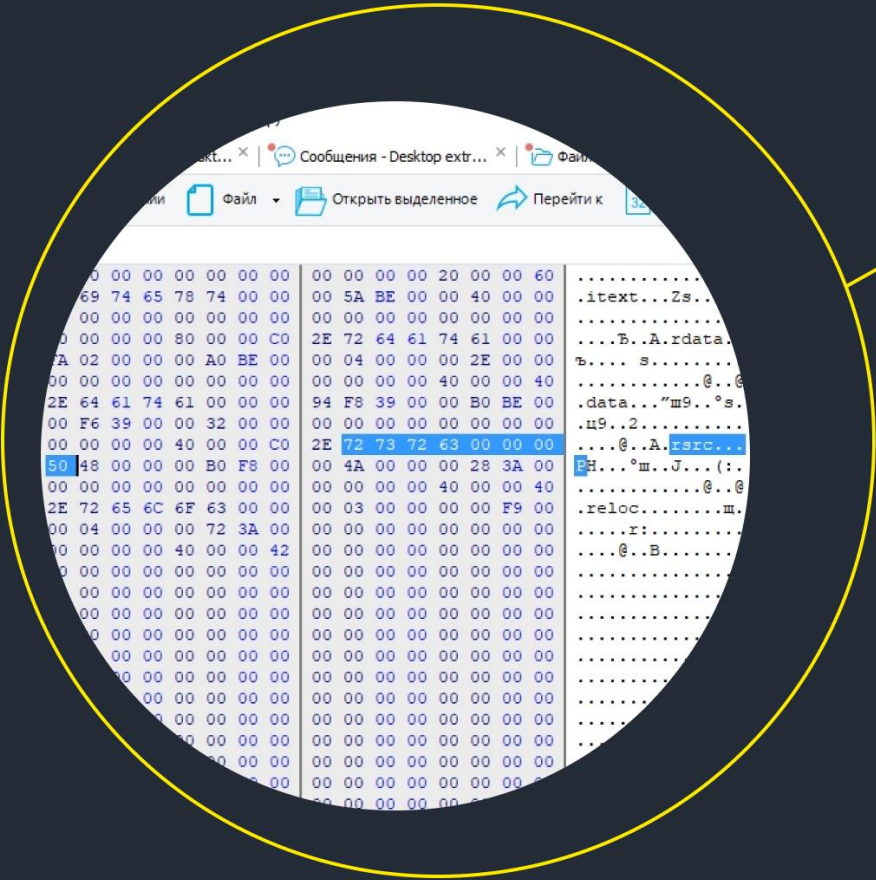
Редактор YARA

```
1 rule Rule_1
2 {
3   strings:
4     $my_hex_string = { 72 73 72 63 00 00 00 50 }
5
6   condition:
7     $my_hex_string
8 }
```



ПОИСК ПО СОДЕРЖИМОМУ

ПРАВИЛА YARA



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
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

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-CC...
Бедняков Валерий	bednyakov	bednyakov	Онлайн	Маркетинг	192.168.6.243	Active	D408-DC72-0A2A-06...
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	mariaрc	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

- 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

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 (OCR)
- Статистика

↑ Показать извлечения ↑

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							C72-E743-CC...
Бедняков Валерий							C72-0A2A-06...
Сервер SIEM							C72-34A4-FF...
Сервер DC							C72-F1EF-F4...
Мария Петрова							C72-6B3F-F4...
Копылова Анна							C72-B612-F4...
Ермакович Вадим							C72-60B1-2A...

