RT Protect EDR

Endpoint Detection and Response

РТ-Информационная безопасность

Нами за 2023 год выявлено:

Более

60 000

зафиксированных событий ИБ, которые удалось предотвратить.

Увеличение количества внутренних и внешних атак на гос. организации

в 1,5 раза

по сравнению с данными 2022 года.

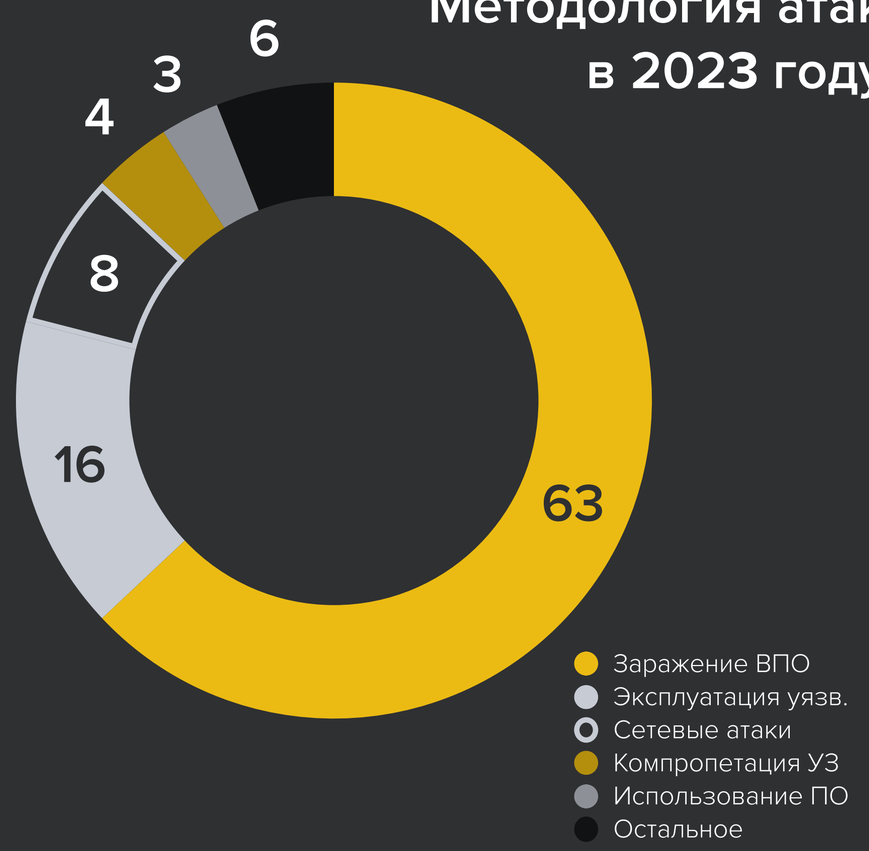
Увеличение количества атак на госучреждения практически

в 2,5 раза

по сравнению с данными 2022 года.

RT Protect EDR - актуальное средство защиты ИБ, отразившее 100% атак на Киберполигоне 2022

