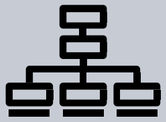
# RT Protect EDR

Endpoint Detection and Response

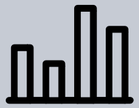
# Современные тенденции

PT
Информационная безопасность



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

## Сбор телеметрии (ingest)

- Процессы
- Файловая система
- Реестр
- Сеть
- Адреса в памяти
- Пользователи и группы
- WMI
- Автозагрузки
- Различные скрипты (PowerShell, AMSI, Bash и проч.)

## Обнаружение (detection)

**IoC / IoA**

Автоматизированное выявление следов и TTP атакующих

**YARA**

Автоматизированное выявление инструментов атакующих

**Vulnerability management**

Своевременное оповещение об уязвимостях

**Threat hunting**

Ручной проактивный поиск следов / TPP атакующих

**Золотой образ**

Отслеживание белого списка ПО

## Реагирование (response)

- Скачивание / загрузка / удаление файлов
- Завершение процесса
- Сбор данных
- Изоляция хоста
- Интерактивная консоль
- Запуск процессов / скриптов (bash)
- Антишифровальщик
- Автоматическое блокирование по хешу, имени

# Как решать такие классические задачи EDR

Сбор «сырых» низкоуровневых событий с расширенной моделью данных

Сбор классических журналов (ETW)

Синхронная обработка индикаторов атак/компрометации на агентах

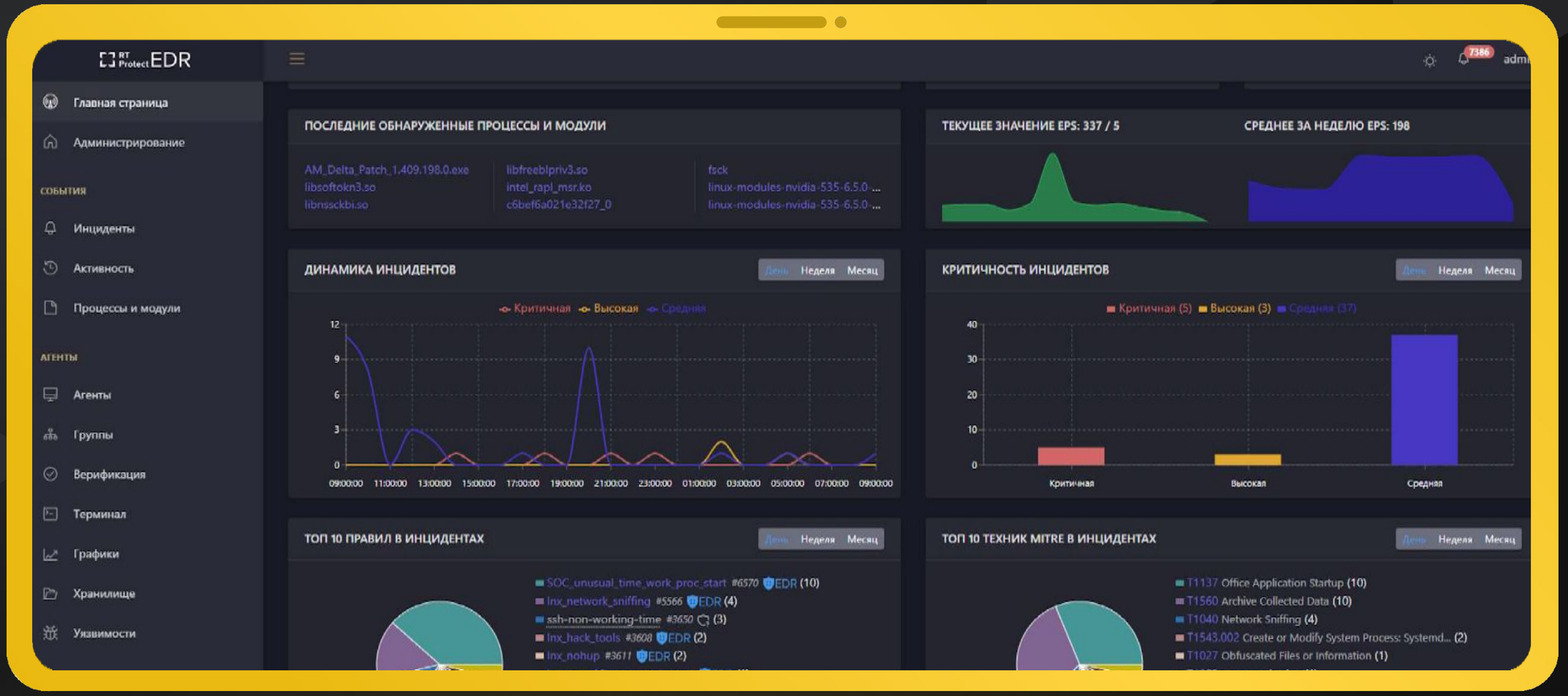
Профили сбора событий и реагирования на инциденты

Расширение возможностей модулей Anti-Ransomware, Deception, VM

Расширение аналитического обогащения

PT
Информационная безопасность

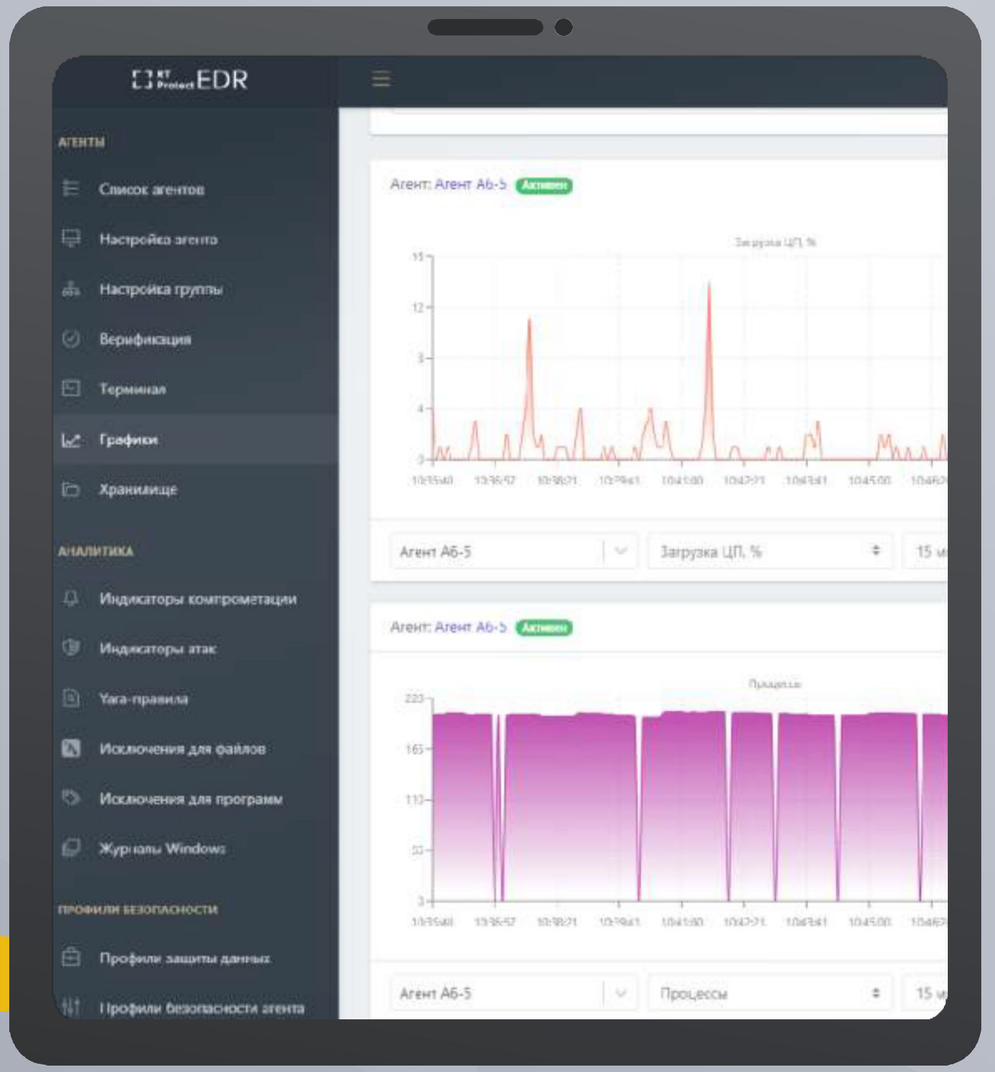
**RT Protect EDR** — система обнаружения целенаправленных атак и сложных угроз. Решает все классические задачи и имеет дополнительные модули.