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

<input checked="" type="checkbox"/>	Имя профиля	Создан	Изменен	Описание
<input checked="" type="checkbox"/>	Полный Аудит Системы	2022/09/13 10:34:46		
<input type="checkbox"/>	Аудит События	2022/09/13 10:31:49		
<input type="checkbox"/>	Поиск малвари 18b964	2022/09/12 19:37:44	2022/09/12...	
<input type="checkbox"/>	Аудит подозрительной ...	2022/09/12 18:41:08		

Экспорт результатов извлечения в МКЕ

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)	

Полное исследование / Игорь Петров

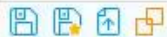


Часовой пояс: (UTC+03:00) Москва (Европа)

ОС: Windows 10.0.19044

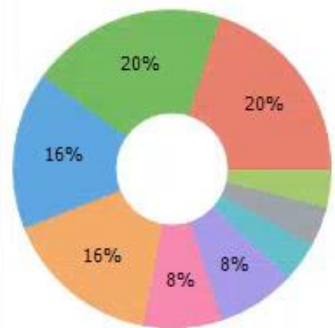
Номер инцидента: [Добавить номер инцидента](#)

Номер вещдока: [Добавить номер вещдока](#)



Статистика Извлечение Владелец Общая информация Устройство Фото Заметка

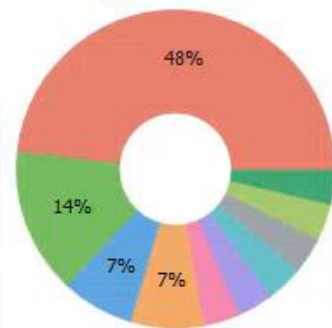
Топ 10 контактов



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](#)

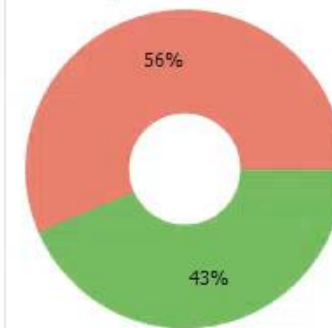
Топ 10 групп



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 5

Hardware 500

Информация об ОС 11 338

Autorun 507

Журнал событий 54 078

NTFS 667 880/156 600

Источники	Тип	Время (Москва)	Детали
<input checked="" type="checkbox"/> <ul style="list-style-type: none"> Autorun 	<input checked="" type="checkbox"/> <ul style="list-style-type: none"> 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
<input checked="" type="checkbox"/> <ul style="list-style-type: none"> Без тега 	<input checked="" type="checkbox"/> <ul style="list-style-type: none"> Связь между триггером и подп... 	09/05/2022 10:5...	Триггер: SignalUpdate Подписчик: SignalUpdate
<input checked="" type="checkbox"/> <ul style="list-style-type: none"> Без тега 	<input checked="" type="checkbox"/> <ul style="list-style-type: none"> Триггер события 	09/05/2022 10:5...	Название триггера: SignalUpdate Запрос: SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedData_PerFOS_System'

Источник Autorun
Тип Подписчик события
Имя SignalUpdate
подписчика
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 COMMANDLINECONS...
триггера
Триггеры SignalUpdate
Приоритет Normal
Создатель petrov

- 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

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-FFFFFFFFFFFFFF}' 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	

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: SFN MACB, \$SI ...B

Путь к файлу: Users\petrov\AppData\Roaming\Signal\SignalUpdate.exe

Дубликаты

Дубликатов не обнаружено



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](#)



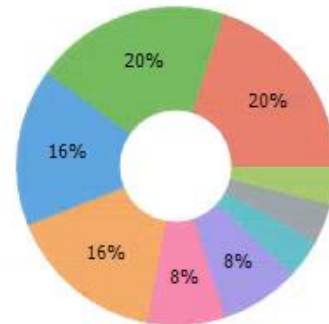
Статистика [Извлечение](#) [Владелец](#) [Общая информация](#) [Устройство](#) [Фото](#) [Заметка](#)

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](#)