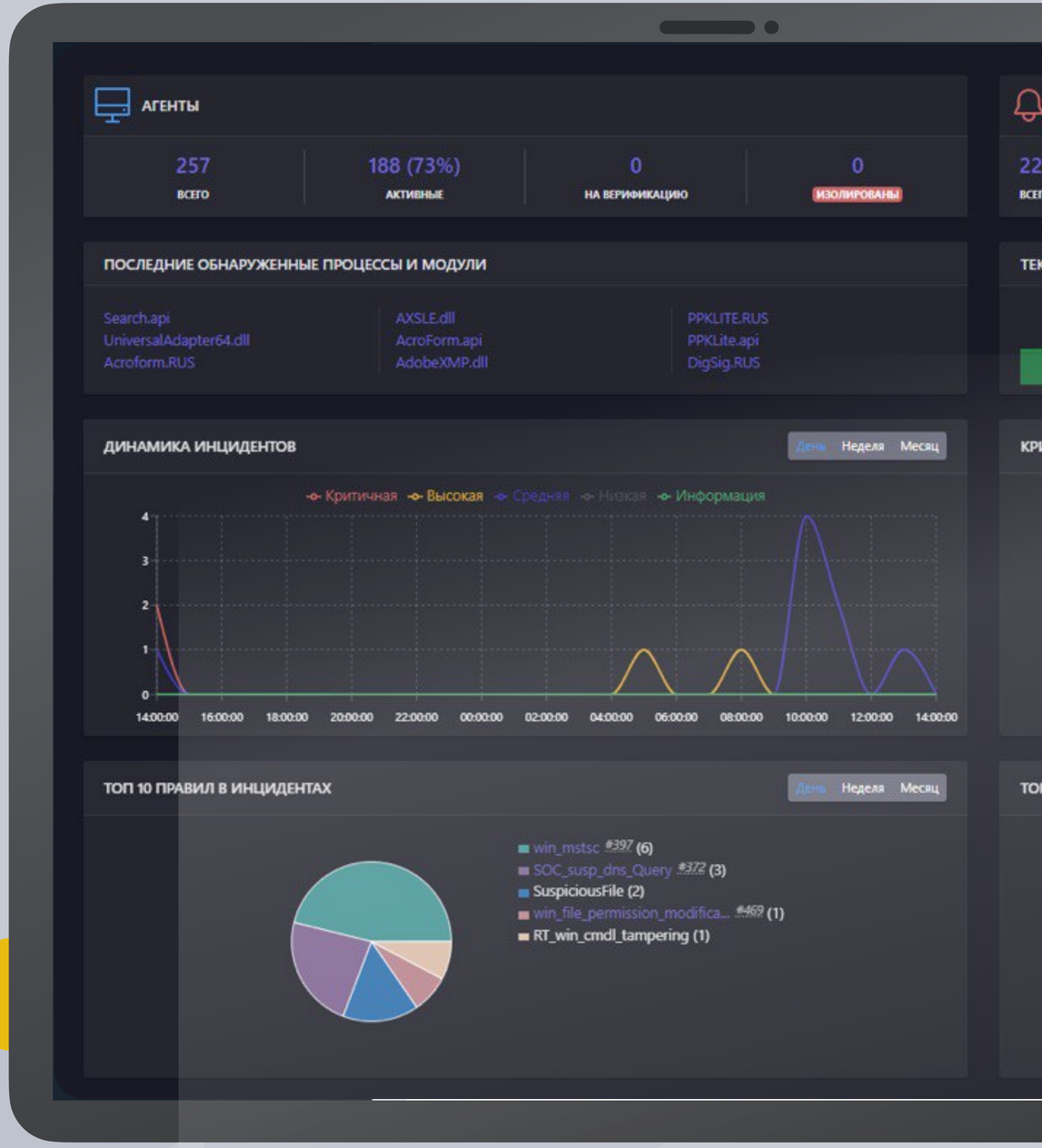
Методология атак в 2023 году



РТ
Информационная безопасность

Система обнаружения целенаправленных атак и сложных угроз

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



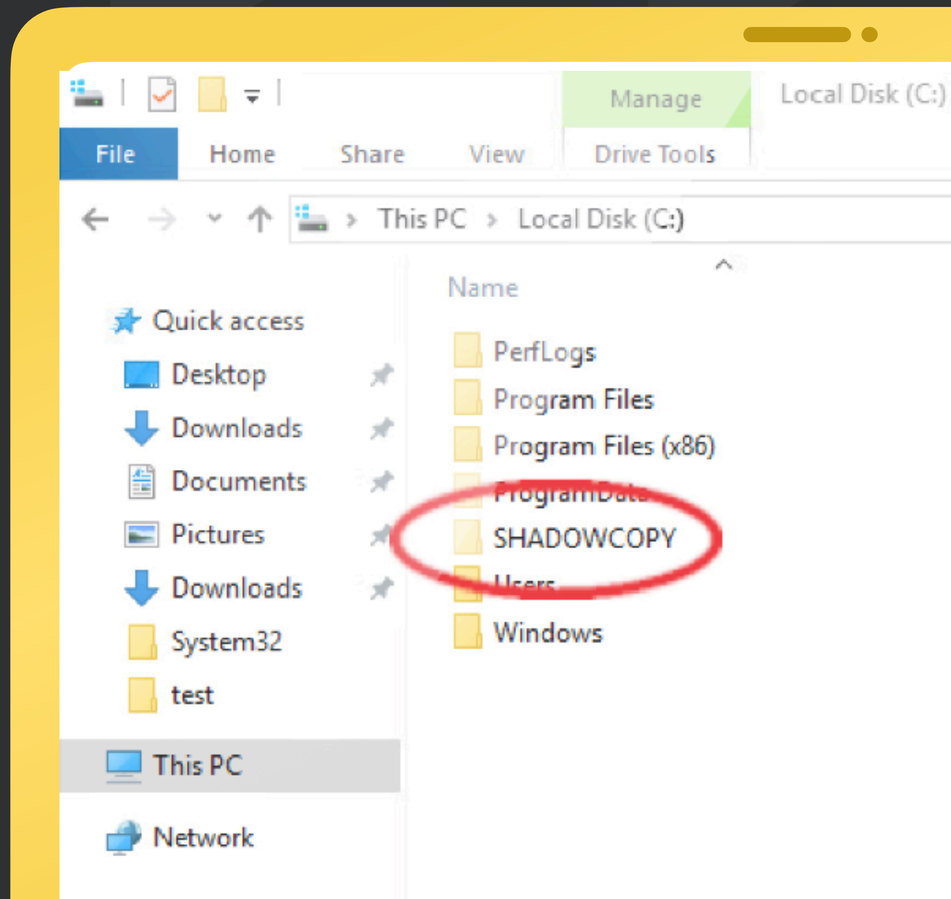
PT
Информационная безопасность

Защита 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

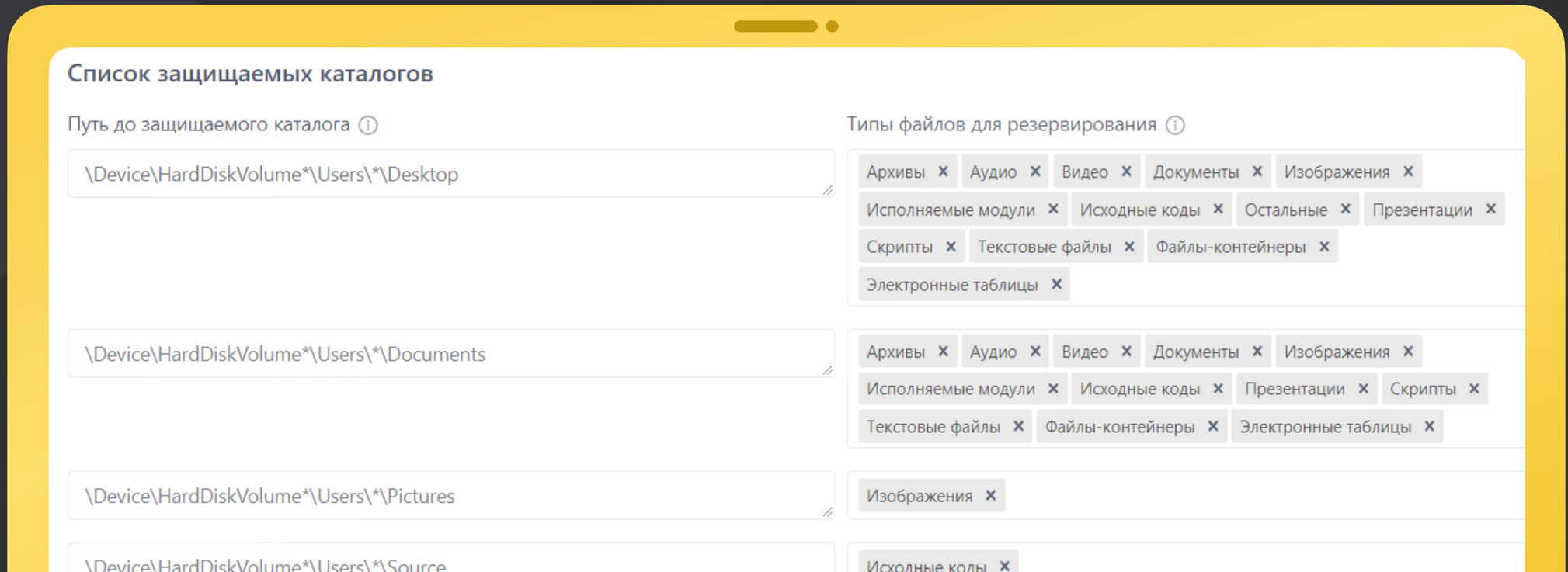


PT
Информационная безопасность

Защита от вирусов-вымогателей

восстанавливает резервируемые файлы в случае утраты

поддерживает все типы файлов и предоставляет возможность гибкой настройки резервирования



PT
Информационная безопасность

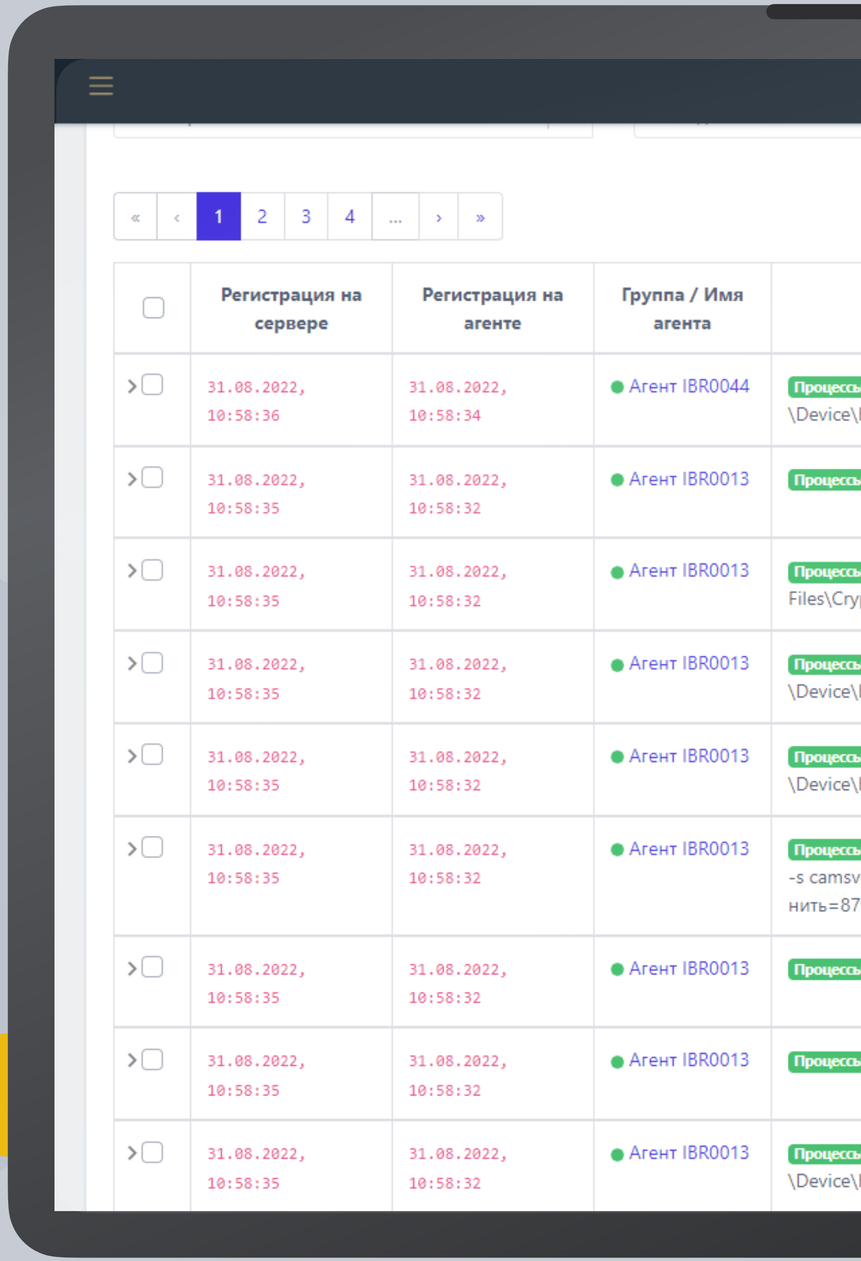
Анализ запускаемых файлов и загружаемых модулей

Анализ всех исполняемых модулей перед загрузкой:

