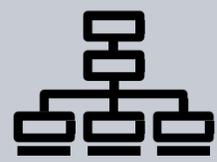




RT
Protect EDR

Endpoint Detection and Response





Расширение разнообразия используемых для написания ВПО языков программирования и технологий, усложнение архитектуры



Все более сложные социотехнические атаки, что требует повышения осведомленности об информационной безопасности обычным работникам



Рост активности группировок связанных с одной из сторон конфликта



Эксплуатация уязвимостей:

Microsoft Exchange (ProxyNotShell - CVE-2022-41040)

Apache Tomcat (Log4Shell - CVE-2021-44228)

Microsoft Outlook Elevation of Privilege (CVE-2023-23397)

Vmware Spring Framework (Spring4Shell - CVE-2022-22965)

Самые популярные уязвимости:

CVE-2022-27228 (Bitrix vote module RCE)

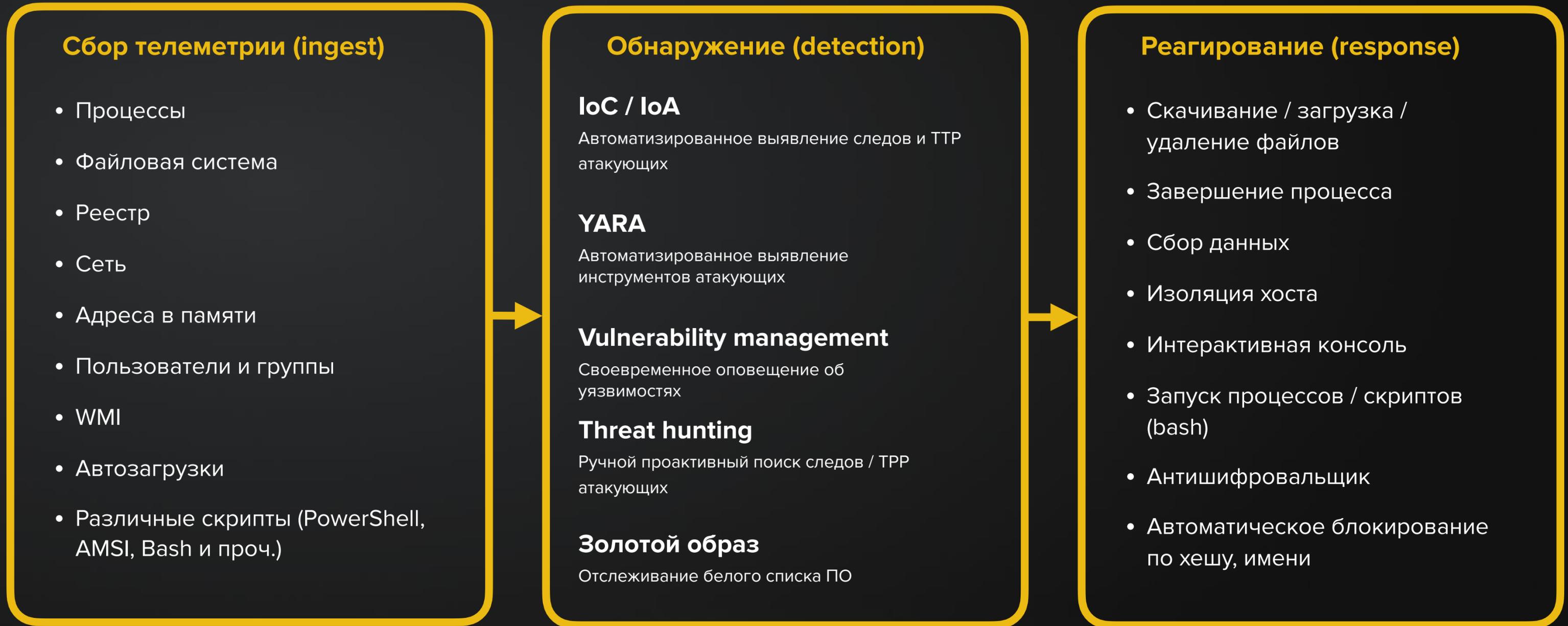
CVE-2021-34473 (MS Exchange RCE ProxyShell)

CVE-2022-41040+CVE-2022-41082 (MS Exchange RCE ProxyNotShell)



Как следствие, повышение требований к защите конечных точек

Классические задачи EDR



Как решать такие классические задачи EDR



Сбор «сырых» низкоуровневых событий с расширенной моделью данных



Профили сбора событий и реагирования на инциденты



Сбор классических журналов (ETW)