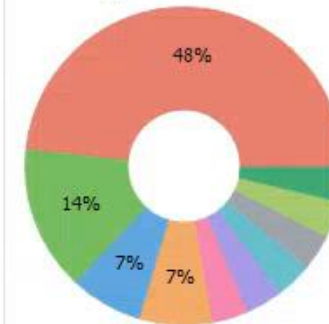
Топ 10 контактов



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
500



Информация об ОС
11 378



Autorun
507



Журнал событий
54 078



NTFS
667 880 / 156 600

```
Field1
zonedTimeFromTimeImp1
zonedTimeFromAdjTimeImp1
name
bCryptGenRandom
queryProcessCycleTime
queryUnbiasedInterruptTime
queryIdleProcessorCycleTime
coresCount
hIntel
ValueError
base64.nim
decode
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
@) at location
@` (ord
@Invalid base64 format character `
7456789; <=
! "$%&'()*+,-./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:
@[!] fdLED0gpCumVBVeGRrtSINPD FAILED to resume thread:
@[*] fdLED0gpCumVBVeGRrtSINPD resumed thread successfully.
@[!] gYu0iGRPCKWTubonbibfqXsQ FAILED to add routine to APC queue:
@[*] gYu0iGRPCKWTubonbibfqXsQ 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 successfully.
@[*] Started process with PID:
@calc
@bcmode.nim(503, 9) `len(input) <= len(output)`
@GsIUCZ2QrF2ad+yWakIpwg==
@JEpsjbbnvsedRXLaaqFxQxLQpHbngKTV
@n+XQi38M7lshABSTjGeu5QaU7Jvq4vqiHP9AP/yPhwKa8nb8BTHEptcVhWbF8iWft2I9zn1PEdYycX6U7Mza3IxeJ6ymNpZdmuUHshmfplbc485tyKgQzjrtl+S6LoIzeIAzHA56AKS1nPhUyJkSZ6eMFD8WssI5bdntp2mRmT5qLo0bWw4CPKwJCAFAAUzLkFvYmjg92Ef
StZBG/nwVpeAiAP4shMkuUHlNcX5e9ZlH5mXrK3q1+9G/DavbqeA6EXNFJgw7FhIEBQtOxdG302aaXaZyP2nE6nHpxXxyVduUbQBT401eL7c9JyKYPBaG8qdZyOHEXRlwqNRg+/+6fwlKnEeQefKoQ912VsbI60lH6rmkc9PCa9hiNOLitgPAVRNM948nQOXzrPQyZsIOIr
IjzzbRCaf1YJwxaorQTzoc7Bbw6n9NlOLGGuizn4styqgIeKtqpl3DM5jSNRM5wYrNw50kNIHhTOR9qWBF65Jj1REM1CZZEDrBn4nvVaNL7xx1vb2vNYLEBAu37UM9tB/T05yB5jLgqA+Jn2Kz0VwZX8EYbUrEuw+GKktD50cIs5s4TiPo558n4ik1sAwR8Jc1iu4lVH3Kv
u1Ah0mUGAKNlWtnYgnBqbVfhVazHnCF4w7HJ+nqiKPDq51BDcLhe6K5wvnaUslj0GVPVfVDYVFKTAqna/m0d8opzoo+dGcwmdn8rF6wdRf8t0ek0y2c+un5r6YdFNoductS7ztft70k/XMIjQ1ehPE6MrDqQKuTopT9ubVaCvZEHV27ZY/bksix7t3+2M4PqXC0gZ650C3VU
+RZ+P4YY4g/8Se7BCgNFev2ezJTqybAzh0TnlMQ05f3wrT5/NfknfCdr8Yyby0jMqrI20aNabG1v51Q10Crnw07xBYwG4DRl+GIk3K3yKGTMap9JeuFcbiR0h71K42i9j/Cyf5N1yaDagk/cKua0P0eWh4886M0aZuw65xYusQSYOLcgq6JM15RKF8WIFBssw+QP6NY4qyM
zHsp8fN4J3s0VcfEwBOHIDnr0nz6nmfSmJrod1mH9pIcFv0nYt3C6qXjMdte8mHYBPB4jrYttfppE4MICuyIhLaAC9A3Tn87ZKxcyQPMiobUgBC4azf1+Yvhp5+7xnGCUuUn7jdd1T4zmzeP3XBSQPtb1Y3xAp0s2jXkvnJQLfx5w7mrtE0tZ09vak5VPwNaKgn06KRjI
