RT Protect EDR

Endpoint Detection and Response

Современные тенденции

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

Всё 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

PT
Информационная безопасность

Классические задачи EDR

PT Информационная безопасность

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)

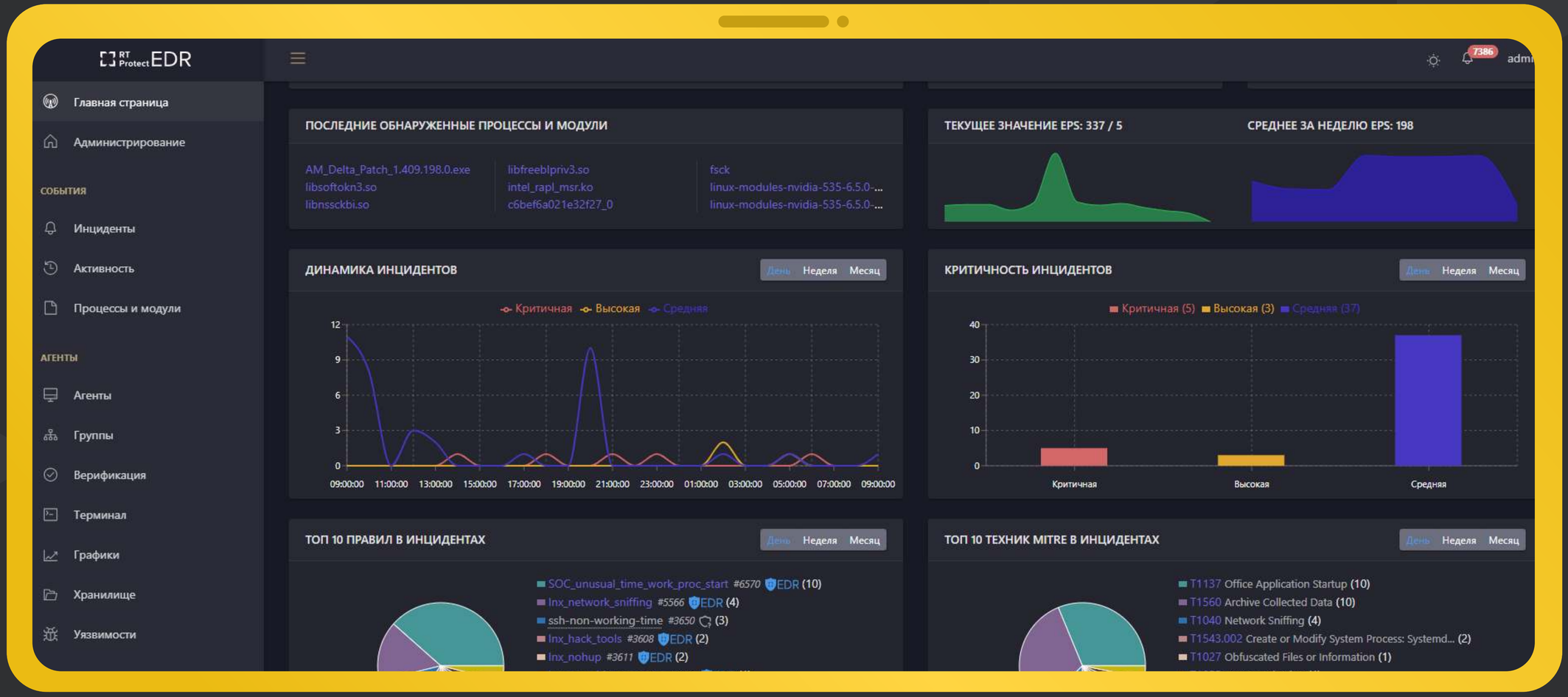
- Скачивание / загрузка / удаление файлов
- Завершение процесса
- Сбор данных
- Изоляция хоста
- Интерактивная консоль
- Запуск процессов / скриптов (bash)
- Антишифровальщик
- Автоматическое блокирование по хешу, имени

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
- Расширять аналитическое обогащение