Расширение возможностей модулей Anti-Ransomware, Deception, VM

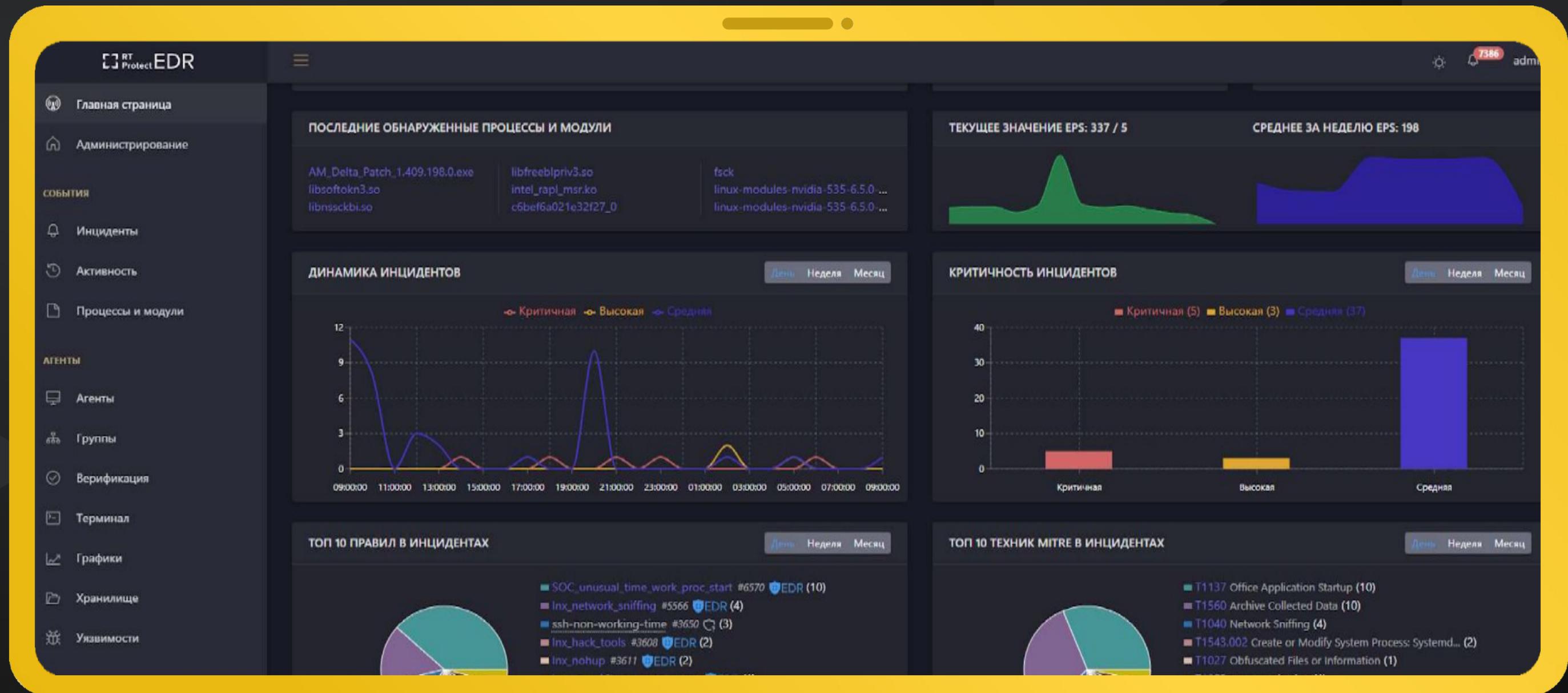


Синхронная обработка индикаторов атак/компрометации на агентах



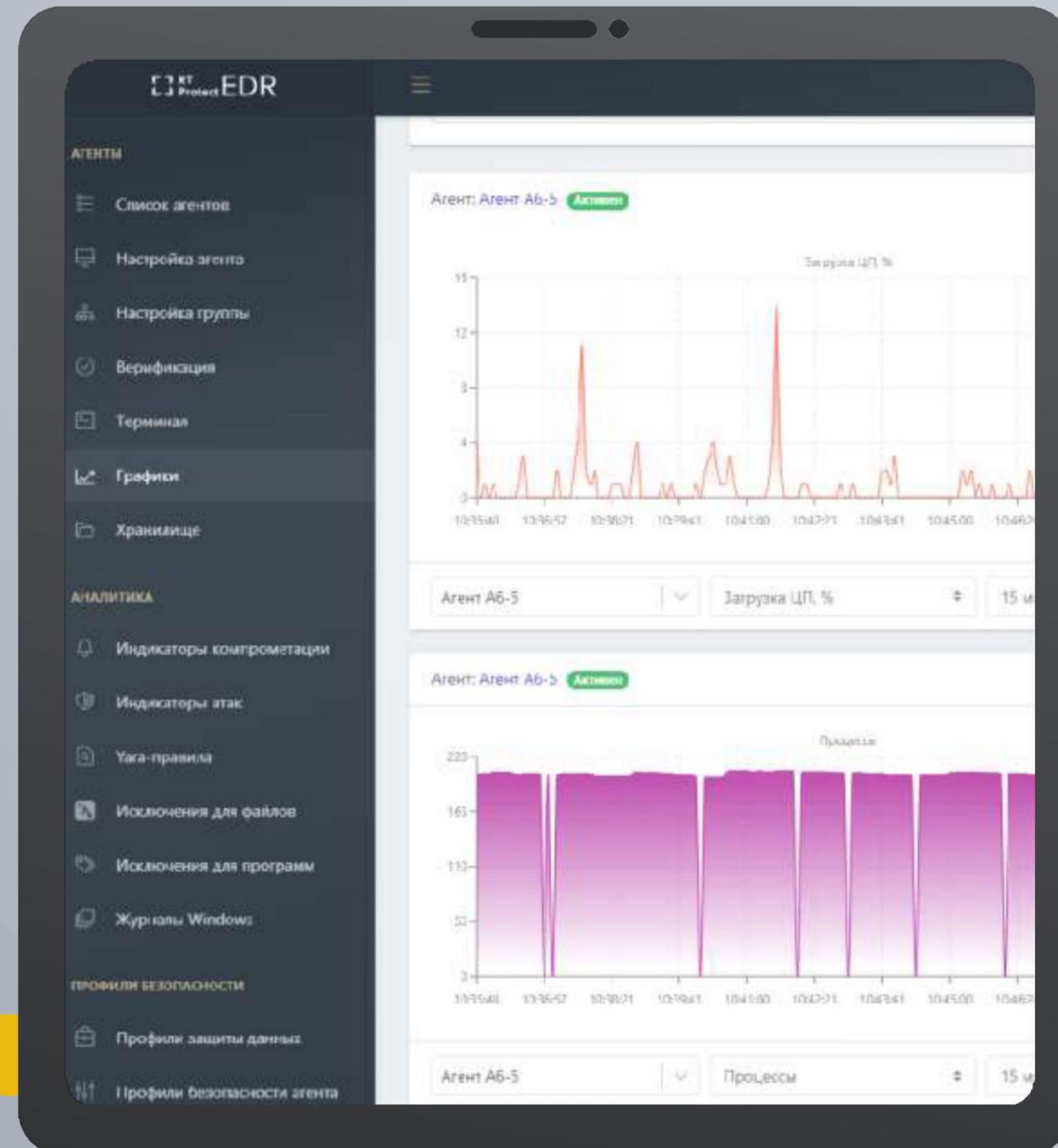
Расширение аналитического обогащения

RT Protect EDR — система обнаружения целенаправленных атак и сложных угроз. Решает все классические задачи и имеет дополнительные модули.



RT Protect EDR

Обеспечивает своевременное обнаружение вторжений, эффективное автоматическое противодействие, наглядную визуализацию событий и инцидентов, сбор цифровых улик и тщательное расследование.