Pt2LwrDLpj88TVTbCmcVH0oHTqBmYN3TH365oWviVd7DpsELX07a1/Lr7KVElIwvLk1hdvDC7vuT6oPa4J7BaBe18k3LdXumoXoQMfN7CjTT27mJt4HXKgP1FXLCUme5EArmhU9bw7rFoBm5yJz+3a8w0guCmzd9Eurq/63nQYTVQgnP/V/AwVFA4iib0sd1bQ/3d01bimh/
3IOYubzj0/+yTdeIMQBB5uEht5SA3XrAWMdiTJFX1keCLubNAQ5fLLFAEZ1BgP9as460aujozt0Ef60Vgl4aHr/8tLkUir2sFe2beQALwerN1ehXJGYIxvt5DNk+oPTX7bPCJuc8NgIaQ8vzkR6+9nBeNfP9Zdet3Bqhd8dn7TKeLgxf5It6YgkvgvtG03ZfhpUIiA5k1456
aoxZMCQWY86gTfrXUME/v+T5yL/VXf1Y3bQzVKSRCamZkcvb8XWbB5Zzr74FUCeaJyKL5bn3V5r839Vb866xGzjWHFzIDbXLcwniEbNaxvAAZby/eopDvN2Vf/Pg8/mBe02i25W8/udiMuLj3DyKw8Mxwc+qRQNOUtvU2W4VqPk16rD39nbX0tYBNfg+prJjvWnDt4DKLY0
9EZS4jaZ6Tj00Zk84zw+ljtyFvrSkQ/NWC36XTWq17+Zhh6pL/MWBQj7dDjC9yXoC7FKQjQ2RjBzCwoQZF1Bwkd+BjVr/ukUqkxYfBw+jLuM25Byjcht/GPi3y20UsaMSeiC7GxTmlahJ881nfCt9RacIASweXyivYm0/kjoZGG2cqTwtFTX7RYlAN84mLeiDxZutCj+Myi
CuM/obi1fC3Xob1bFrbA7ePa5N+/EGxKNzVgniUGxQTxDJUVsLo4q5w71G7u085g2uFkyEXrMuxZk44T2j8f1sDlEhdI7jLECR00XWY2gd1Q1EMie6MPTd5swqyB0vQ3Ak0oKpFkg/U8o3zHeM8H6ZCD03Zw+Gr4txuOqhmmw/Agj6uRY9djZdFPo/0NpScznX9KENm/c1
Kt6NqhcS/iKU44MW5tcQ0kM0jZNdMbFUah/H2uk+fb0DhqWYBb0Uaysx2UI1eu85mf4eBM03NHJrSIEzKmUU06wIr4gUbrVTgWVbDhlm7zrCV845cfNH0odvMe2i5dULMn7sCw0Mk/wa63u5y9dDG4NOZuBviV/OceIa+nDdAoNb7a8sgPnQQQRFtd8Z+RQ3EhvIsbd+2cC
WP/rmHEYTbXb4A/NFYahwSiLaep8QI9G8DUQ9ISpWqJr7GPm+FzdgP8m0Imx6kGsPrF6S10ps/CyqAdmIOJUwZ099+asDezqGnmJj3sDhYOvNNbrCmCI0y3upL0jN8Hbp0gQ/fa6QCA2cSzjA5kEmkbQvjqIADgJjftB7lTmrT5wdekMhVwvA9Bsj/Qj1EUxpLquFDJbj6rBn
pLl9wvy6RPLRiBBKfRwLcbpVb43tU09067FsZ12dbeF4fsCzafydJHjqpJnvwtpWyg9NBbGdsbPmehukP8QCoAwKKNRmCIzIcUDK+BXwUTzhDeNuqzYUAdcvyky6wJMXD0e/r3kGwiXaB5b15y1L2w1X4EwodlIQxbnctv1xajqWv5JEYiA/NMFUU2ps7DNeY5KGmxTk8Iug
DCPGcHePrBeKd+KYp1sWkUzmv/WgYghU8lIqQ47Mg09B/kkjGdwf84WNUcmfK04l0bobVbx1tdV8v51tkFUNvVHKPOJ9NerKWGLaooFA2I+ZufSdxZDN2VRAjmtTDFwweA6YXL920ZSMhusWF5d/RCNxG/4tgemTBMFhwciKemo3wf4NJGOWDNAkwmPKWLCu1MvYzB8T49C9
T1esPgdPdI6tZ8807cYkaiJ9Wa7yepyZBMTfP66usT5/xIcws1tV1B1x9kGNpMf3egH26ea5iPN+SwcVDS70kFHEZq7tGPaTko56g14t6r0bDYKkV2j1PUuQGHjd4c4+U6jQAeZwv2PdtS1lBUvd04Rvk9ncfJv91j1JMi5b8zfpDgyj40iUHmZ7Z9gIcyY20REpTqo+20
oC45988FDE45UB1zMuSotWvqNbAwHsLQGHvrdvUis1BVYA+8Ww+EAERfaG2/a+vEt7uEL80UJGHxM1T/I4o8VtVNC/TfHoiWzIu2utxL4vf3kFwdeKGF80rZ04icDp8ZKxYmhZLV9MNvwhGZhbKkTUKB1vwyJ6aH+G9N94xaf11Z2mTcluiT7DxEmiOhNMvSJ81+Rau14ucp
```