сигнатурный анализ

эвристика

легковесная модель машинного обучения

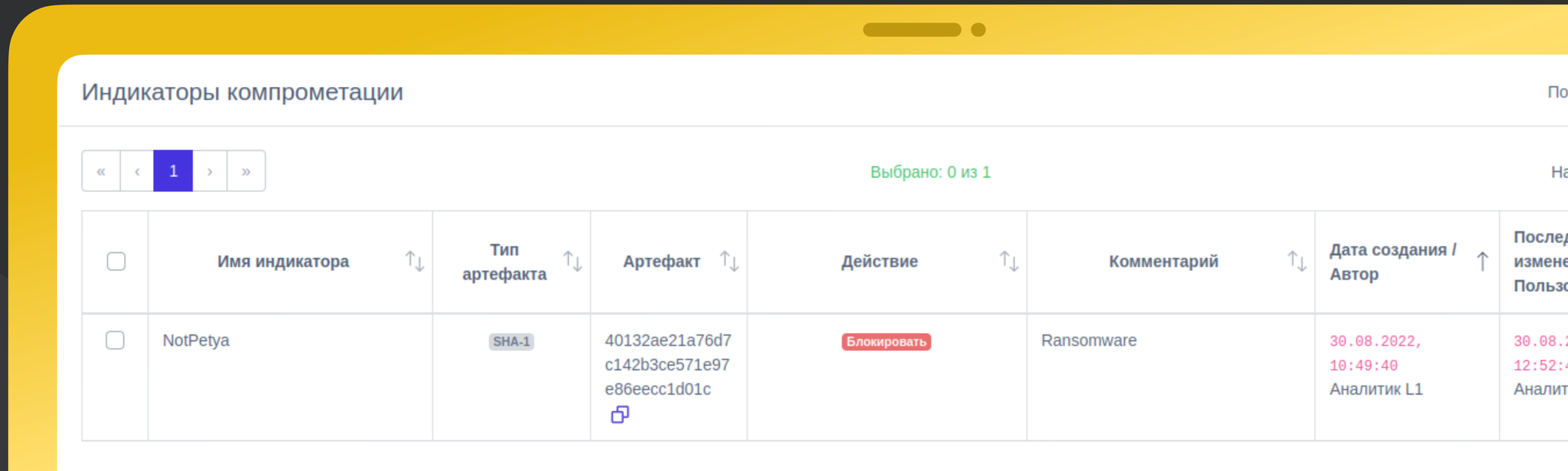


PT
Информационная безопасность

Индикаторы компрометации

Многообразие типов индикаторов компрометации

Удобная система управления индикаторами компрометации и их наборами

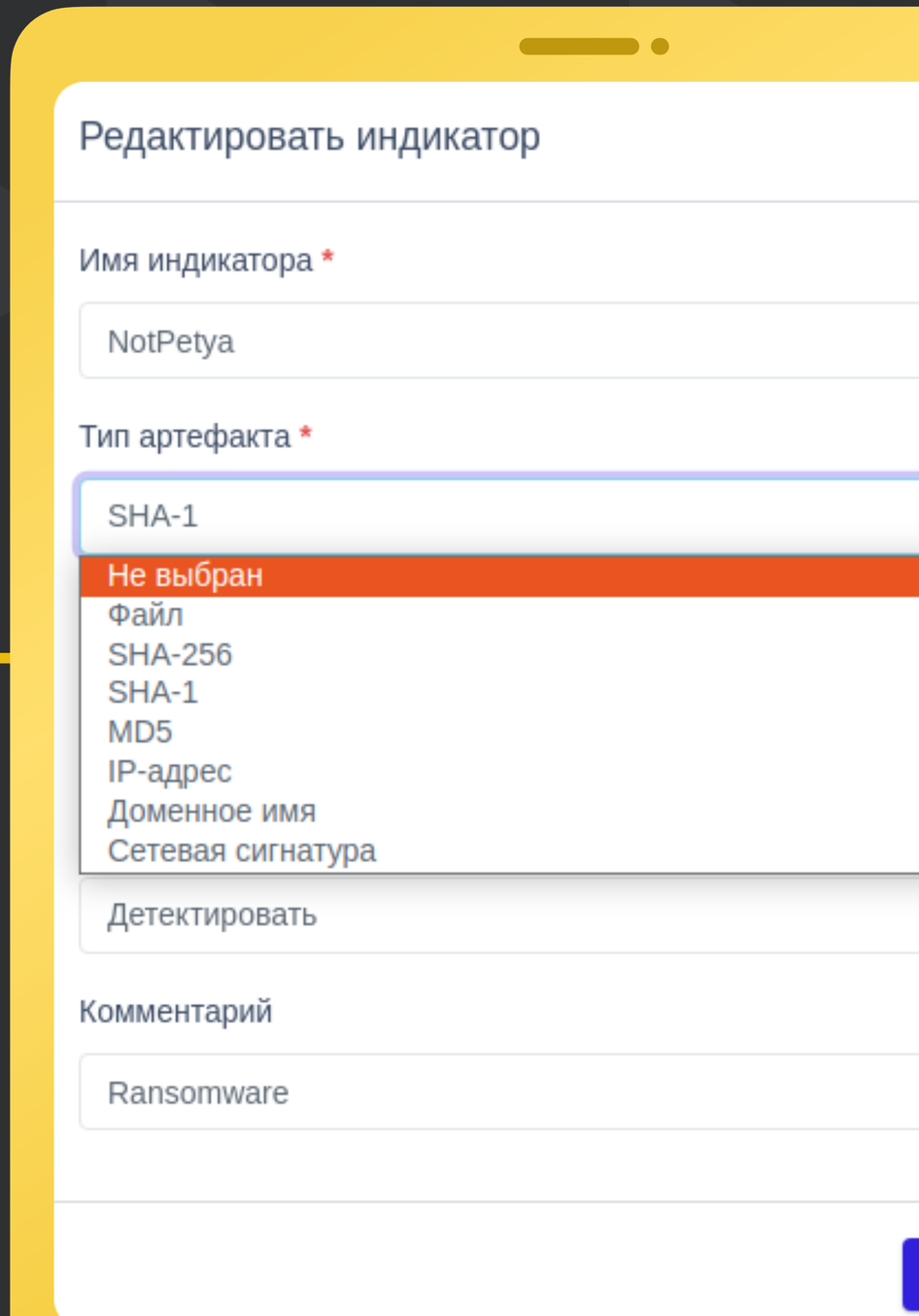


PT
Информационная безопасность

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

Работающие в режиме реального времени

Классификация по матрице MITRE ATT&CK

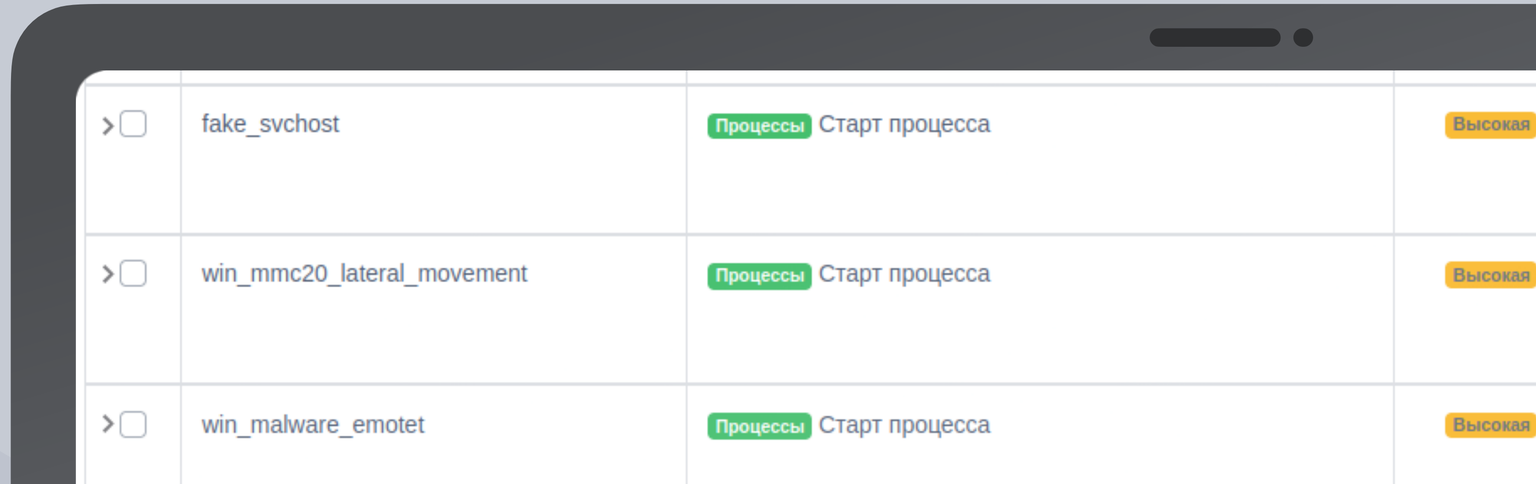
Удобная система управления индикаторами атак и их наборами

Регулярное обновление специалистами TI

Собственные правила выявления угроз с интуитивно понятным механизмом написания IOA