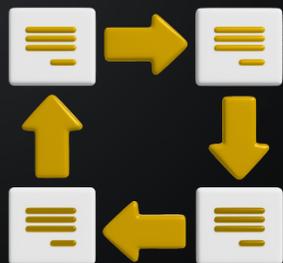


Имеет модуль защиты от вирусов-вымогателей

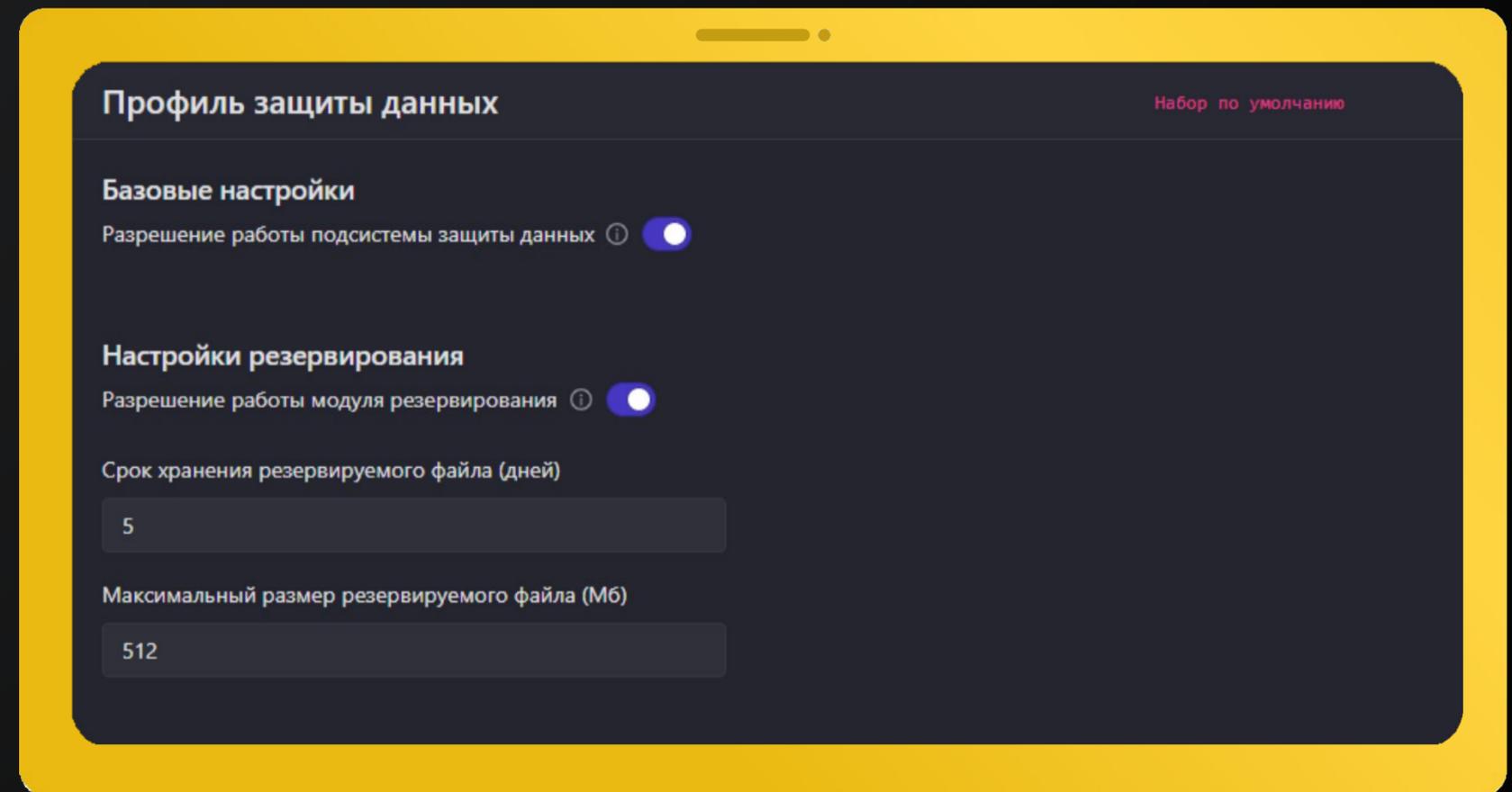
Отдельный модуль на базе эвристического анализа поведения программ:



Реализует защиту от шифровальщиков как класса, а не его отдельных представителей



Осуществляет прозрачное резервирование пользовательских файлов



Защита от вирусов-вымогателей



Восстанавливает резервируемые файлы в случае утраты



Поддерживает все типы файлов и предоставляет возможность гибкой настройки резервирования

Список защищаемых каталогов

Путь до защищаемого каталога ⓘ

\Device\HardDiskVolume*\Users*\Desktop

\Device\HardDiskVolume*\Users*\Documents

\Device\HardDiskVolume*\Users*\Pictures

\Device\HardDiskVolume*\Users*\Source

Типы файлов для резервирования ⓘ

Архивы x Аудио x Видео x Документы x Изображения x

Исполняемые модули x Исходные коды x Остальные x Презентации x

Скрипты x Текстовые файлы x Файлы-контейнеры x

Электронные таблицы x

Архивы x Аудио x Видео x Документы x Изображения x

Исполняемые модули x Исходные коды x Презентации x Скрипты x

Текстовые файлы x Файлы-контейнеры x Электронные таблицы x

Изображения x

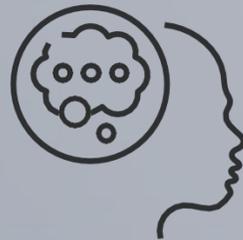
Исходные коды x

Анализ запускаемых файлов и загружаемых модулей

Анализ всех исполняемых модулей перед загрузкой



Сигнатурный
анализ



Эвристика



Легковесная модель
машинного обучения

<input type="checkbox"/>	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	
> <input type="checkbox"/>	31.08.2022, 10:58:36	31.08.2022, 10:58:34	● Агент IBR0044	Процес \Device
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес Files\C
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес \Device
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес \Device
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес -s sam нить=8
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес
> <input type="checkbox"/>	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процес \Device

Работа с индикаторами компрометации

- ▶ Многообразие типов индикаторов компрометации
- ▶ Удобная система управления индикаторами компрометации и их наборами

Индикаторы компрометации

Показывать по: 50

« < 1 > »

Выбрано: 0 из 1

Найдено: 1, показано: с 1 по 1

<input type="checkbox"/>	Имя индикатора	Тип артефакта	Артефакт	Действие	Комментарий	Дата создания / Автор	Последнее изменение / Пользователь	Управление
<input type="checkbox"/>	NotPetya	SHA-1	40132ae21a76d7c142b3ce571e97e86eccc1d01c	Бложировать	Ransomware	30.08.2022, 10:49:40 Аналитик L1	30.08.2022, 12:52:40 Аналитик L2	  

Индикаторы компрометации

Предназначены для выявления известных атак по следующим артефактам:

хеш файла
имя файла
IP-адрес
доменное имя
сетевая сигнатура

Редактировать индикатор

Имя индикатора *

NotPetya

Тип артефакта *

SHA-1

Не выбран

Файл

SHA-256

SHA-1

MD5

IP-адрес

Доменное имя

Сетевая сигнатура

Детектировать

Комментарий

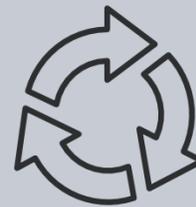
Ransomware

Индикаторы атак

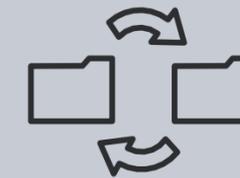
Работающие в режиме реального времени



Классификация по матрице MITRE ATTACK



Регулярное обновление TI



Конвертер Sigma правил



Удобная система управления индикаторами атак и их наборами



Собственные правила выявления угроз с интуитивно понятным механизмом написания IOA

Индикаторы атак

Показывать по: 50

Выбрано: 0 из 39

Найдено: 39, показано: 2

<input type="checkbox"/>	Имя	Тип	Критичность / Действие	MITRE	Дата создания / Автор	Последнее изменение / Пользователь	Управ	
<input type="checkbox"/>	fake_svchost	Процессы	Старт процесса	Высокая	T1036	29.08.2022, 14:16:59 Аналитик TI	29.08.2022, 14:16:59 Аналитик TI	<input type="checkbox"/>
<input type="checkbox"/>	win_mmc20_lateral_movement	Процессы	Старт процесса	Высокая	T1021003	29.08.2022, 14:16:59 Аналитик TI	29.08.2022, 14:16:59 Аналитик TI	<input type="checkbox"/>