PT
Информационная безопасность

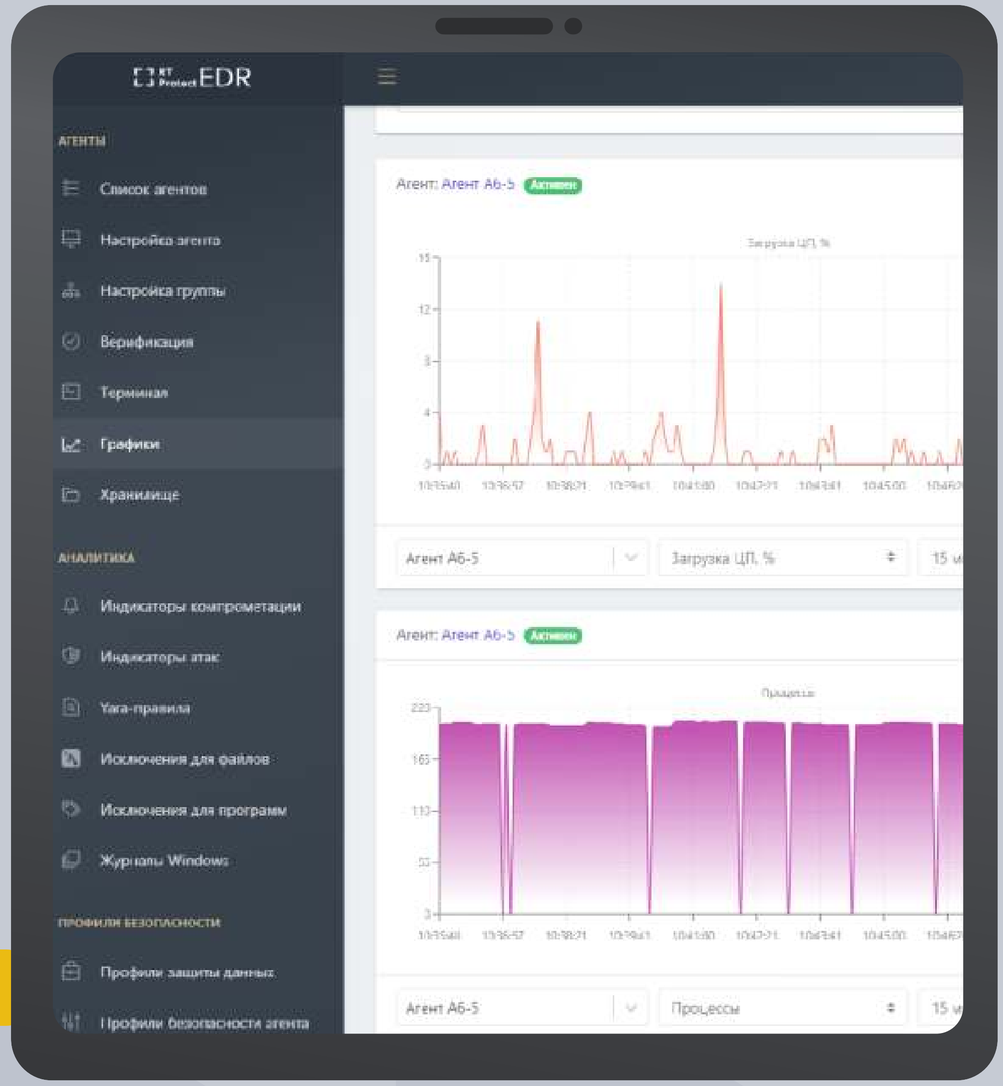
RT Protect EDR - Система обнаружения целенаправленных атак и сложных угроз. Решает все классические задачи и имеет дополнительные модули.



PT
Информационная безопасность

RT Protect EDR

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

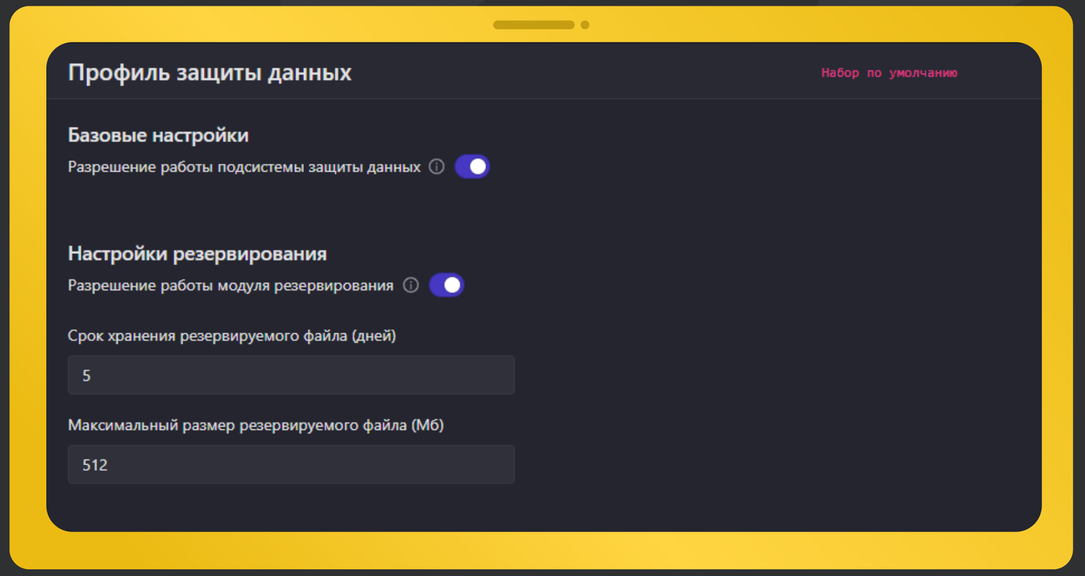


Имеет модуль защиты от вирусов-вымогателей

Отдельный модуль на базе эвристического анализа поведения программ:

реализует защиту от «шифровальщиков» как класса, а не его отдельных представителей