Конвертер Sigma правил

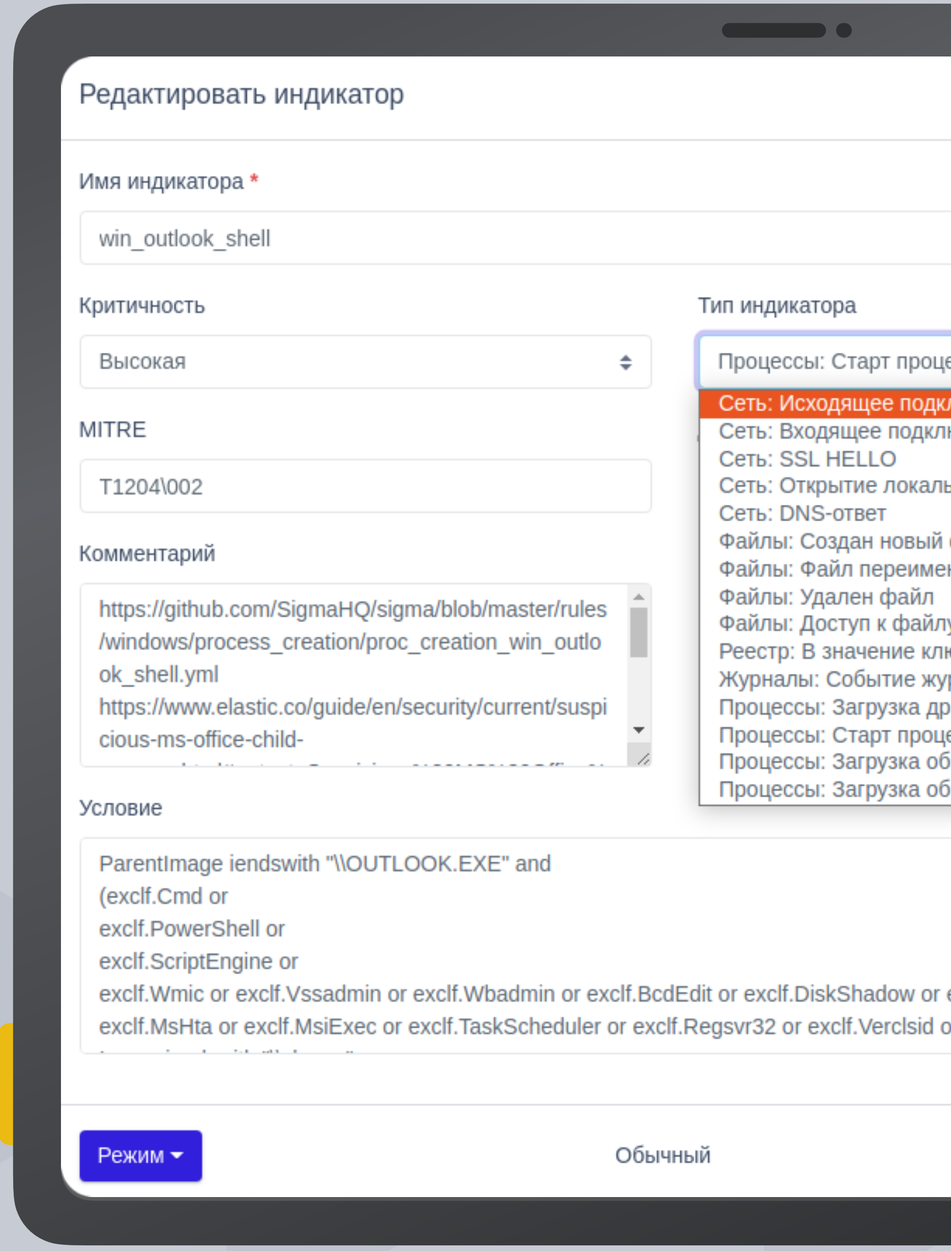
PT
Информационная безопасность



Индикаторы атак

Возможность писать правила обнаружения атак на основе событий:

- создания процесса
- загрузки исполняемого модуля
- создания/ модификации файла
- DNS-запроса
- сетевого соединения (CONNECT)
- открытие порта для входящих соединений (LISTEN)