PT
Информационная безопасность

# RT Protect EDR

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

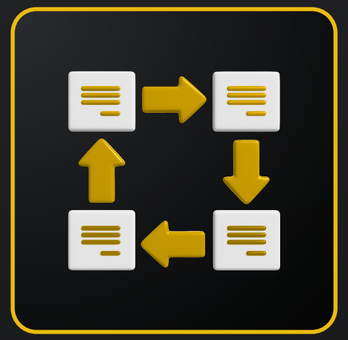



# Имеет модуль защиты от вирусов-вымогателей

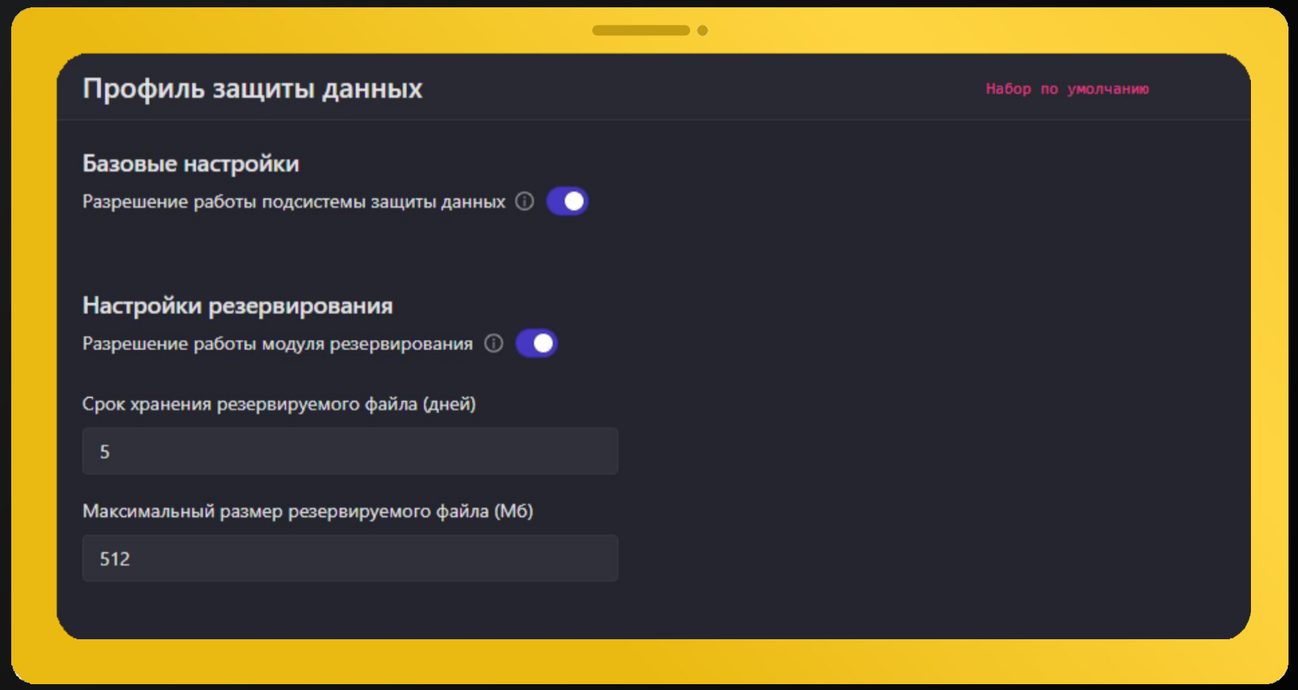
PT
Информационная безопасность

## Отдельный модуль на базе эвристического анализа поведения программ:

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



Осуществляет прозрачное резервирование пользовательских файлов

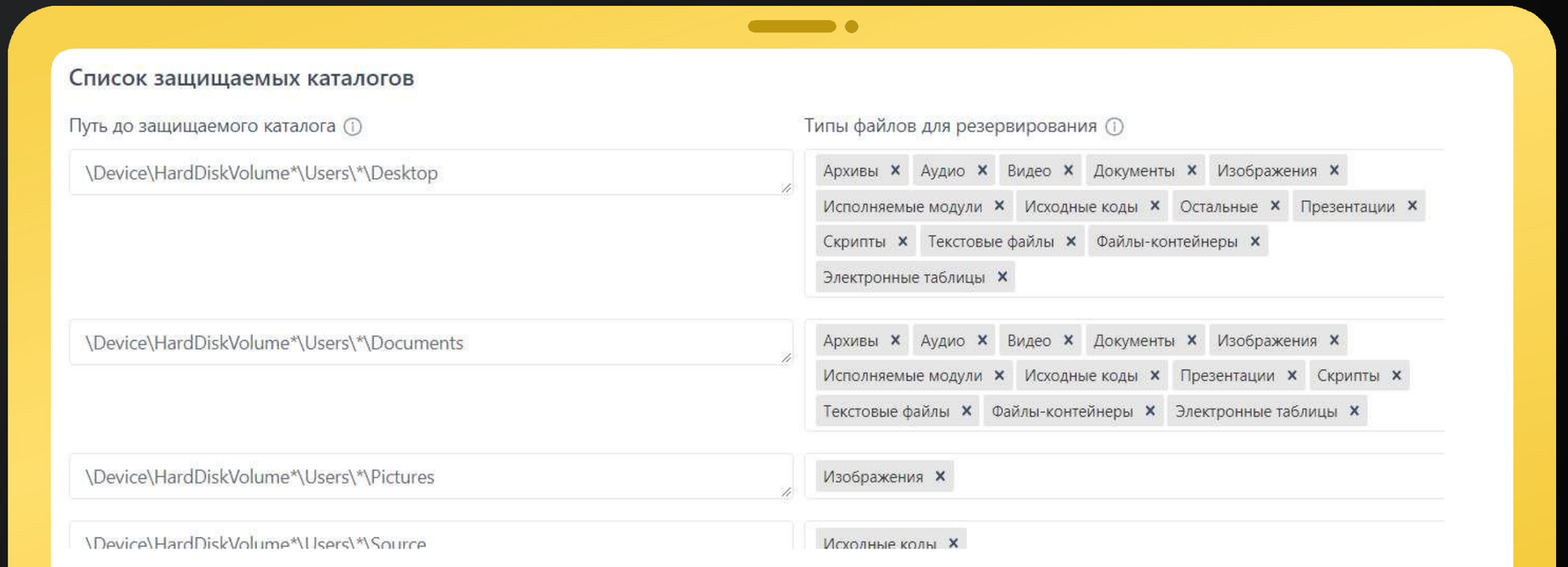


# Защита от вирусов-вымогателей

PT
Информационная безопасность

Восстанавливает резервируемые файлы в случае утраты

Поддерживает все типы файлов и предоставляет возможность гибкой настройки резервирования