осуществляет прозрачное резервирование пользовательских файлов



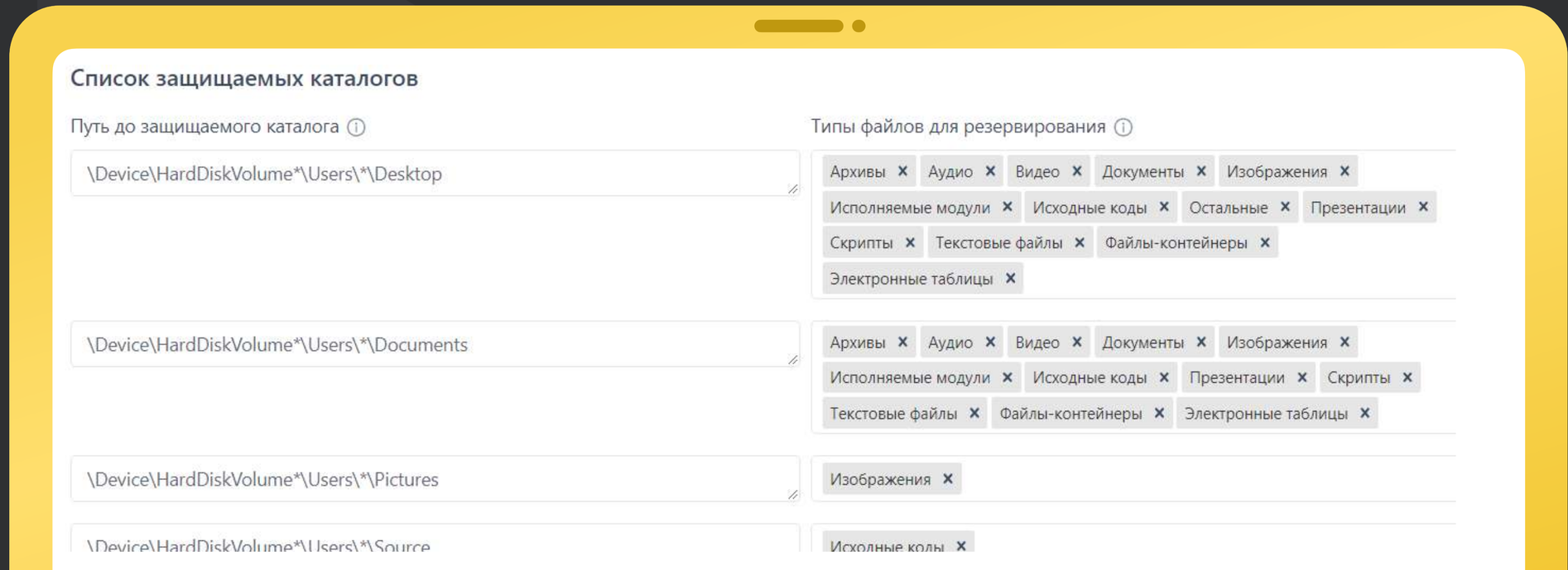
PT
Информационная безопасность

Защита от вирусов-вымогателей

PT
Информационная безопасность

восстанавливает резервируемые файлы в случае утраты

поддерживает все типы файлов и предоставляет возможность гибкой настройки резервирования



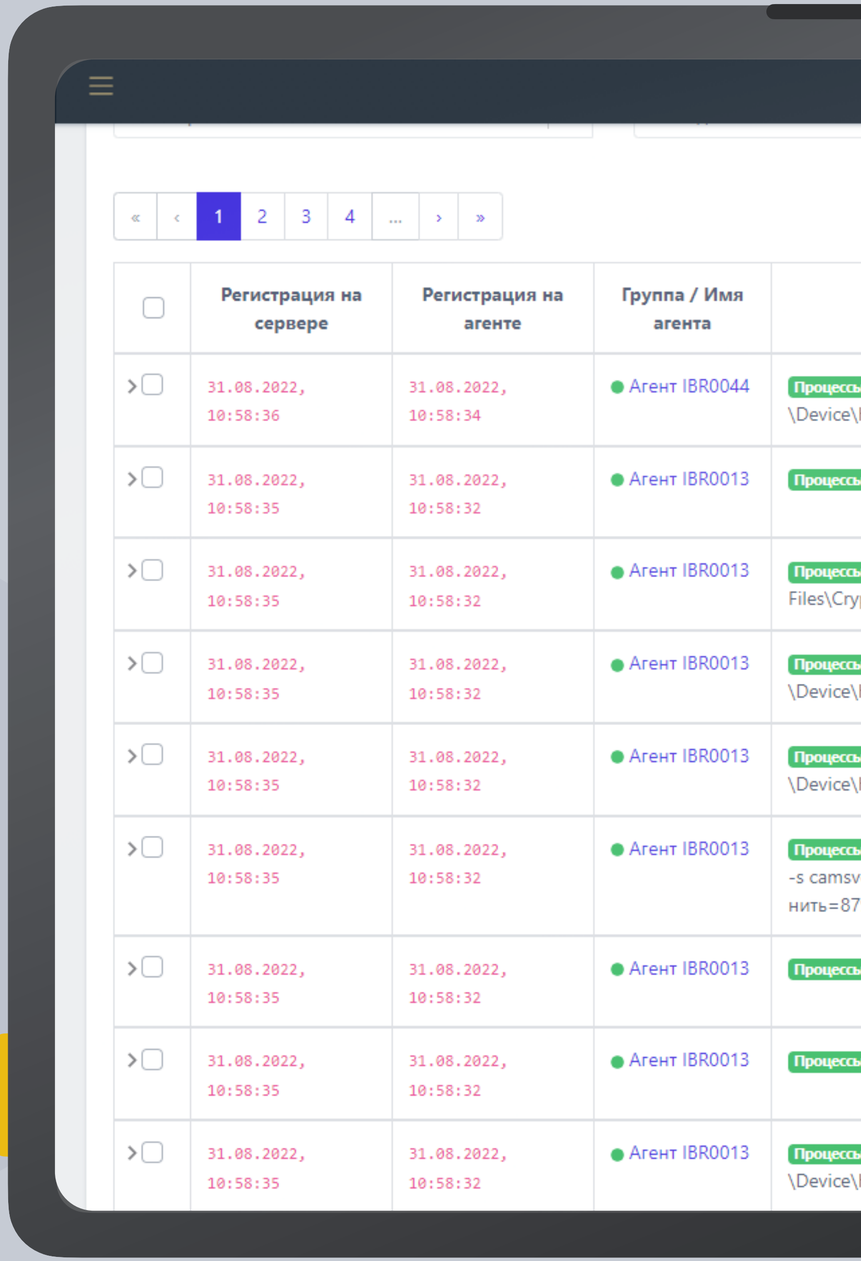
Анализ запускаемых файлов и загружаемых модулей