PT
Информационная безопасность

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

PT
Информационная безопасность

Threat Hunting

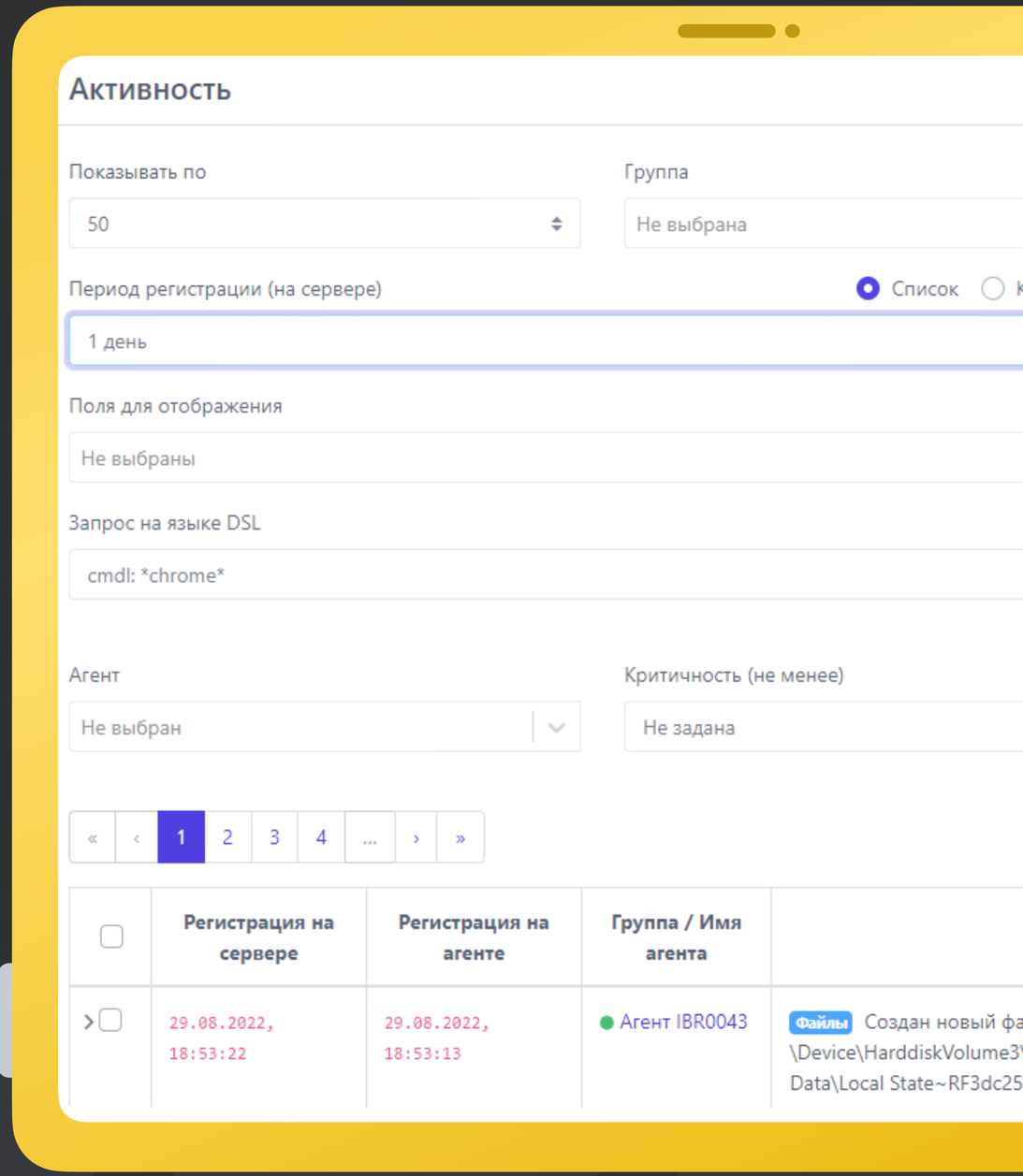
Гибкий поиск угроз

Быстрый и удобный поиск угроз в корпоративной сети по событиям EDR

Настраиваемая фильтрация событий по различным параметрам

DSL

Возможность использования языка DSL для продвинутой фильтрации



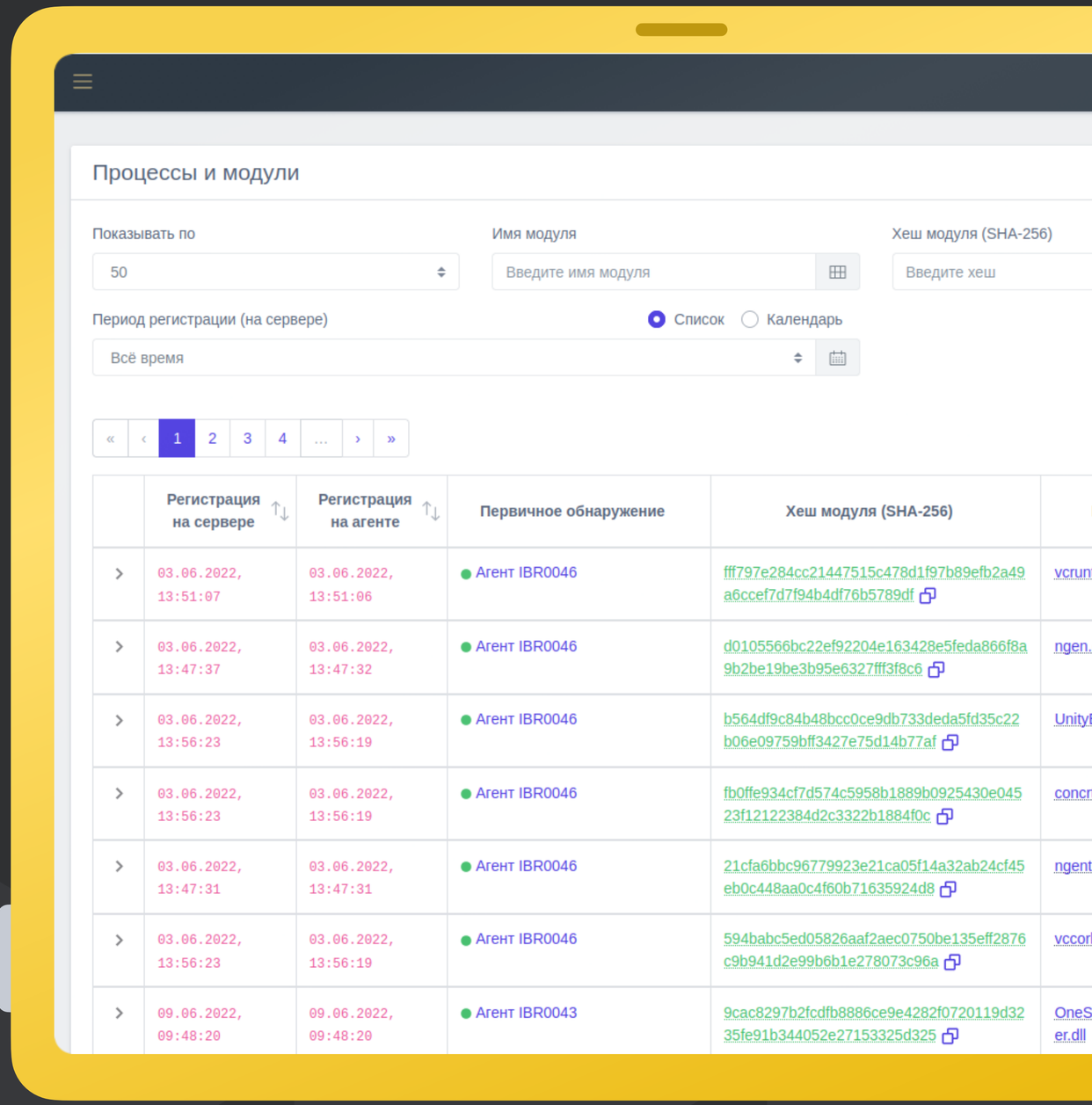
PT
Информационная безопасность

Threat Hunting

Процессы и модули

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

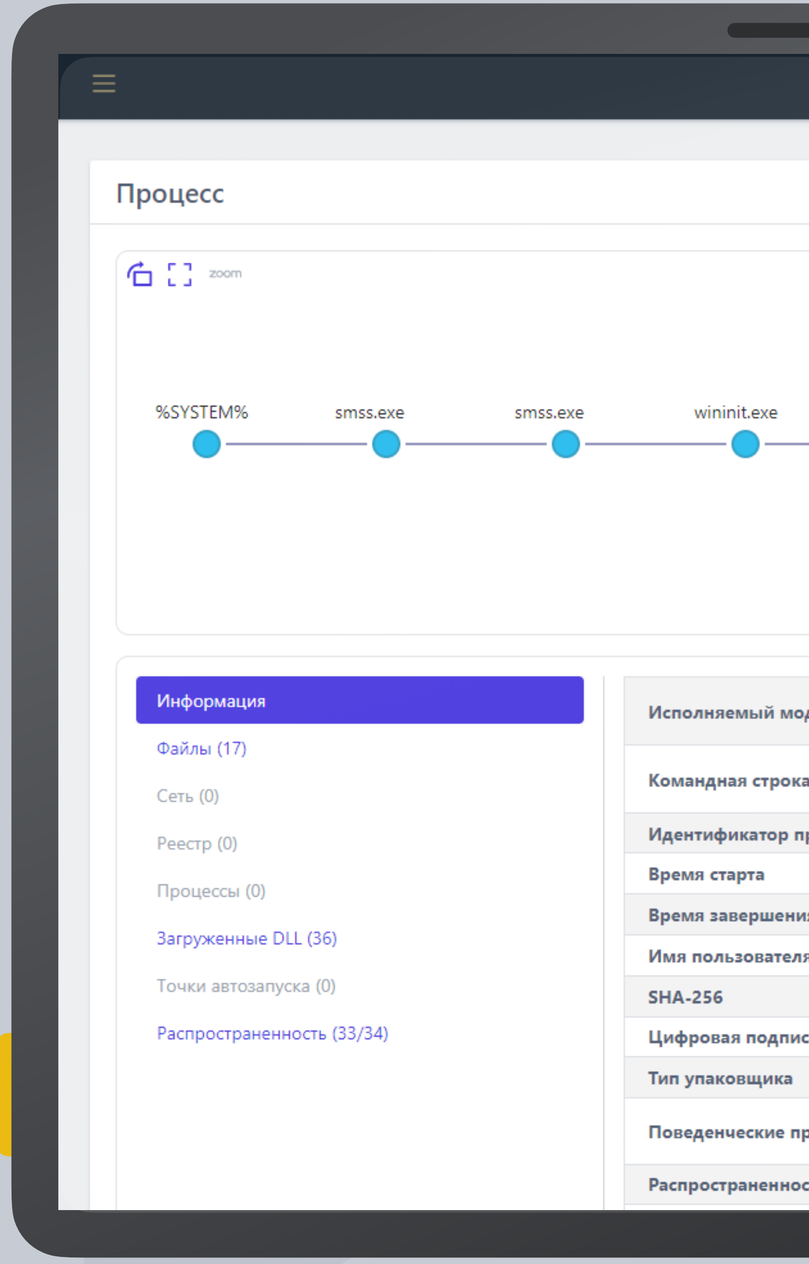
PT
Информационная безопасность



Богатый инструментарий расследований инцидентов

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

сведения о распространенности подозрительных исполняемых модулей в агентской сети