Индикаторы атак

Возможность писать правила обнаружения атак на основе событий:

- ▶ Создания процесса
- ▶ Загрузки исполняемого модуля
- ▶ Создания/модификации файла
- ▶ DNS-запроса
- ▶ Сетевого соединения (CONNECT)
- ▶ Открытия поста для входящих соединений (LISTEN)

Редактировать индикатор

Имя индикатора *

win_outlook_shell

Критичность

Высокая

MITRE

T1204\002

Комментарий

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_outlook_shell.yml
<https://www.elastic.co/guide/en/security/current/suspicious-ms-office-child->

Условие

ParentImage iendswith "\\OUTLOOK.EXE" and
(exclф.Cmd or
exclф.PowerShell or
exclф.ScriptEngine or
exclф.Wmic or exclф.Vssadmin or exclф.Wbadmin or exclф.BcdEdit or exclф.DiskShadow or e
exclф.Mshta or exclф.MsiExec or exclф.TaskScheduler or exclф.Regsvr32 or exclф.Verclsid or

Тип индикатора

Процессы: Старт проце
Сеть: Исходящее подкл
Сеть: Входящее подкл
Сеть: SSL HELLO
Сеть: Открытие локаль
Сеть: DNS-ответ
Файлы: Создан новый о
Файлы: Файл переимен
Файлы: Удален файл
Файлы: Доступ к файлу
Реестр: В значение ключ
Журналы: Событие жур
Процессы: Загрузка дра
Процессы: Старт проце
Процессы: Загрузка обр
Процессы: Загрузка обр

Режим ▾

Обычный

Threat Hunting



Гибкий поиск угроз по событиям EDR



Аналитика по поведенческим признакам

Время регистрации события (UTC)	29.08.2022, 18:47:05
Тип события	Файлы
Подтип события	Удален файл
Критичность (уровень важности) события	Информация
Агент	Агент IBR0038
Уникальный идентификатор агента	1d7e14463ec2fb8e10b931fa07e9ff517e
Полное имя исполняемого модуля процесса	\Device\HarddiskVolume3\Program Files (x86)\Kaspersky Lab\NetworkAgent\klnagent.exe
Идентификатор процесса на агентской системе	10760
Идентификатор родительского процесса на агентской системе	828
Уникальный идентификатор процесса	34da31ac-b79e-01d8-8200-000000000000
Командная строка процесса	"C:\Program Files (x86)\Kaspersky Lab\NetworkAgent\klnagent.exe"
Домен (рабочая группа) пользователя, запустившего процесс	NT AUTHORITY

Threat Hunting

Гибкий поиск угроз



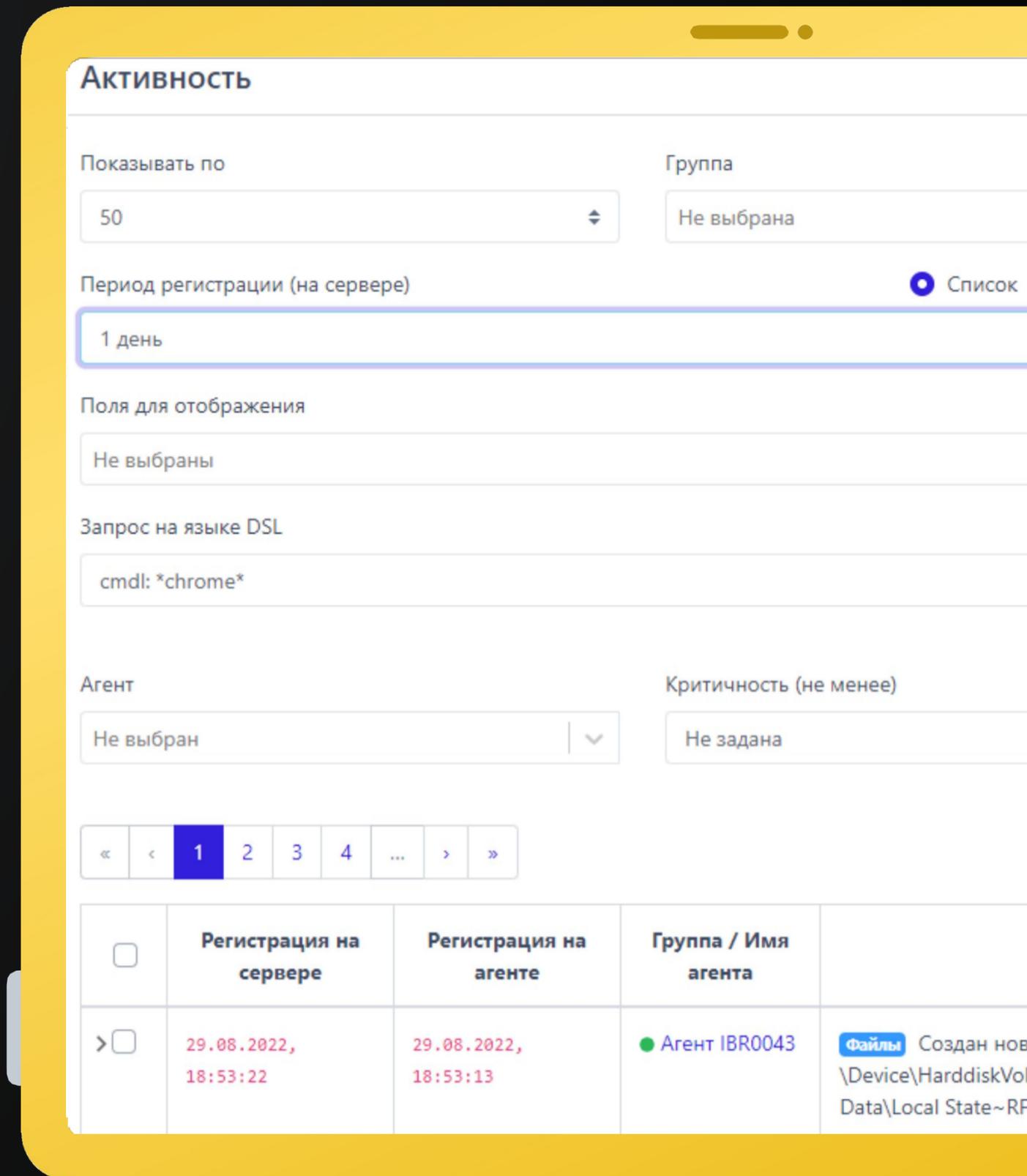
Быстрый и удобный поиск угроз в корпоративной сети по событиям EDR