Анализ всех исполняемых модулей перед загрузкой:

сигнатурный анализ

эвристика

легковесная модель машинного обучения

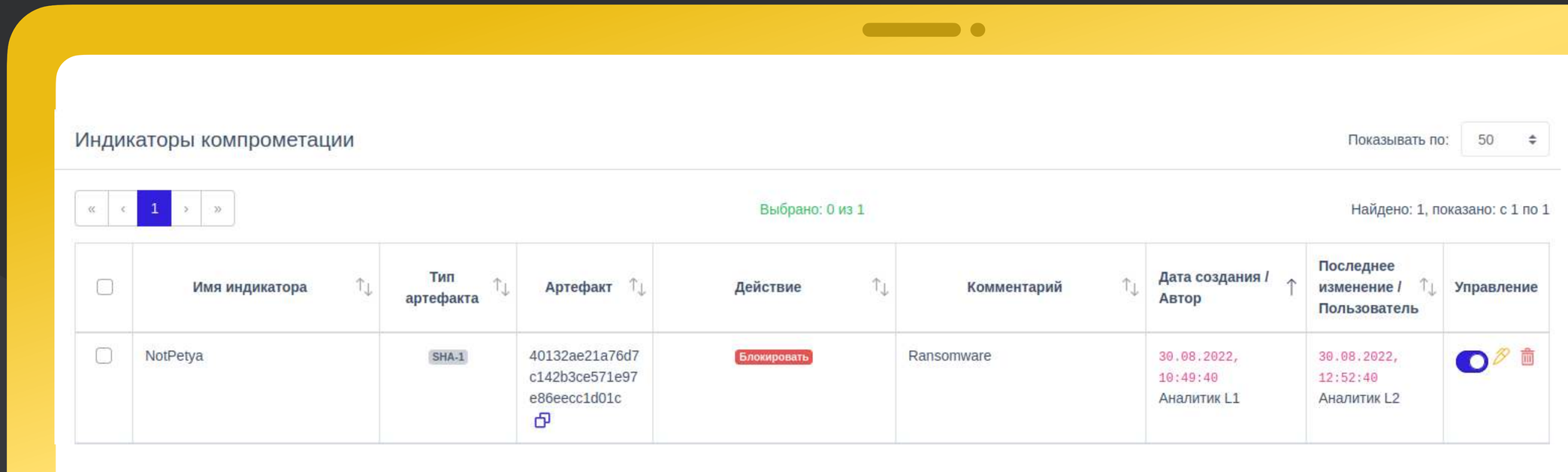


PT
Информационная безопасность

Работа с индикаторами компрометации

Многообразие типов индикаторов компрометации

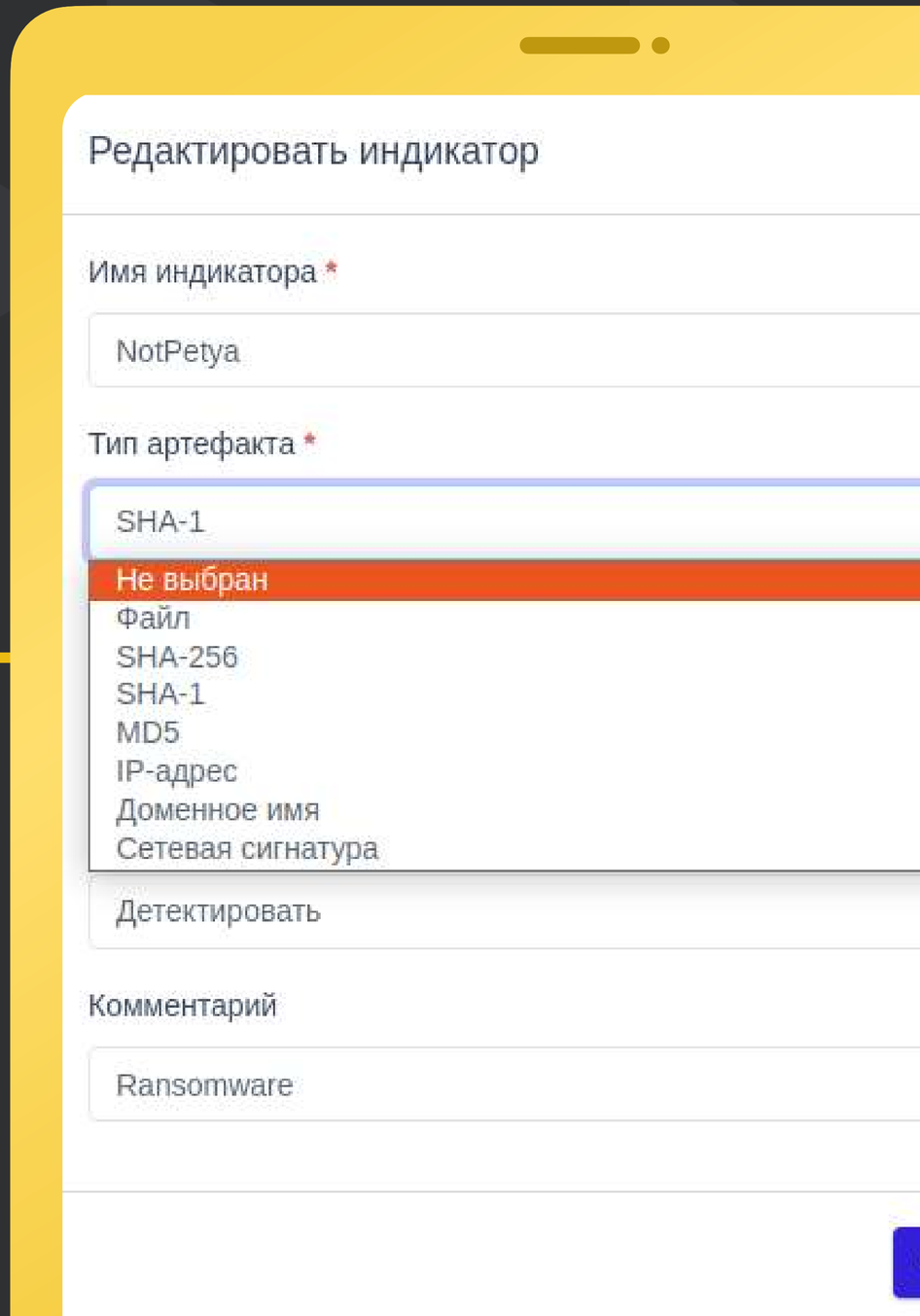
Удобная система управления индикаторами компрометации и их наборами