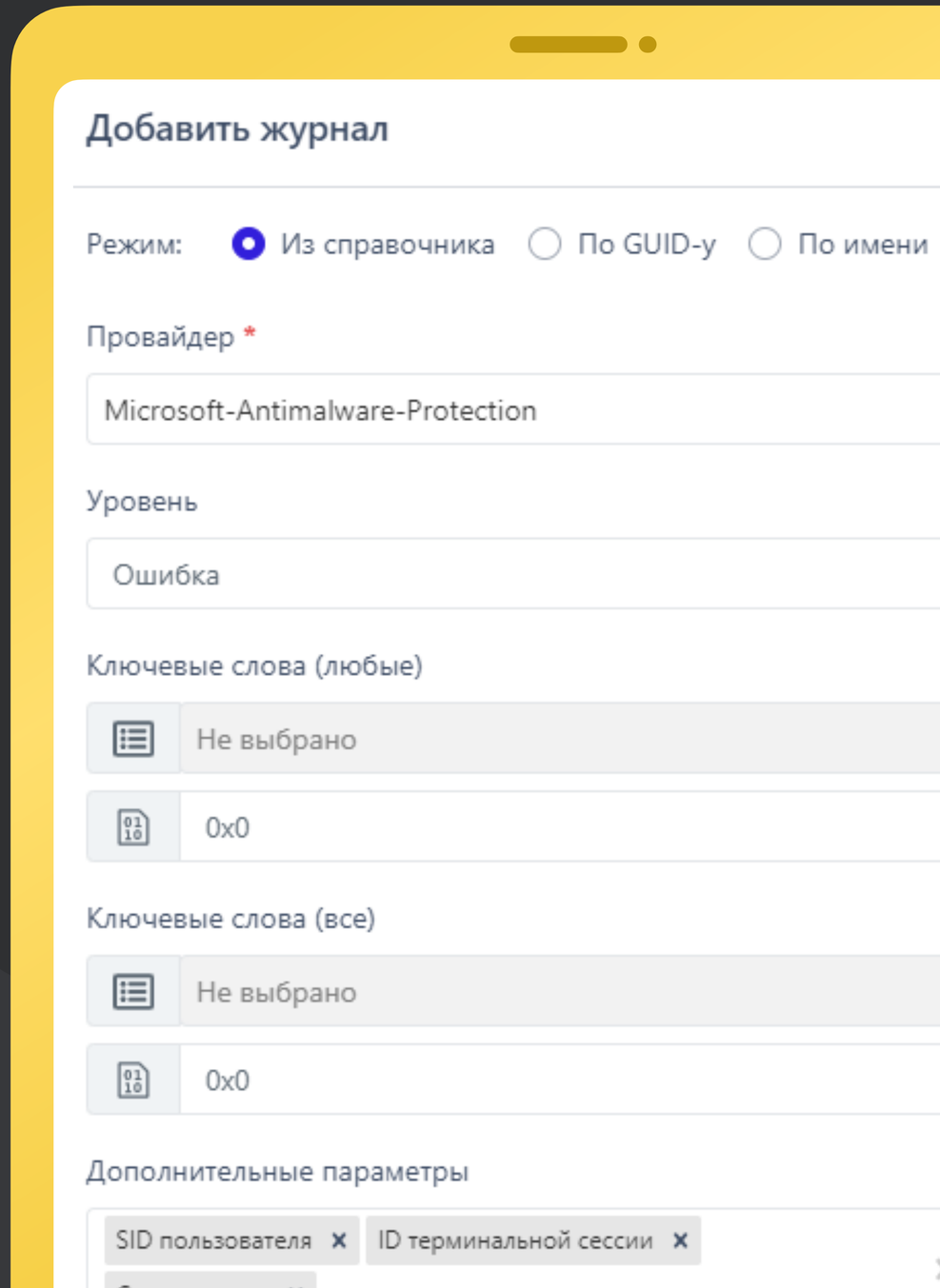


PT
Информационная безопасность

Сбор данных журналов

Взаимодействие с любыми провайдерами журналов Windows

Возможность сбора журналов со средств защиты информации заказчика

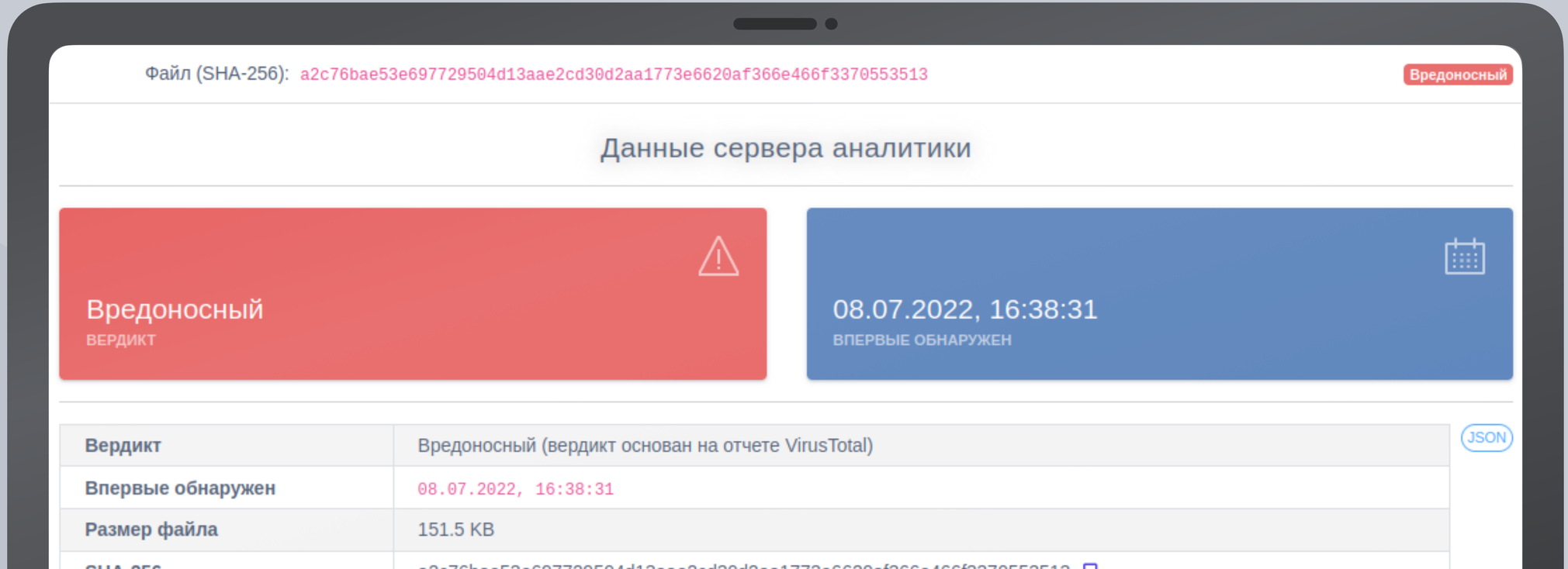


PT
Информационная безопасность

Сервер аналитики (TI portal)