Настраиваемая фильтрация событий по различным параметрам



Возможность использование языка DSL для продвинутой фильтрации



Активность

Показывать по: 50 | Группа: Не выбрана

Период регистрации (на сервере): 1 день | Список

Поля для отображения: Не выбраны

Запрос на языке DSL: cmdl: *chrome*

Агент: Не выбран | Критичность (не менее): Не задана

« < 1 2 3 4 ... > »

<input type="checkbox"/>	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	
> <input type="checkbox"/>	29.08.2022, 18:53:22	29.08.2022, 18:53:13	● Агент IBR0043	Файлы Создан нов \Device\HarddiskVol Data\Local State~RF

Threat Hunting

Процессы и модули



Распространенность по агентам инфраструктуры заказчика



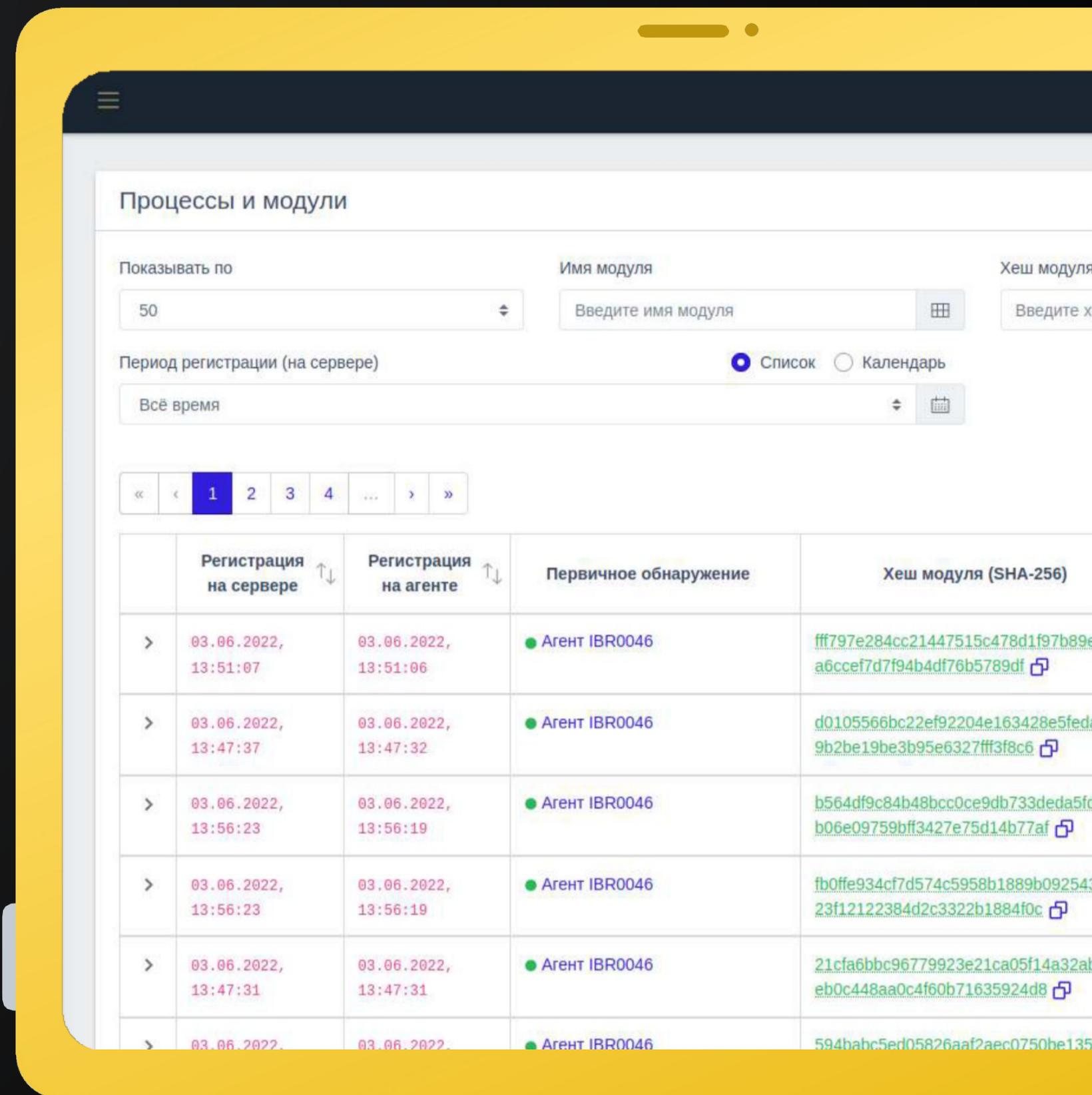
Удобный поиск по хешу (SHA256)



Отображение цифровой подписи



Первоисточник обнаружения



Процессы и модули

Показывать по: 50

Имя модуля: Введите имя модуля

Хеш модуля: Введите х

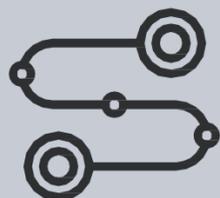
Период регистрации (на сервере): Список Календарь

Всё время

« < 1 2 3 4 ... > »

	Регистрация на сервере ↑↓	Регистрация на агенте ↑↓	Первичное обнаружение	Хеш модуля (SHA-256)
>	03.06.2022, 13:51:07	03.06.2022, 13:51:06	● Агент IBR0046	fff797e284cc21447515c478d1f97b89e a6cce17d7f94b4df76b5789df
>	03.06.2022, 13:47:37	03.06.2022, 13:47:32	● Агент IBR0046	d0105566bc22ef92204e163428e5fed 9b2be19be3b95e6327fff3f8c6
>	03.06.2022, 13:56:23	03.06.2022, 13:56:19	● Агент IBR0046	b564df9c84b48bcc0ce9db733deda5f b06e09759bff3427e75d14b77af
>	03.06.2022, 13:56:23	03.06.2022, 13:56:19	● Агент IBR0046	fb0ffe934cf7d574c5958b1889b09254 23f12122384d2c3322b1884f0c
>	03.06.2022, 13:47:31	03.06.2022, 13:47:31	● Агент IBR0046	21cfa6bbc96779923e21ca05f14a32a eb0c448aa0c4f60b71635924d8
>	03.06.2022,	03.06.2022,	● Агент IBR0046	594bahc5ed05826aaf2aec0750be135