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

Работающие в режиме реального времени

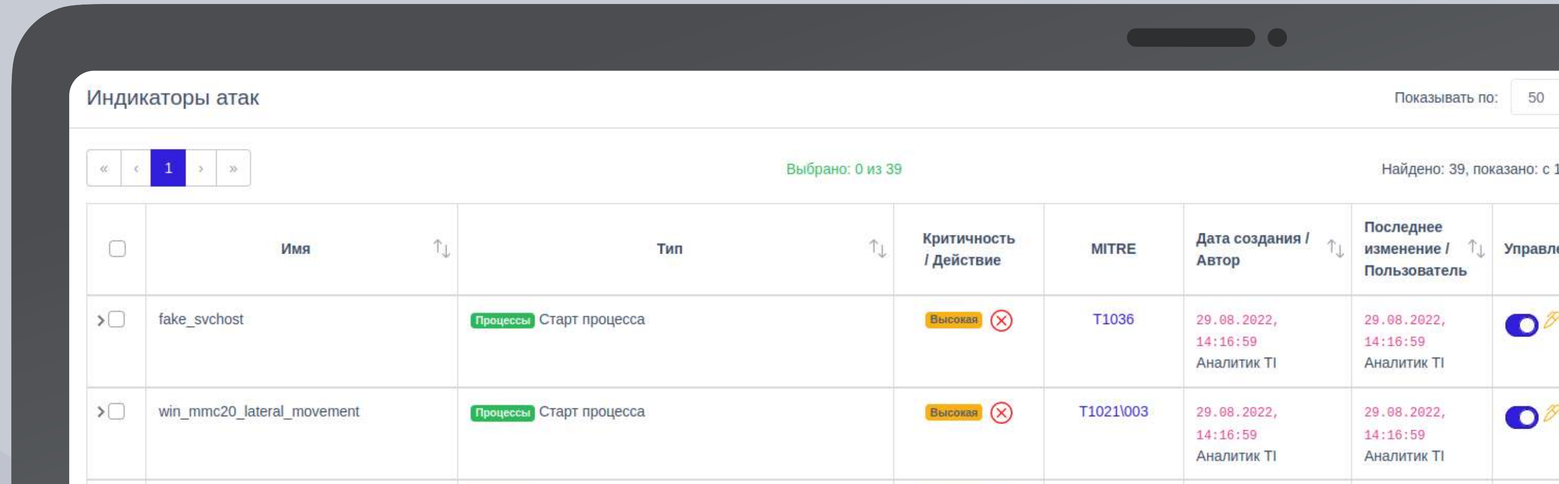
Классификация по матрице MITRE ATT&CK