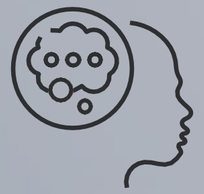


# Анализ запускаемых файлов и загружаемых модулей

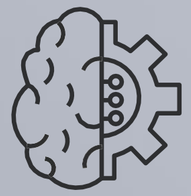
PT
Информационная безопасность

## Анализ всех исполняемых модулей перед загрузкой

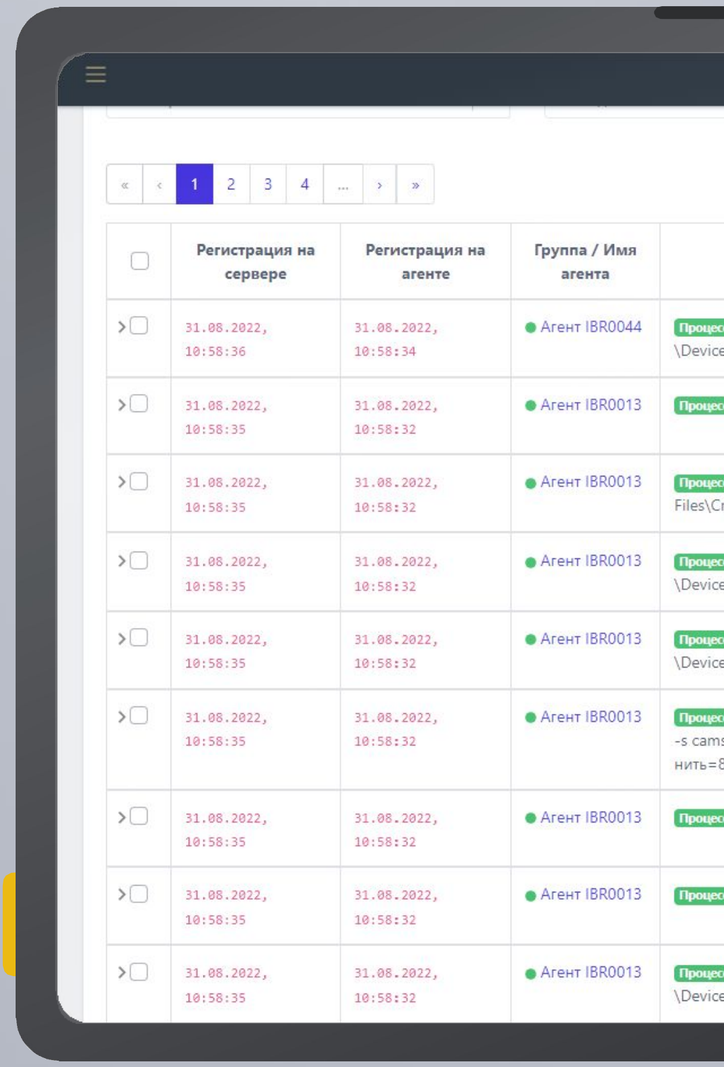
Сигнатурный анализ



Эвристика



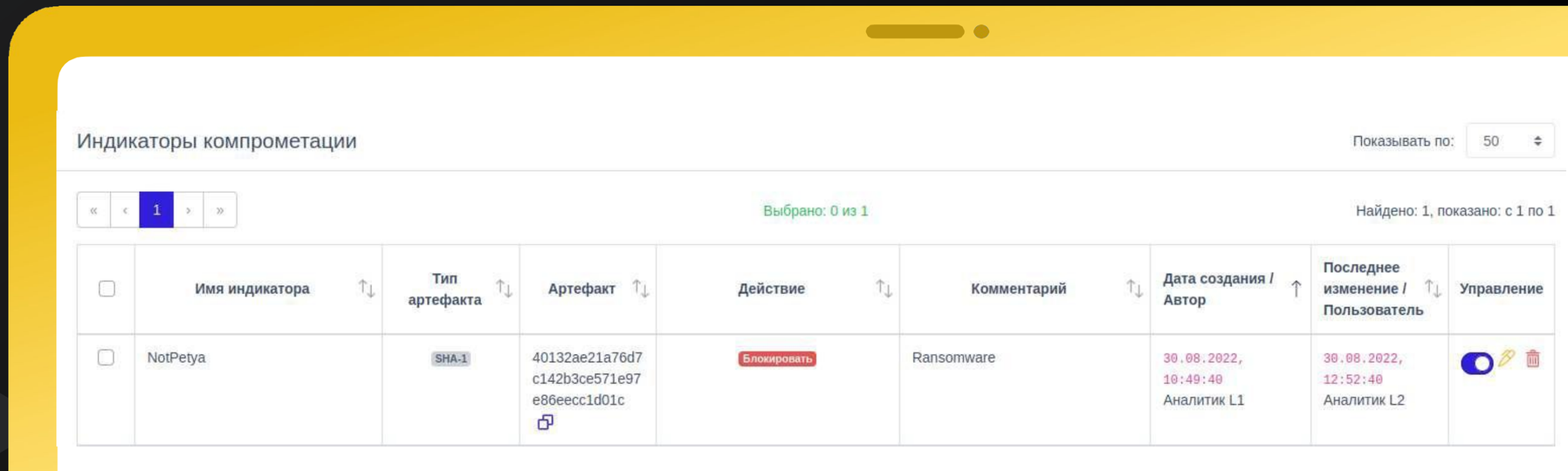
Легковесная модель машинного обучения



# Работа с индикаторами компрометации

PT
Информационная безопасность

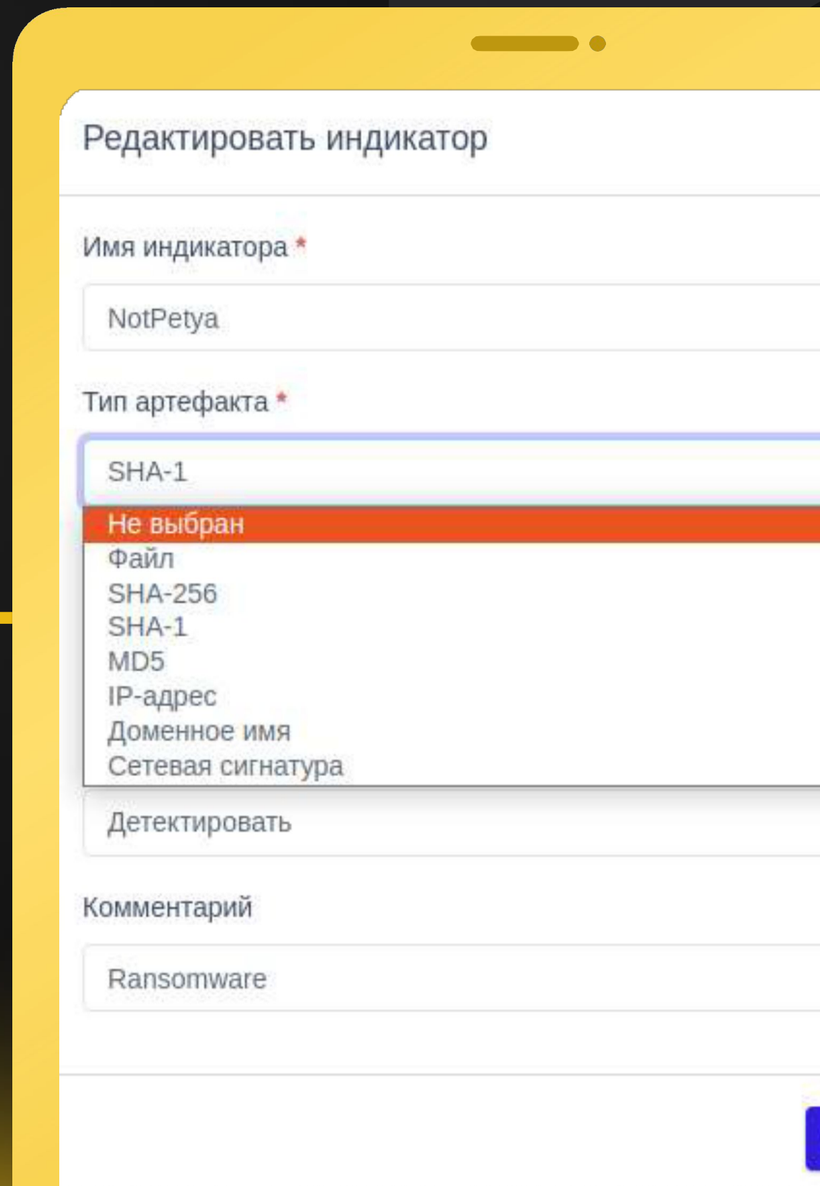
- Многообразие типов индикаторов компрометации
- Удобная система управления индикаторами компрометации и их наборами