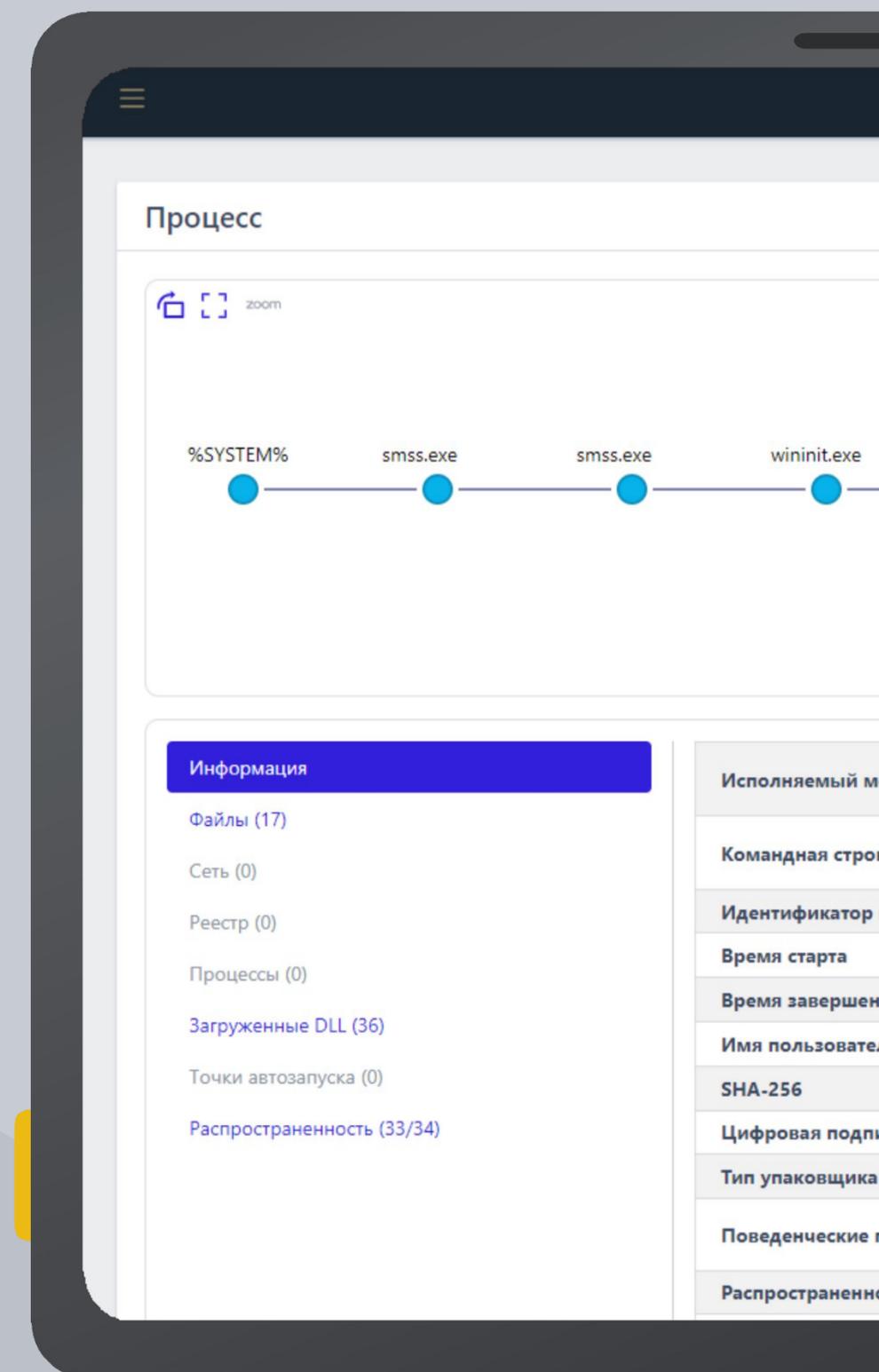
Богатый инструментарий расследования инцидентов



Удобное представление активности процессов в виде дерева со сводной информацией о ключевых событиях



Сведения о распространенности подозрительных исполняемых модулей в агентской сети



Сбор данных журналов



Взаимодействие с любыми провайдерами журналов Windows



Возможность сбора журналов со средств защиты информации заказчика



PT
Информационная
безопасность

Добавить журнал

Режим: Из справочника По GUID-у По имени

Провайдер *

Microsoft-Antimalware-Protection

Уровень

Ошибка

Ключевые слова (любые)

Не выбрано

0x0

Ключевые слова (все)

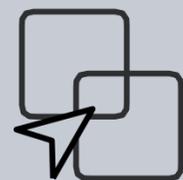
Не выбрано

0x0

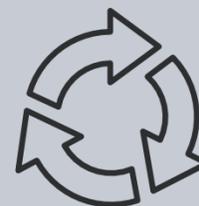
Дополнительные параметры

SID пользователя x ID терминальной сессии x

Сервер аналитики (TI portal)



Интеграция с популярными TI решениями



Регулярное обновление наборов индикаторов компрометации

Файл (SHA-256): `a2c76bae53e697729504d13aae2cd30d2aa1773e6620af366e466f3370553513` Вредоносный