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

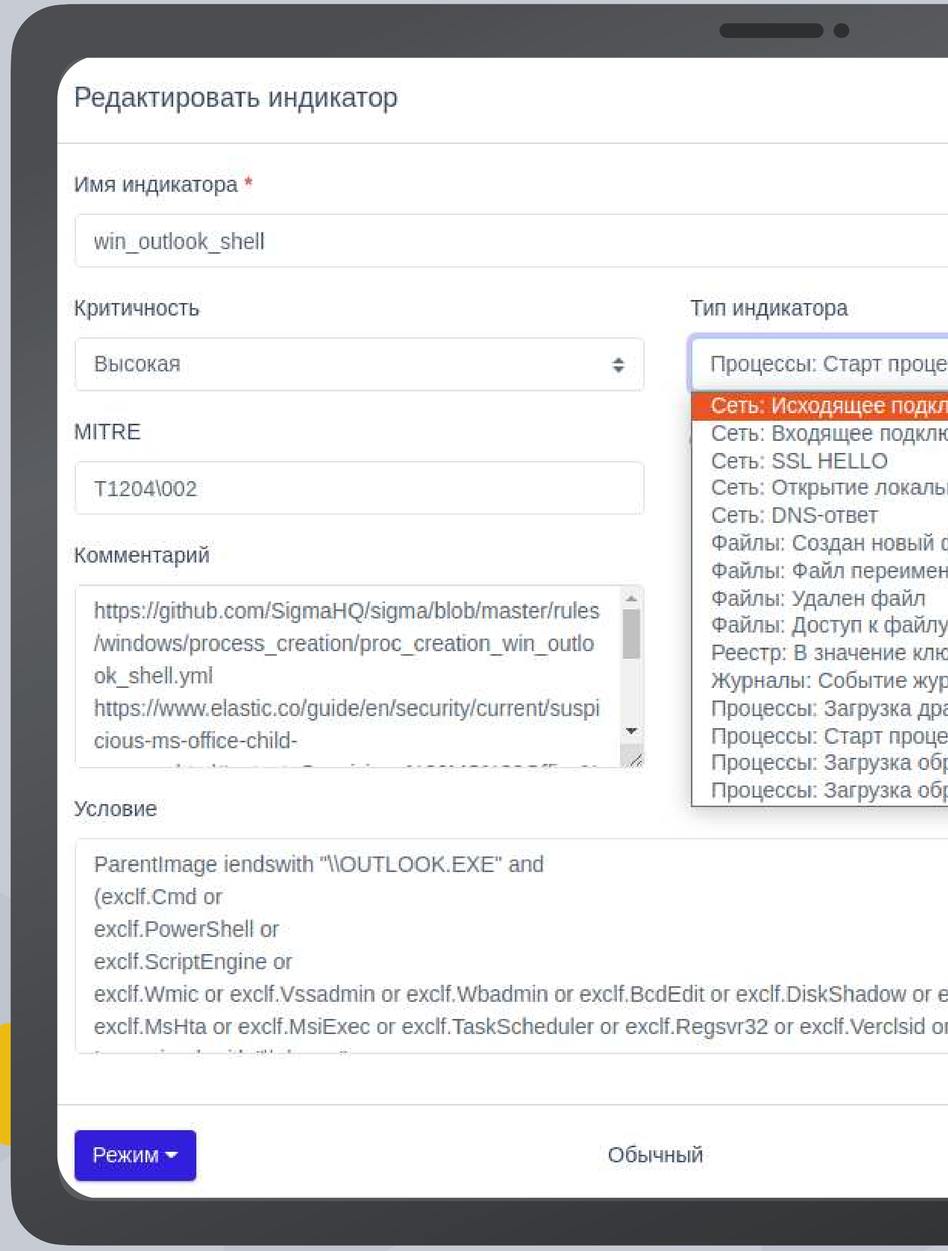


PT
Информационная безопасность

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

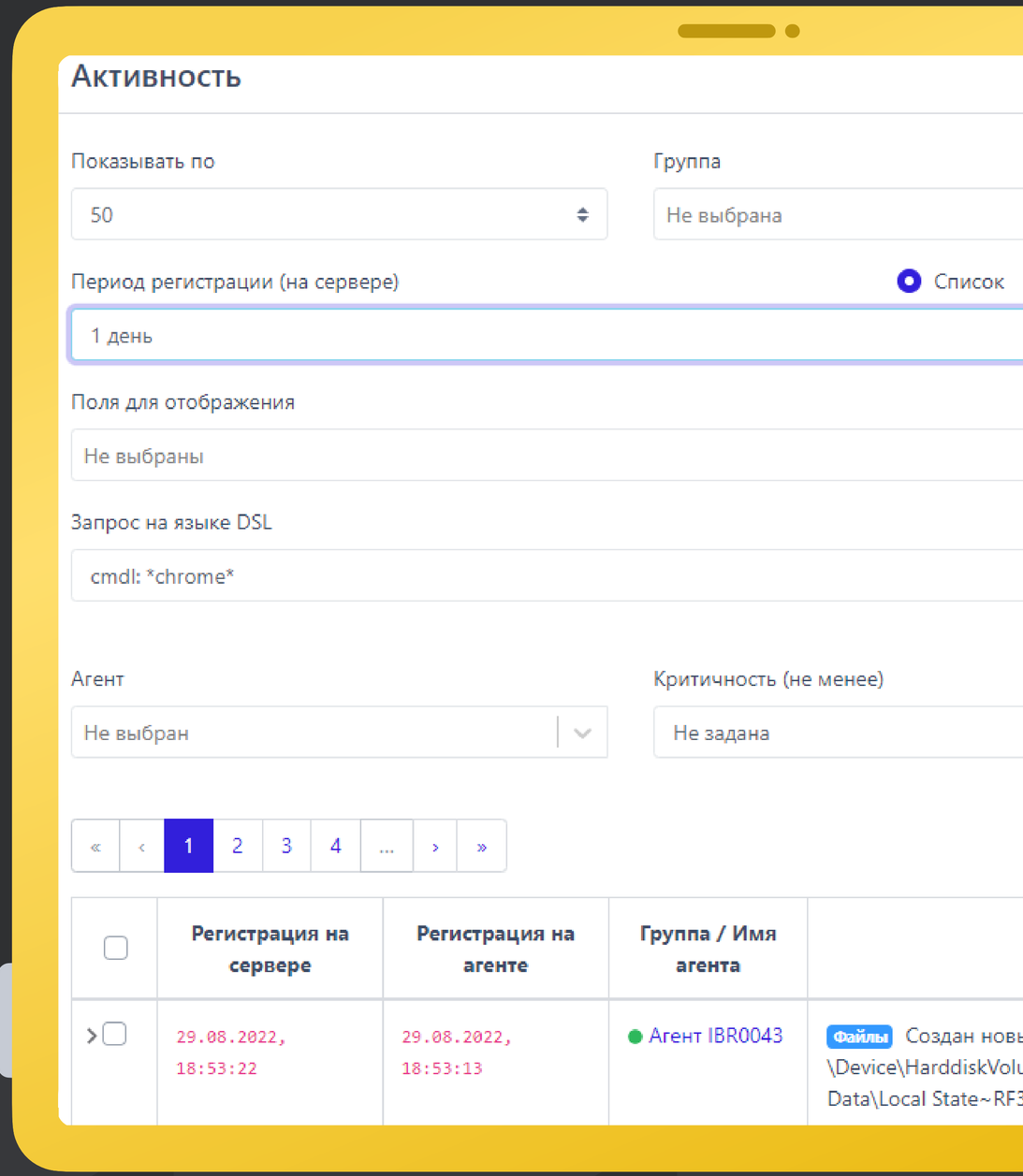