# Индикаторы компрометации

**Предназначены для выявления известных атак по следующим артефактам:**

- хеш файла
- имя файла
- IP-адрес
- доменное имя
- сетевая сигнатура




PT
Информационная безопасность

# Индикаторы атак

PT
Информационная
безопасность

## Работающие в режиме реального времени

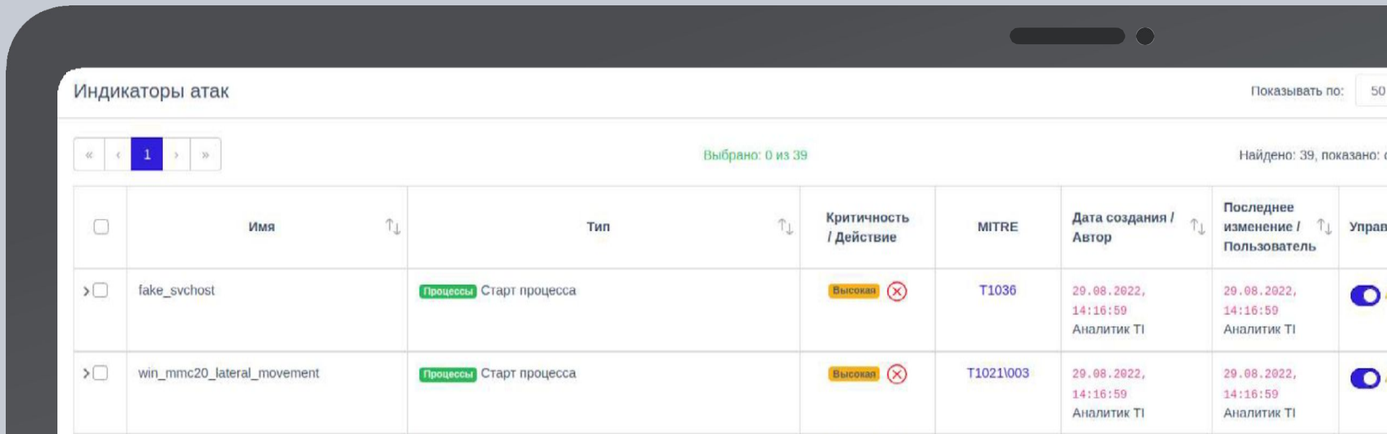
Классификация по
матрице MITRE ATTACK

Регулярное
обновление TI

Конвертер Sigma
правил

Удобная система управления
индикаторами атак и их наборами

Собственные правила выявления угроз с
интуитивно понятным механизмом написания IOA