Интеграция с популярными TI решениями

Регулярное обновление наборов индикаторов компрометации

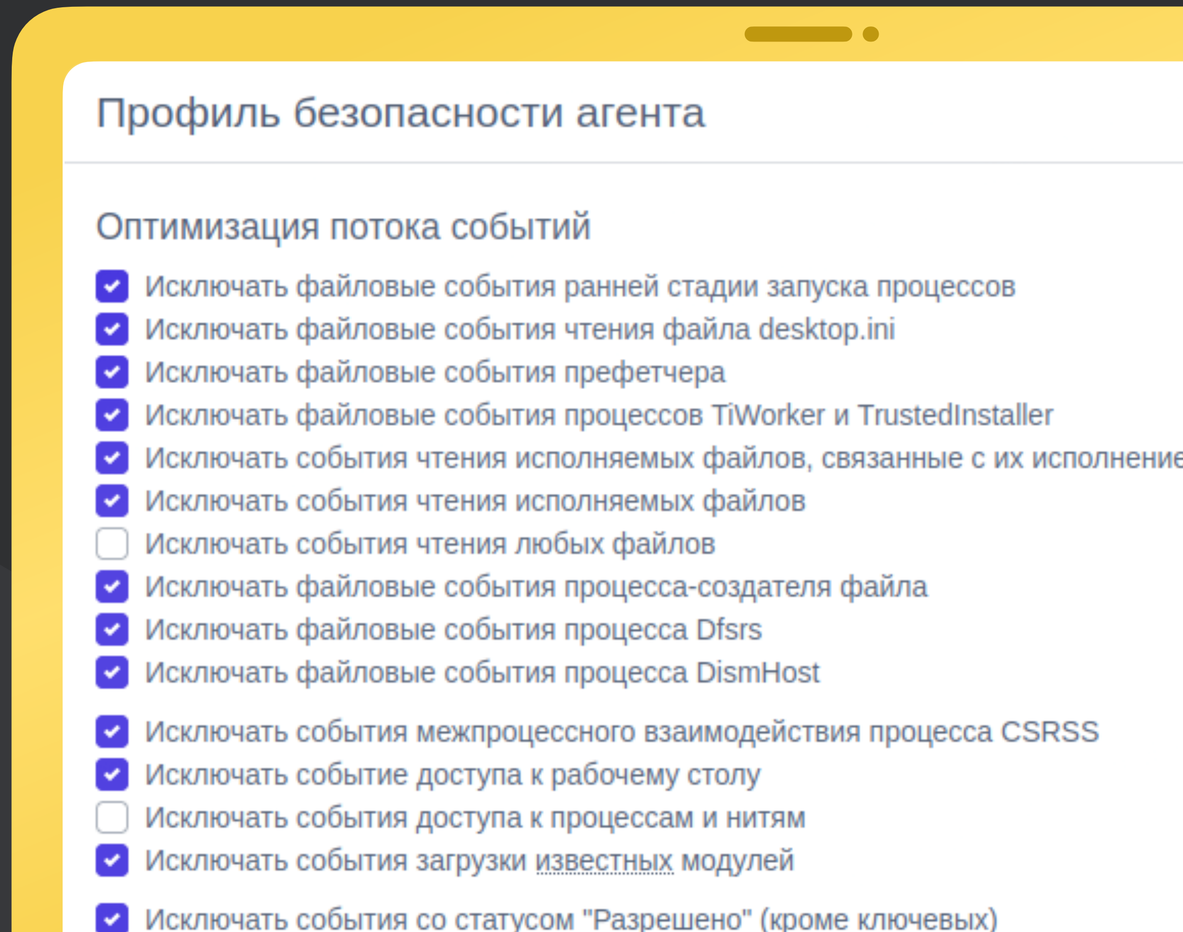


PT
Информационная безопасность

Профиль безопасности агента

Гибкая настройка сбора событий для отправки на сервер

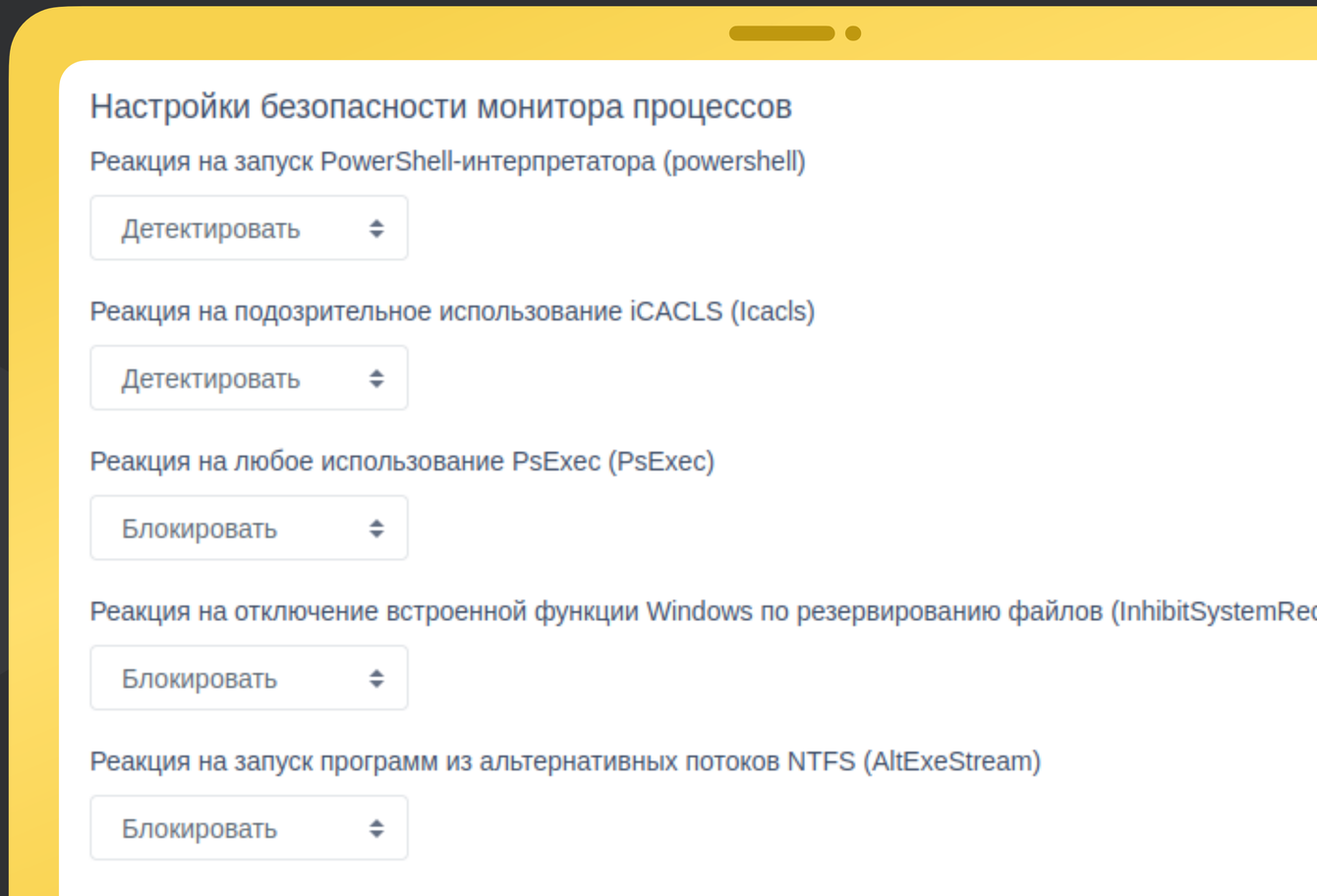
Персонализированный подход конфигурирования агентов для разных типов профилей защиты



PT
Информационная безопасность

Профиль безопасности агента

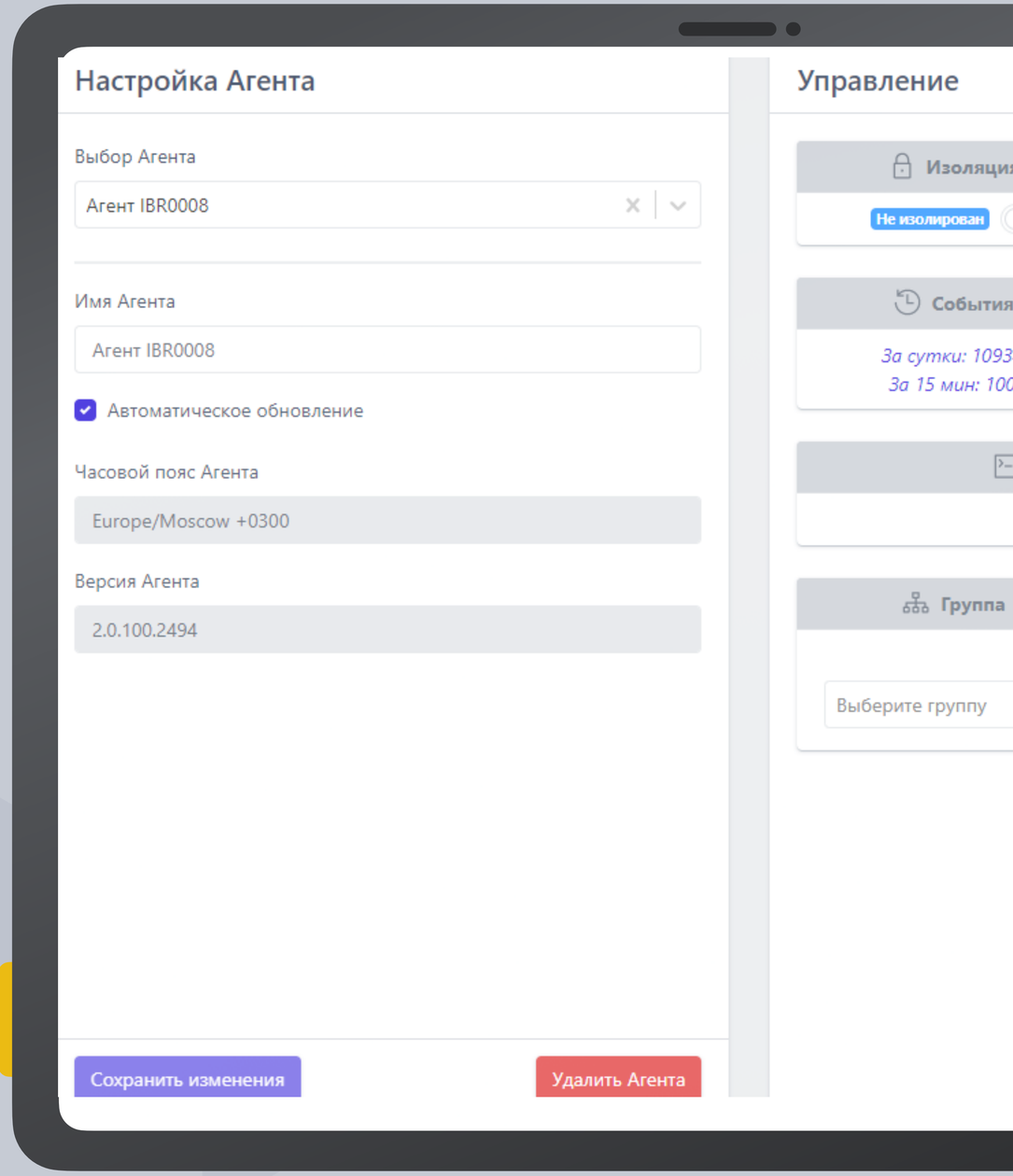
Удобная система распространения профилей безопасности агентов