Гибкий поиск угроз

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

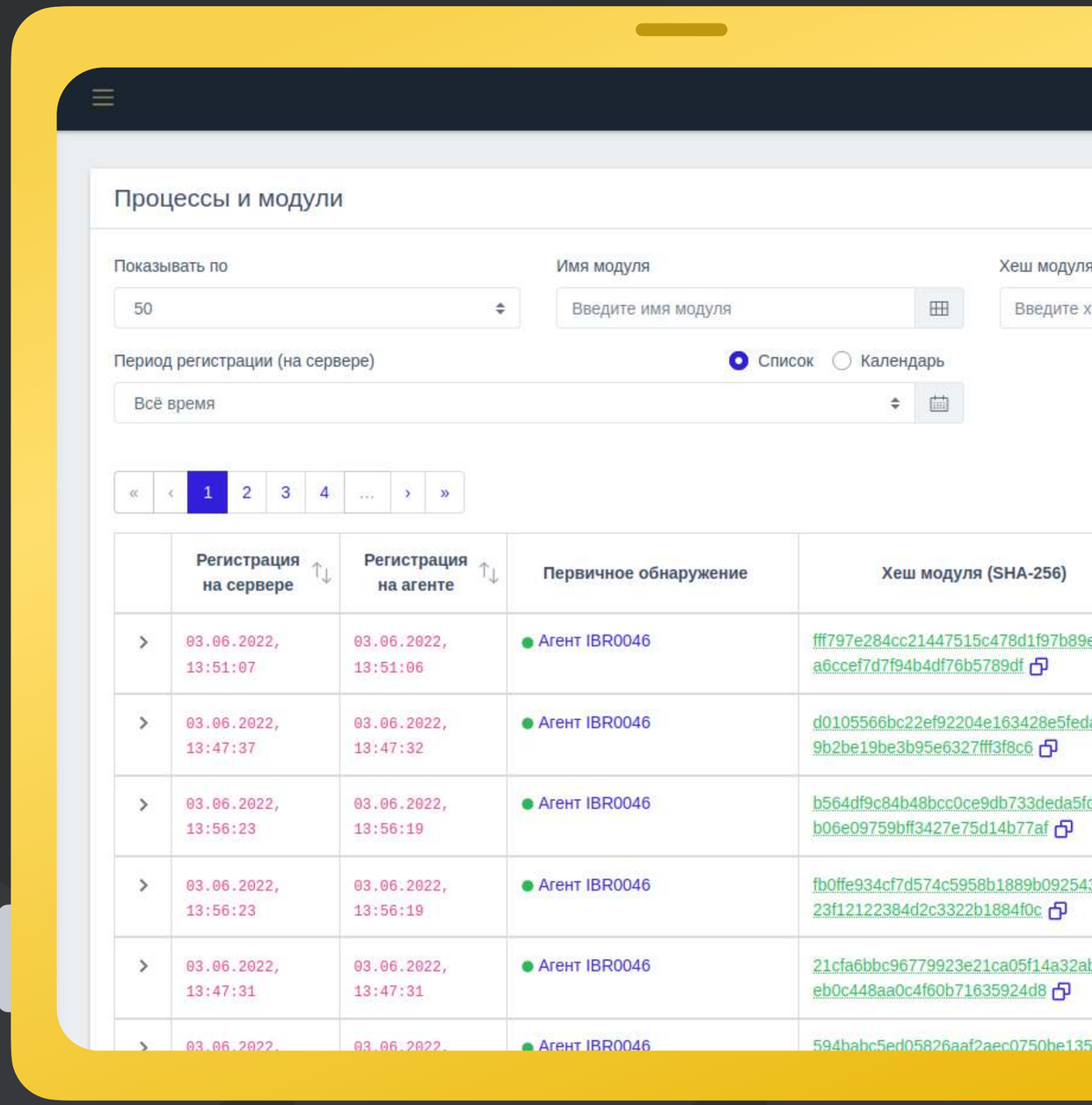


PT
Информационная безопасность

Threat Hunting

Процессы и модули