Данные сервера аналитики

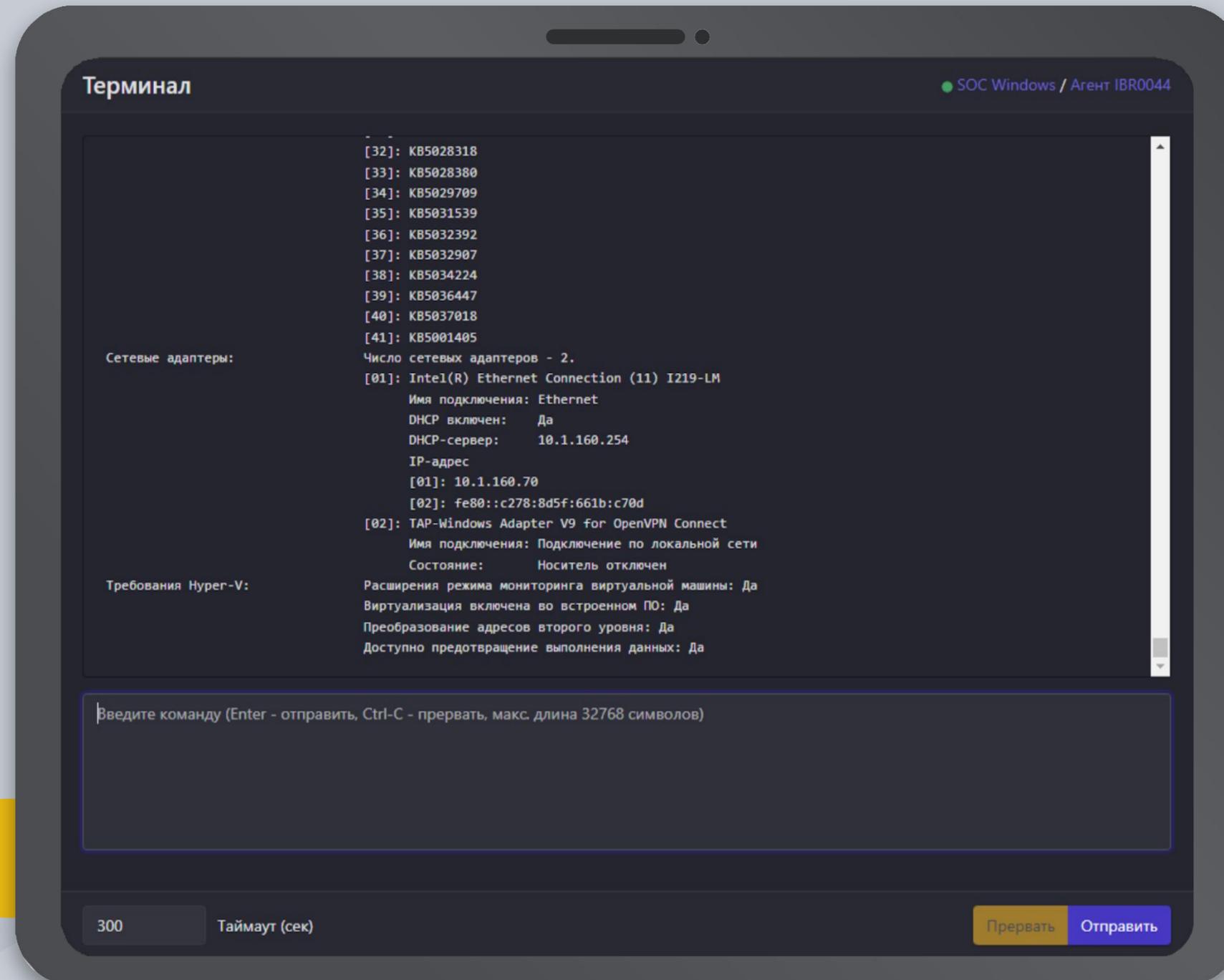
Вредоносный
ВЕРДИКТ

08.07.2022, 16:38:31
ВПЕРВЫЕ ОБНАРУЖЕН

Вердикт	Вредоносный (вердикт основан на отчете VirusTotal)
Впервые обнаружен	08.07.2022, 16:38:31
Размер файла	151.5 KB

[JSON](#)

Терминал удаленного доступа



Терминал SOC Windows / Агент IBR0044

```
[32]: KB5028318
[33]: KB5028380
[34]: KB5029709
[35]: KB5031539
[36]: KB5032392
[37]: KB5032907
[38]: KB5034224
[39]: KB5036447
[40]: KB5037018
[41]: KB5001405

Сетевые адаптеры: Число сетевых адаптеров - 2.
[01]: Intel(R) Ethernet Connection (11) I219-LM
    Имя подключения: Ethernet
    DHCP включен: Да
    DHCP-сервер: 10.1.160.254
    IP-адрес
    [01]: 10.1.160.70
    [02]: fe80::c278:8d5f:661b:c70d
[02]: TAP-Windows Adapter V9 for OpenVPN Connect
    Имя подключения: Подключение по локальной сети
    Состояние: Носитель отключен

Требования Нурег-V: Расширения режима мониторинга виртуальной машины: Да
Виртуализация включена во встроенном ПО: Да
Преобразование адресов второго уровня: Да
Доступно предотвращение выполнения данных: Да
```

Введите команду (Enter - отправить, Ctrl-C - прервать, макс. длина 32768 символов)

300 Таймаут (сек) Прервать Отправить

Профиль безопасности агента



Гибкая настройка сбора событий для отправки на сервер



Персонализированный подход конфигурирования агентов для разных типов профилей защиты



PT
Информационная
безопасность

Профиль безопасности агента

Оптимизация потока событий

- Исключать файловые события ранней стадии запуска процессов
- Исключать файловые события чтения файла desktop.ini
- Исключать файловые события префетчера
- Исключать файловые события процессов TiWorker и TrustedInstaller
- Исключать события чтения исполняемых файлов, связанные с их исполнением
- Исключать события чтения исполняемых файлов
- Исключать события чтения любых файлов
- Исключать файловые события процесса-создателя файла
- Исключать файловые события процесса Dfsrs
- Исключать файловые события процесса DismHost
- Исключать события межпроцессного взаимодействия процесса CSRSS
- Исключать событие доступа к рабочему столу
- Исключать события доступа к процессам и нитям
- Исключать события загрузки известных модулей
- Исключать события со статусом "Разрешено" (кроме ключевых)

Профиль безопасности агента



Удобная система распространения профилей безопасности агентов

Настройки безопасности монитора процессов

Реакция на запуск PowerShell-интерпретатора (powershell)

Детектировать

Реакция на подозрительное использование iCACLS (Icacls)

Детектировать

Реакция на любое использование PsExec (PsExec)

Блокировать

Реакция на отключение встроенной функции Windows по резервированию файлов (InhibitSystemRecovery)

Блокировать

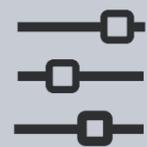
Реакция на запуск программ из альтернативных потоков NTFS (AltExeStream)