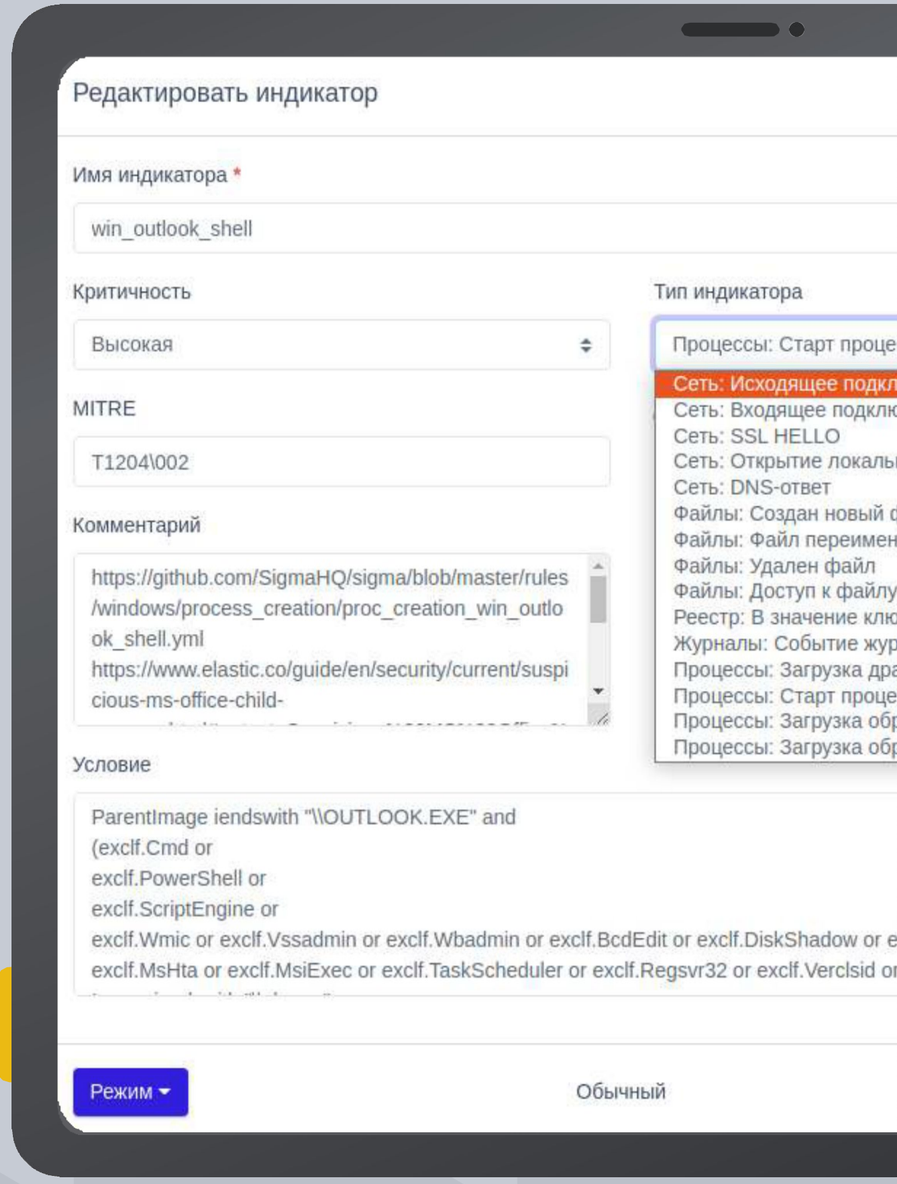


# Индикаторы атак

PT
Информационная безопасность

**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)



# Threat Hunting

PT
Информационная безопасность

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

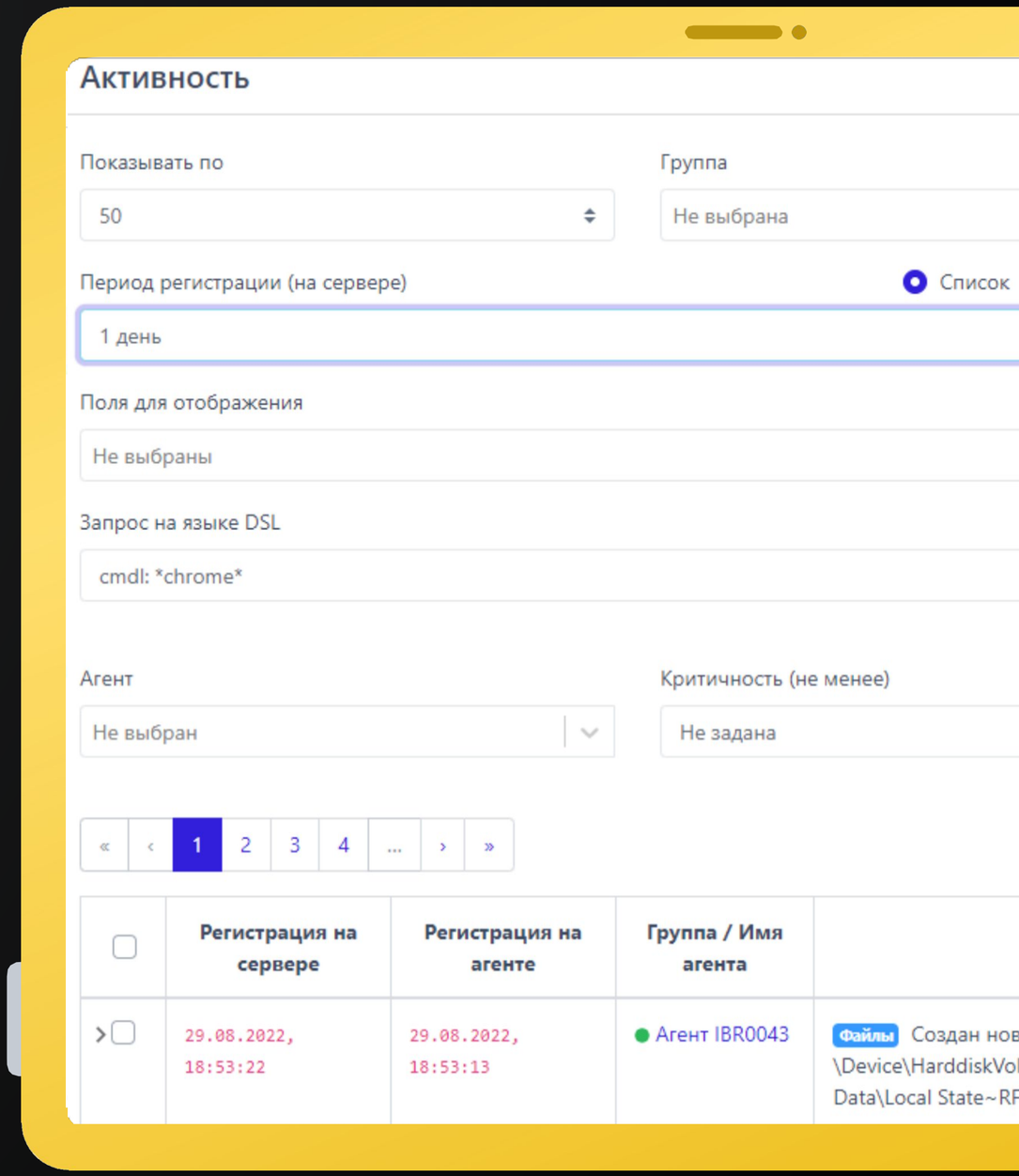
## Гибкий поиск угроз

Быстрый и удобный поиск угроз в корпоративной сети по событиям EDR

Настраиваемая фильтрация событий по различным параметрам

DSL

Возможность использование языка DSL для продвинутой фильтрации

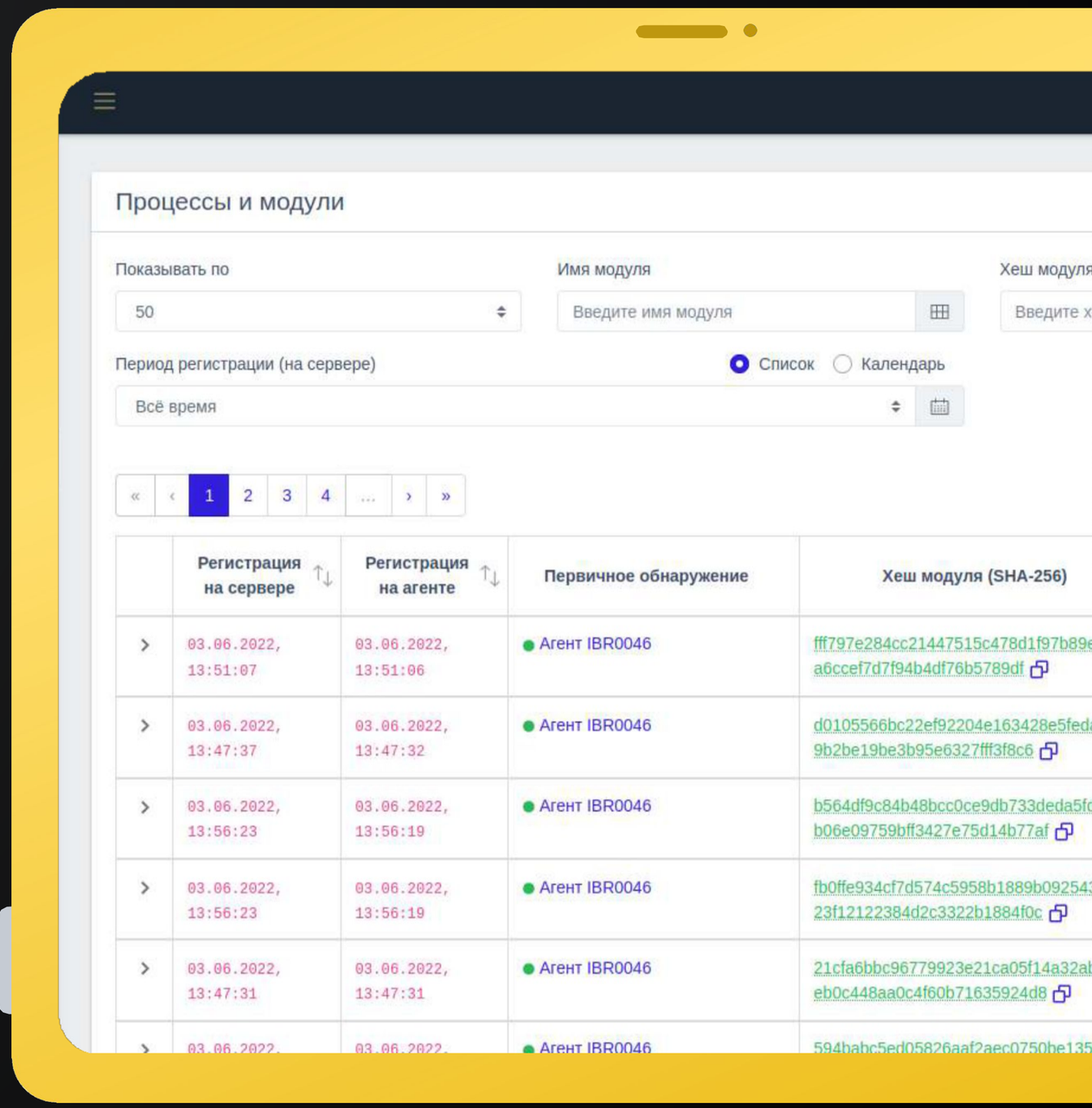



PT
Информационная безопасность

# Threat Hunting

## Процессы и модули

- Распространенность по агентам инфраструктуры заказчика
- Удобный поиск по хешу (SHA256)
- Отображение цифровой подписи
- Первоисточник обнаружения