PT
Информационная безопасность

Настройка профиля безопасности агента

Обилие тонких настроек позволяет создавать эффективные профили безопасности



PT
Информационная безопасность

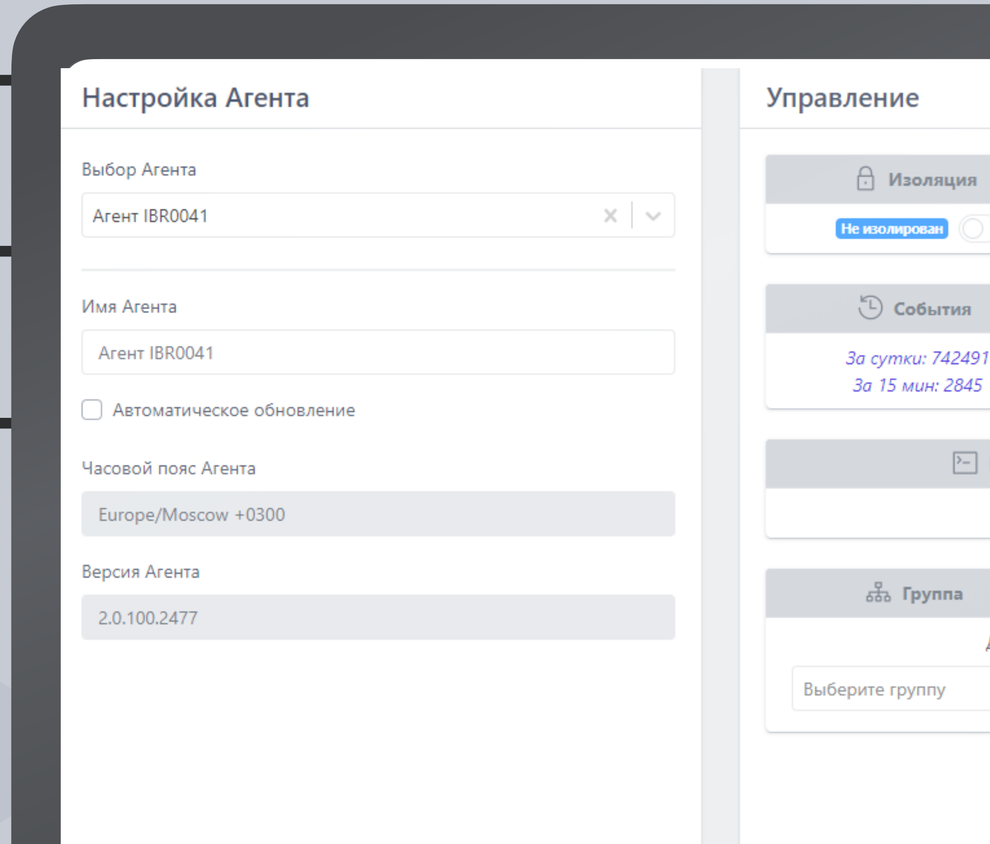
Удаленное управление агентами

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

детальное расследование инцидентов безопасности

устранения последствий атак на корпоративную инфраструктуру

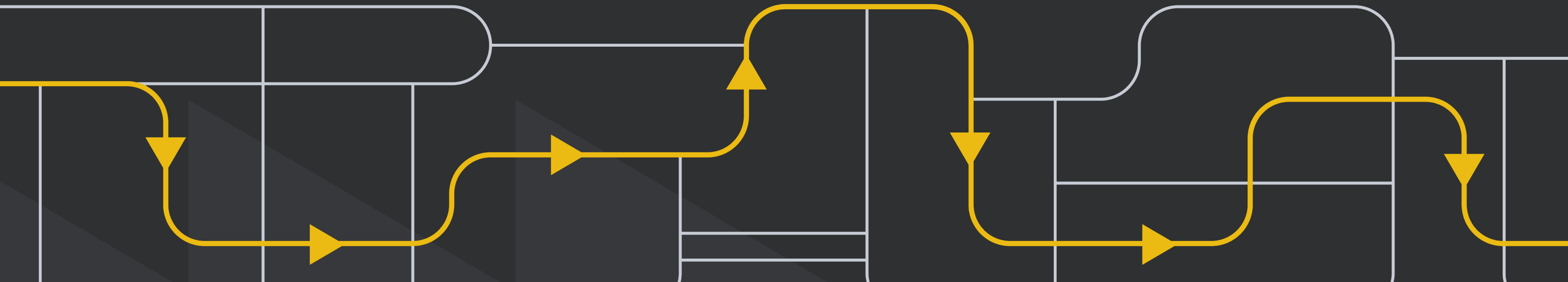
сетевая изоляция хоста



PT
Информационная безопасность

Планы развития

- Linux-агент
- Автоматическое устранение последствий атак
- Продвинутые возможности реагирования (плейбуки, задачи)
- Песочница
- Интеграция с другими системами через json
- Расширение применения методов машинного обучения



Собственный антивирус для ОС семейства Linux RT Protect AV

Работает под управлением сертифицированных ОС

- Astra Linux Special Edition (релиз Смоленск 1.6)
- Astra Linux Common Edition (релиз Орел 2.12.22)
- RedOS 7.3
- ALT Linux SP8

Включен в Единый реестр российских программ для ЭВМ и баз данных, номер записи 10856

Сертифицирован ФСТЭК по профилю защиты САВЗ типа «В» четвертого класса защиты (ИТ.САВЗ.В4.ПЗ)

PT
Информационная безопасность

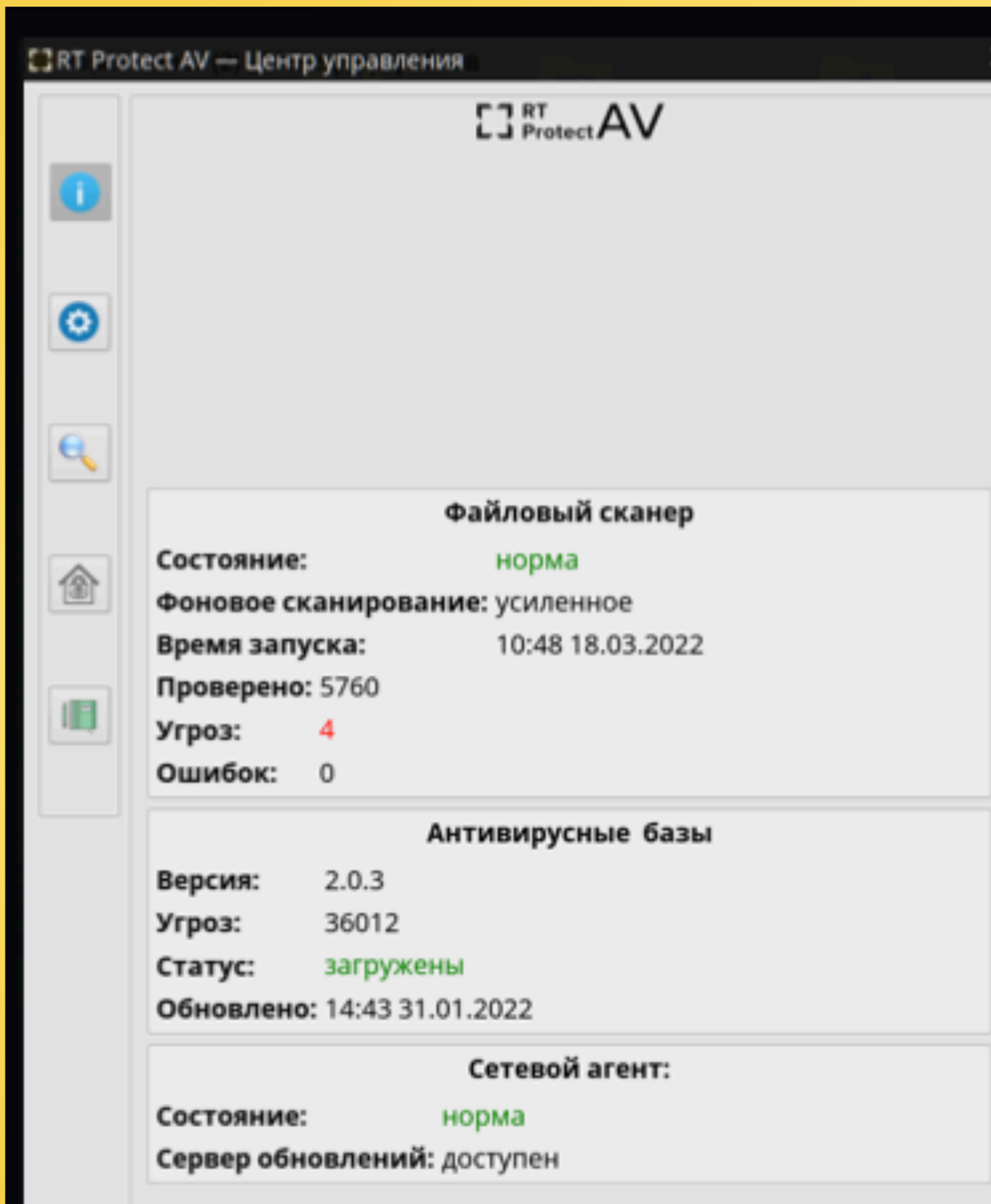
Возможности

Сканирование файловой системы по инициативе пользователя (быстрое, полное, выборочное)

Сканирование активности файловой системы в реальном времени Перехват и блокировка доступа к инфицированным файлам

Поддержка как индивидуального, так и общего карантина Поддержка индивидуальных «белых» списков

Аудит событий безопасности и функционирования



RT
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