Блокировать

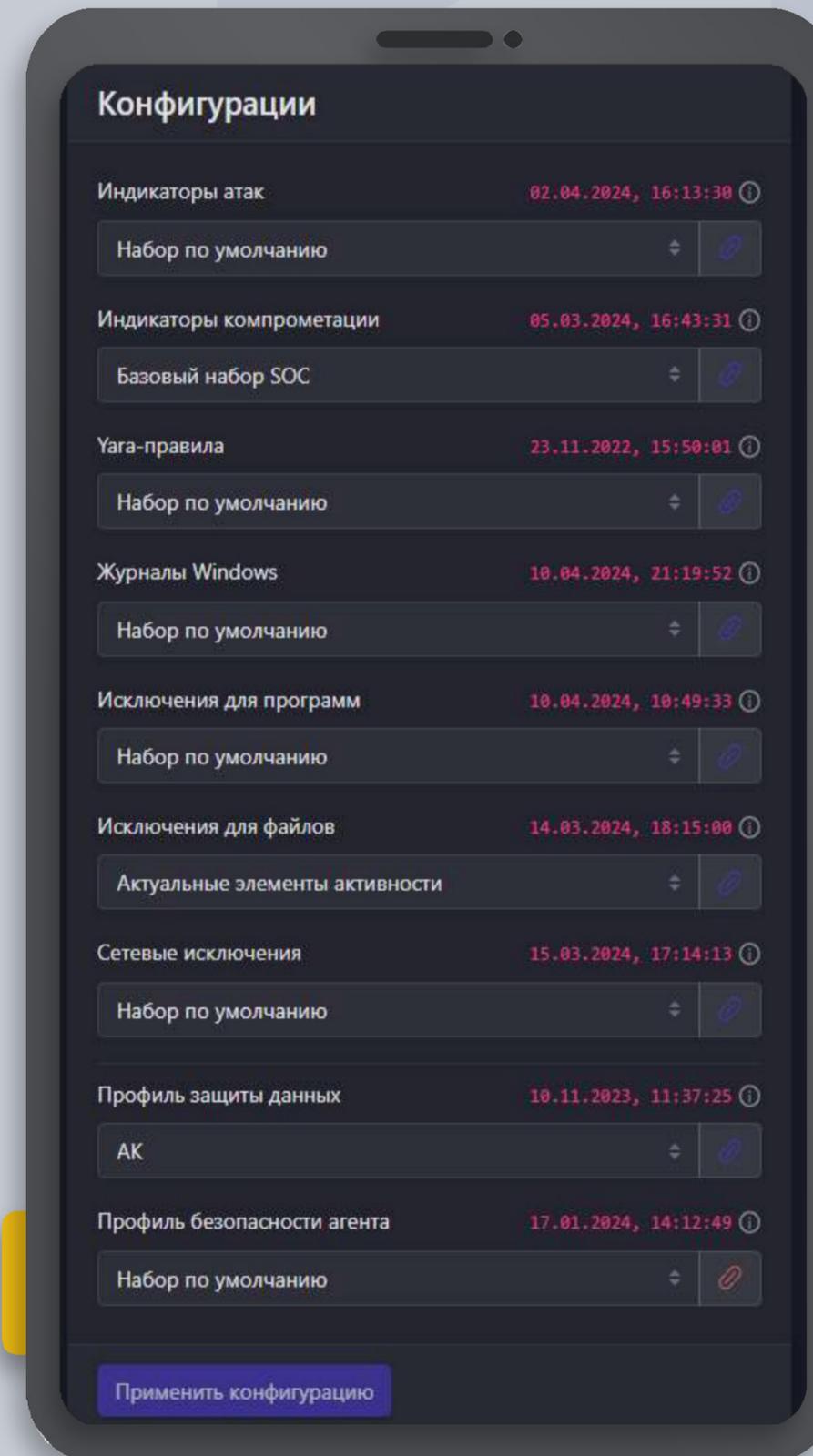


PT
Информационная
безопасность

Настройка профиля безопасности агента



Обилие тонких настроек позволяет создавать эффективные профили безопасности



Сервер аналитики (TI portal)



Консоль управления агентами реализует функционал PowerShell, что позволяет оперативно отреагировать на события конечной точки:

Детальное расследование инцидентов безопасности

Устранение последствий атак на корпоративную инфраструктуру

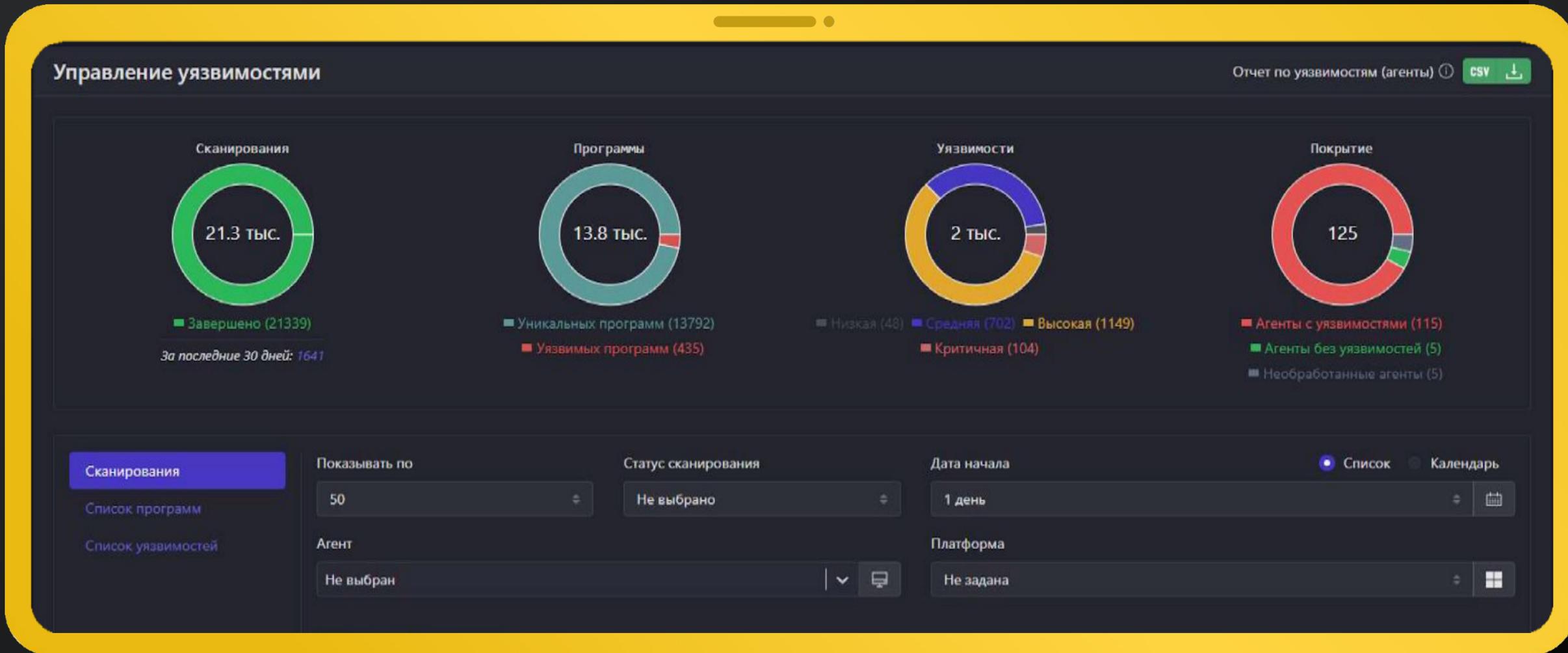
Сетевая изоляция хоста

The screenshot displays the 'Агент' (Agent) management interface. The left pane shows details for 'Агент IBR0044', including its name, last update (01.04.2024, 12:17:38), auto-update status (Включено), agent ID (b2be923615ab...), time zone (Europe/Moscow +0300), version (2.0.132.2632), platform (Windows), installation time (15.03.2024, 17:14:12), last verification (22.06.2022, 16:43:07), and last configuration update (10.04.2024, 21:19:52). It also shows a table of user login data for the last 5 entries.

Домен / Имя компьютера	Пользователь	Время
IBR0044	Администратор	12.04.2024, 08:47:34
IBR0044	-	20.03.2024, 18:45:43

The right pane, 'Управление' (Management), offers various actions: 'Изоляция' (Isolation) with a toggle for 'Не изолирован' (Not isolated) and 'Защита' (Protection) with a toggle for 'Защита включена' (Protection on). It also shows 'События' (Events) for the last 24 hours (62162) and 15 minutes (844), and 'Инциденты' (Incidents) with a total of 77. Other options include 'Терминал' (Terminal), 'Золотой ключик' (Golden Key), 'Защита от удаления' (Anti-removal protection), and 'Группа' (Group) set to 'SOC Windows'.

Модуль управления уязвимостями



Нам доверяют



НОВИКОМБАНК

Контакты

Адрес: 117587, г.

Москва, Варшавское шоссе, дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru



РТ

Информационная
безопасность