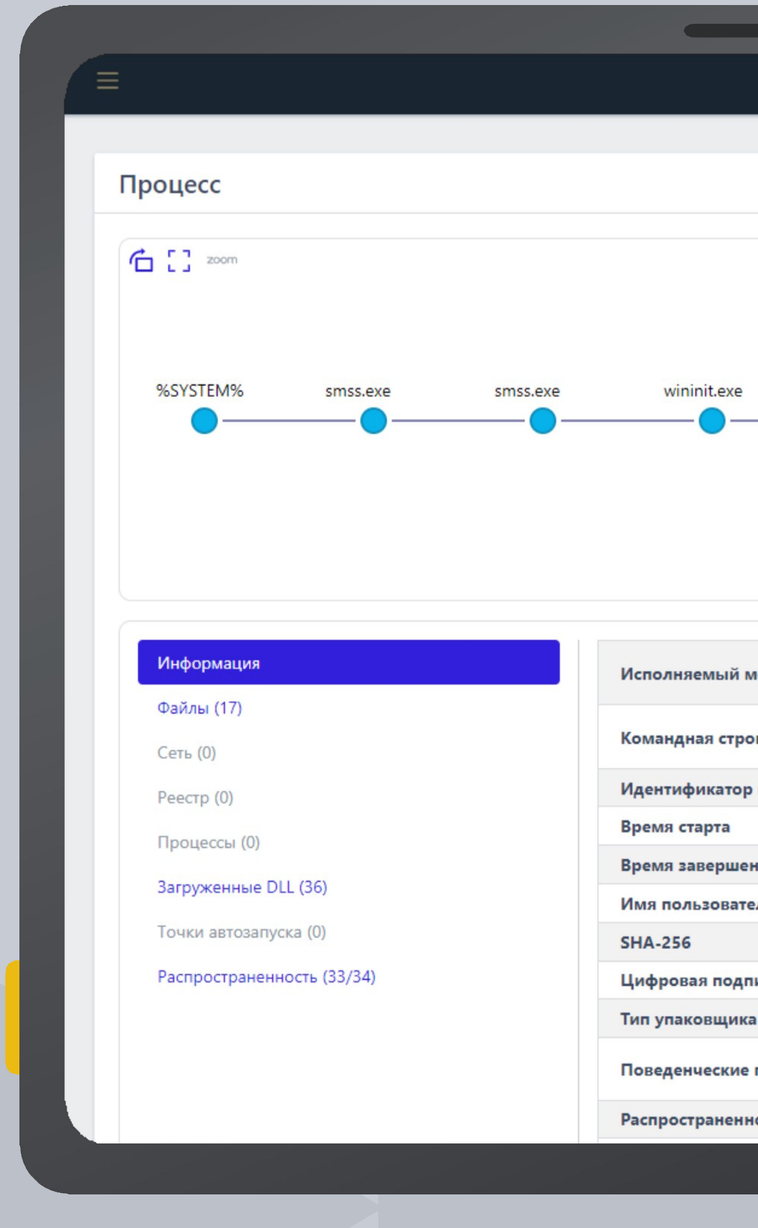

PT
Информационная безопасность

# Богатый инструментарий расследования инцидентов

PT
Информационная безопасность

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

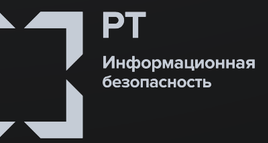
Сведения о распространенности подозрительных исполняемых модулей в агентской сети