- ▼ 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

[+ 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

[↓ Скачать извлечение](#)
[↗ Export extraction to Oxygen](#)
[🗑 Сбросить фильтры](#)

Нет данных для отображения

Нет данных

- ▼ 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

Нет данных

Задачи

Найти...

⌚ Отменить задачу ⬇ Скачать извлечение ↗ Export extraction to Oxygen 🗑 Сбросить фильтры

Нет данных для отображения

- 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	Завершено
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...

- ▼ 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

Отменить задачу Сбросить фильтры

Найти...

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

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

Найти...

ID задачи	Название рабочей станции	Имя хоста	IP адрес	Имя профиля	Файлы	Статус задачи	Начало	Завершение
12	Мария Петрова	mariarc	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	annarc	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

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...

<input type="checkbox"/>		Правила поиска	YARA правила	Файл	Полный путь	Размер файла	Время создания (Москва)	Время пос
<input checked="" type="checkbox"/>		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



<input checked="" type="checkbox"/>		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
-------------------------------------	--	-----------	------------------	------------------	---	--------	-----------------------------	-----------



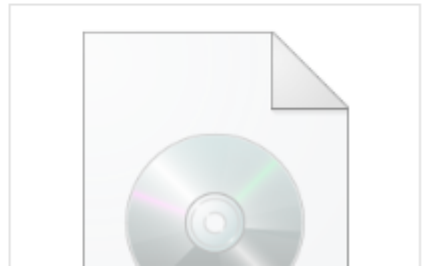
[Важное](#) [Добав...](#) [Добавит...](#)

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

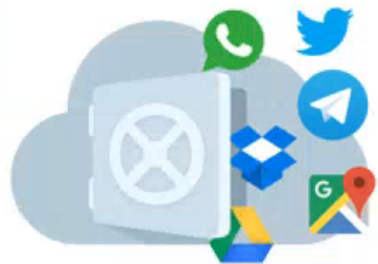
Размер файла 524 Кб
Время создания (Москва) 2022/07/13 09:22:56 (UTC+3)
Время последнего изменения (Москва) 2022/07/13 09:22:56 (UTC+3)
Время последнего доступа (Москва) 2022/07/13 09:24:19 (UTC+3)



Фильтры

Тип

- Токен
- Учетная запись



Мобильный Криминалист Облачные Сервисы

 Сервис Telegram Добавить сервис...

Учетные данные

Токен доступа: TGT:eyJkZXNjcmVudGlvbiI6IiRlYVZmcmFtdEpTT04...

Статус



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

Назад

Проверить

Отмена

>> Детали

[★ Важное](#) [Доба...](#) [Добав...](#)

Исходный раздел Telegram (desktop)

Исходный файл main.db3

Служба Telegram Desktop

Учетная запись 974758870

Токен

TGT:eyJkZXNjcmVudGlv...

Источник Telegram (desktop)



Мобильный Криминалист Облачные Сервисы

Извлечение завершено!

Данные успешно извлечены из облака

Id извлечения: 99A1AB45DF9F4E718EE40205E146F8D5

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



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

Далее

Отмена



Карты памяти/MTP извлечения



Импорт резервных копий

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