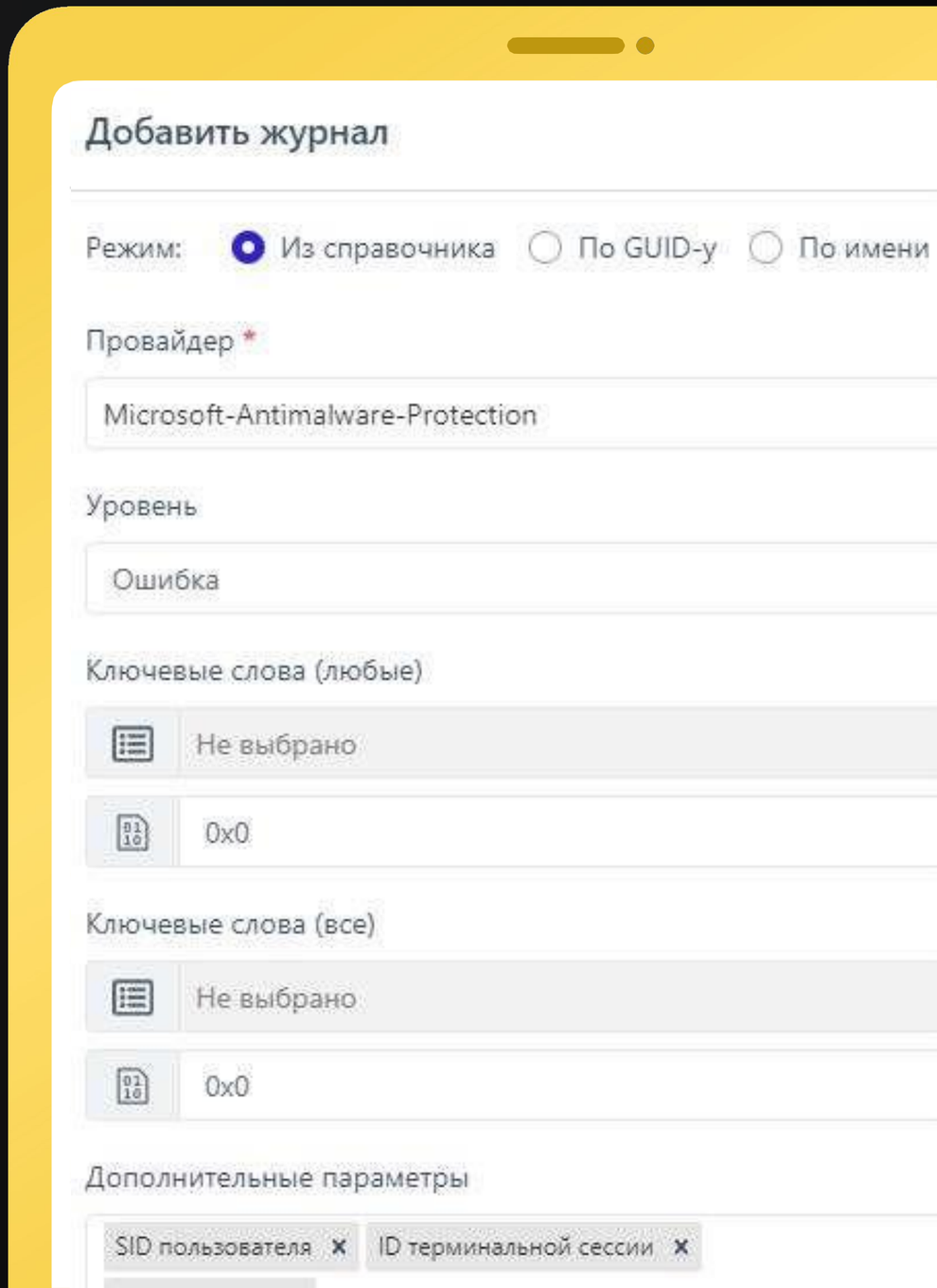


# Сбор данных журналов

Взаимодействие с любыми провайдерами журналов Windows

Возможность сбора журналов со средств защиты информации заказчика



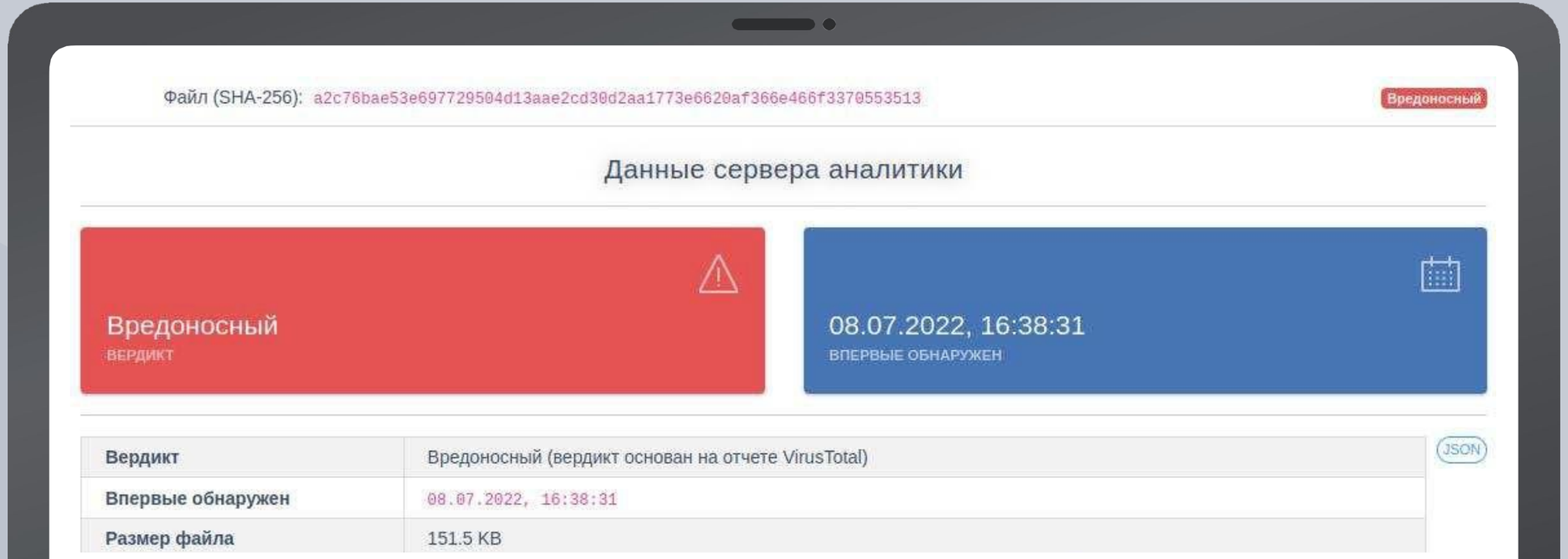



# Сервер аналитики (TI portal)

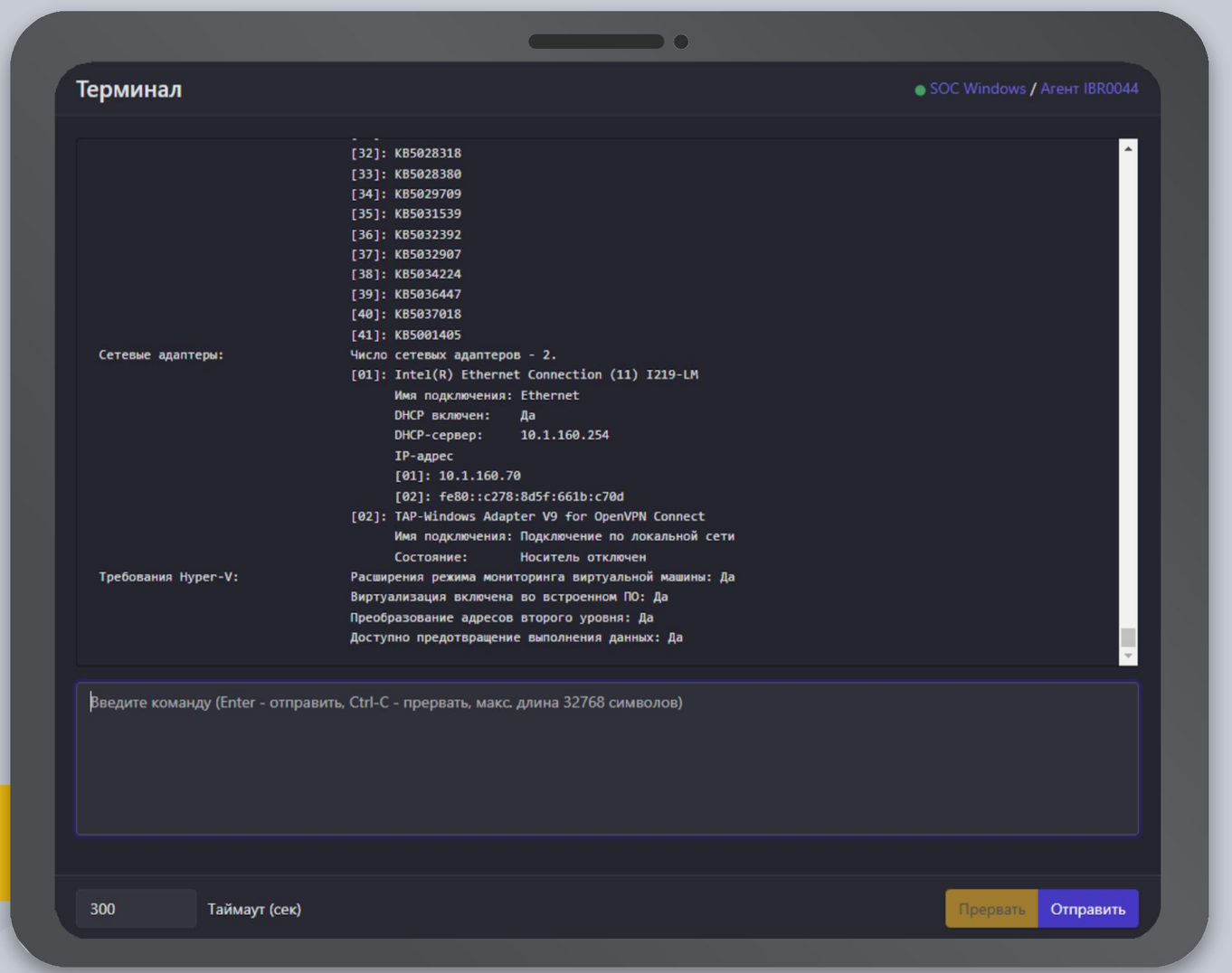
PT
Информационная безопасность

Интеграция с популярными TI решениями

Регулярное обновление наборов индикаторов компрометации



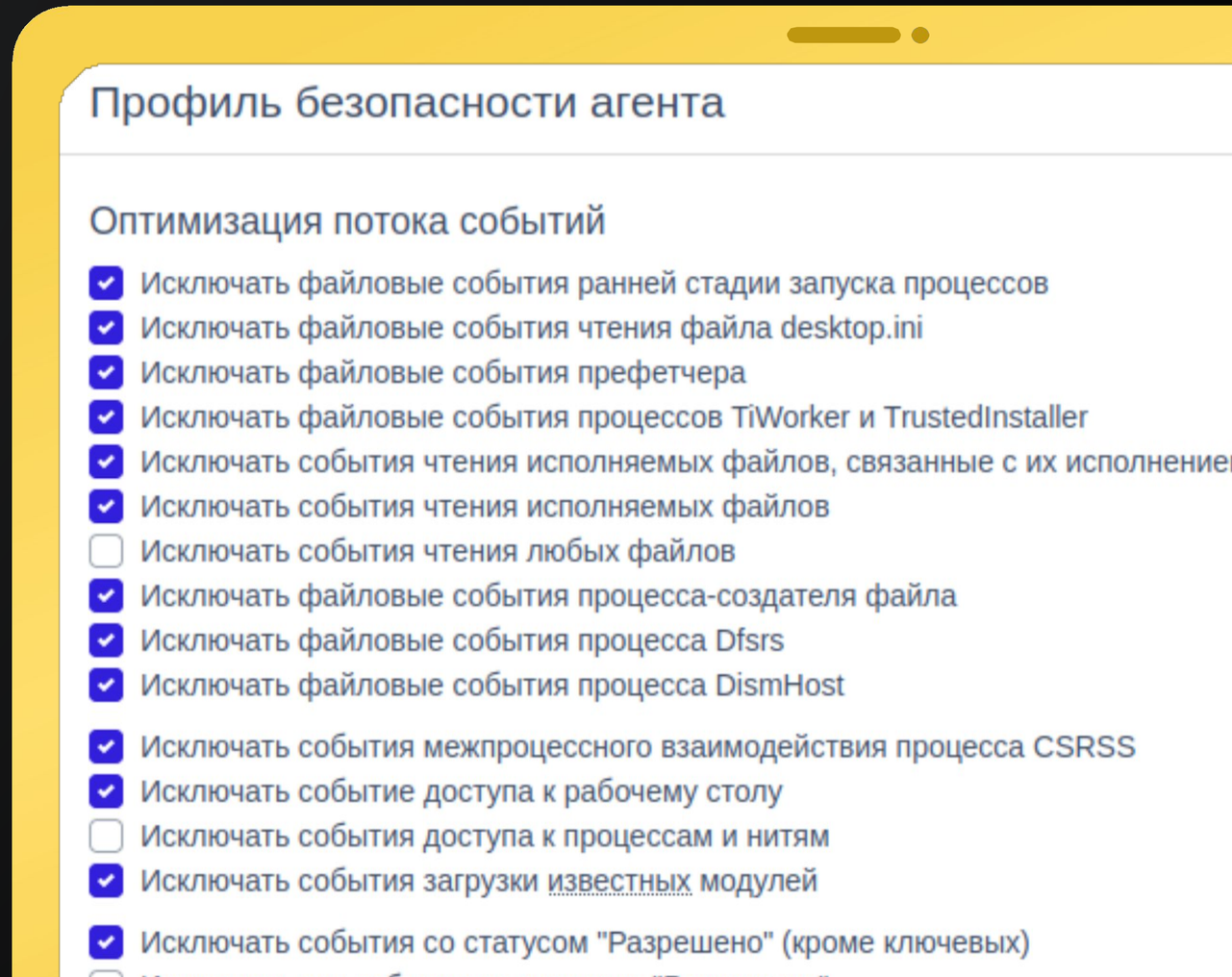
# Терминал удаленного доступа



# 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

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 (InhibitSystemRe

Блокировать

Реакция на запуск программ из альтернативных потоков NTFS (AltExeStream)

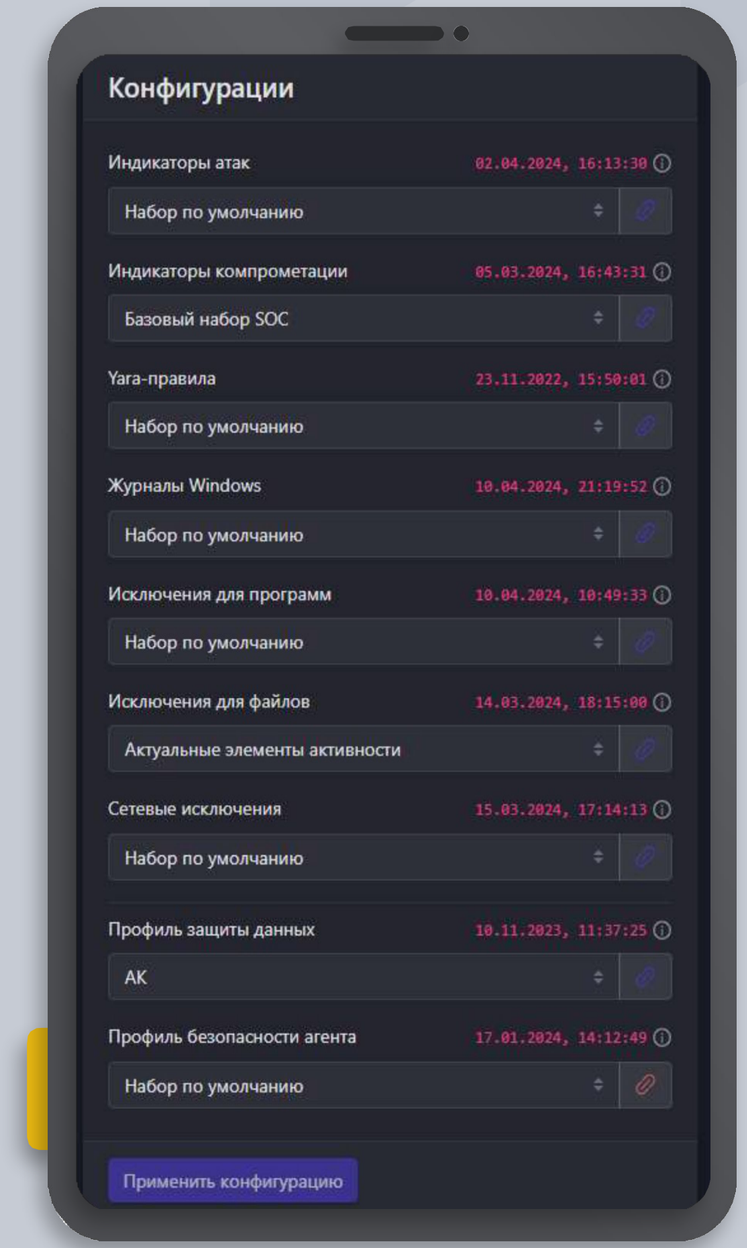
Блокировать

PT
Информационная безопасность

# Настройка профиля безопасности агента

PT
Информационная безопасность

Обилие тонких настроек позволяет создавать эффективные профили безопасности



# Сервер аналитики (TI portal)

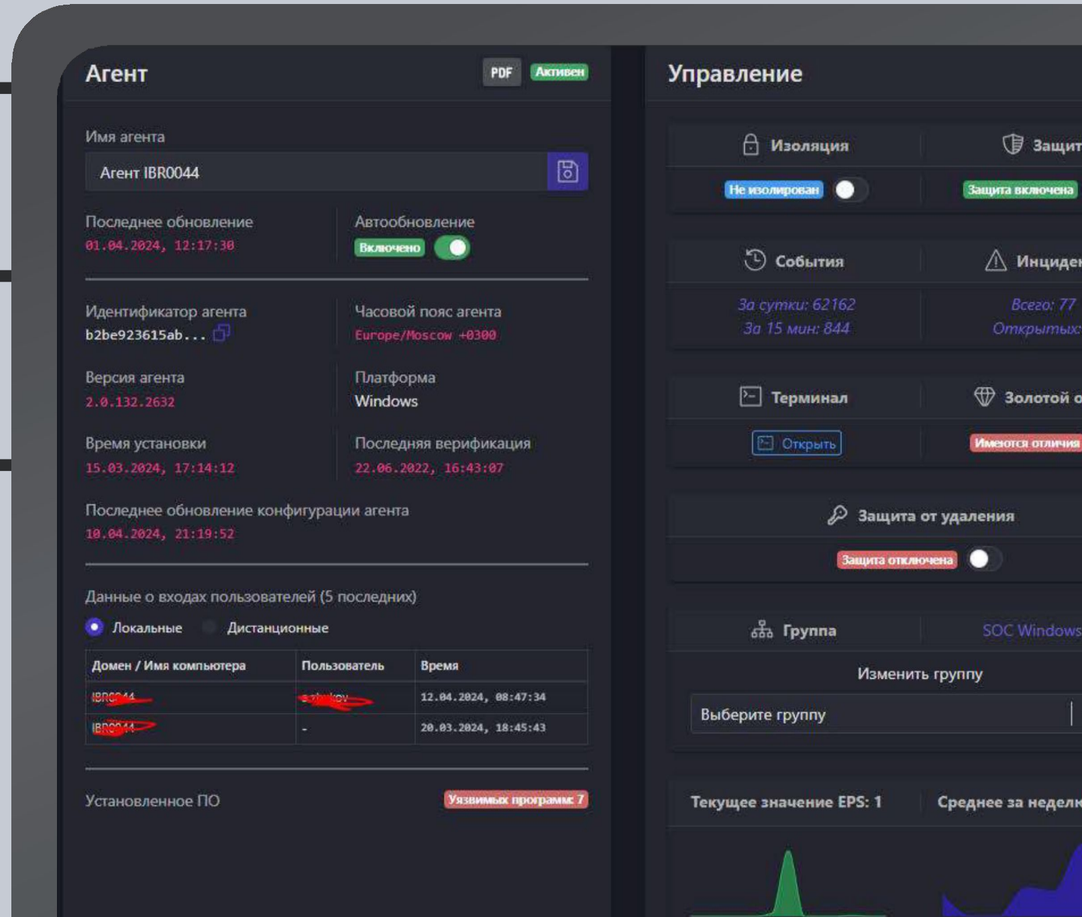
PT
Информационная безопасность

**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



# Модуль управления уязвимостями

PT
Информационная безопасность

# Нам доверяют

Ростех
РТ-Энергоэффективность
РТ
Развитие бизнеса
Ростех
Техприемка
Ростех
KAMAZ
ОАК
Объединенная авиастроительная корпорация
ОДК
КБП
СИБЕР
Нацимбио
Высокоточные комплексы
УВЗ
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