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

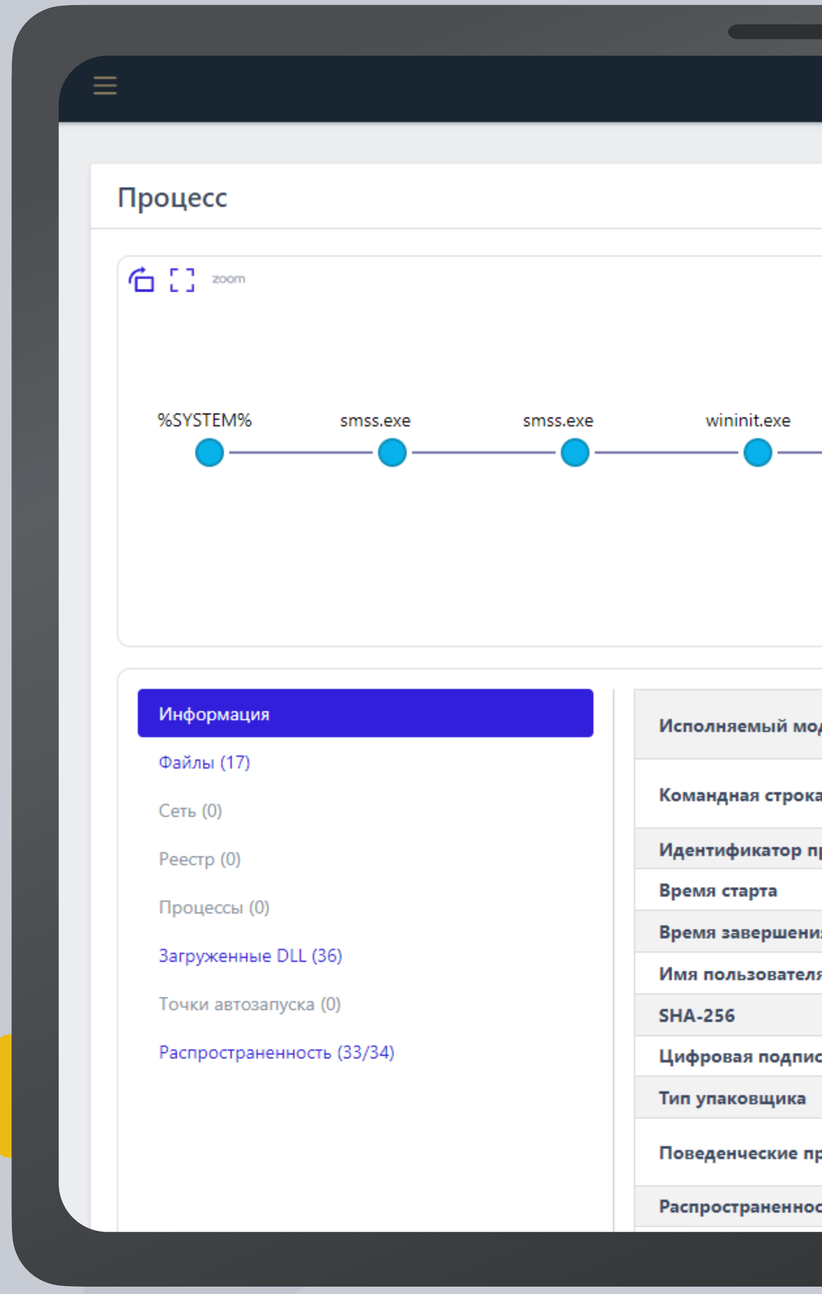


PT
Информационная безопасность

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

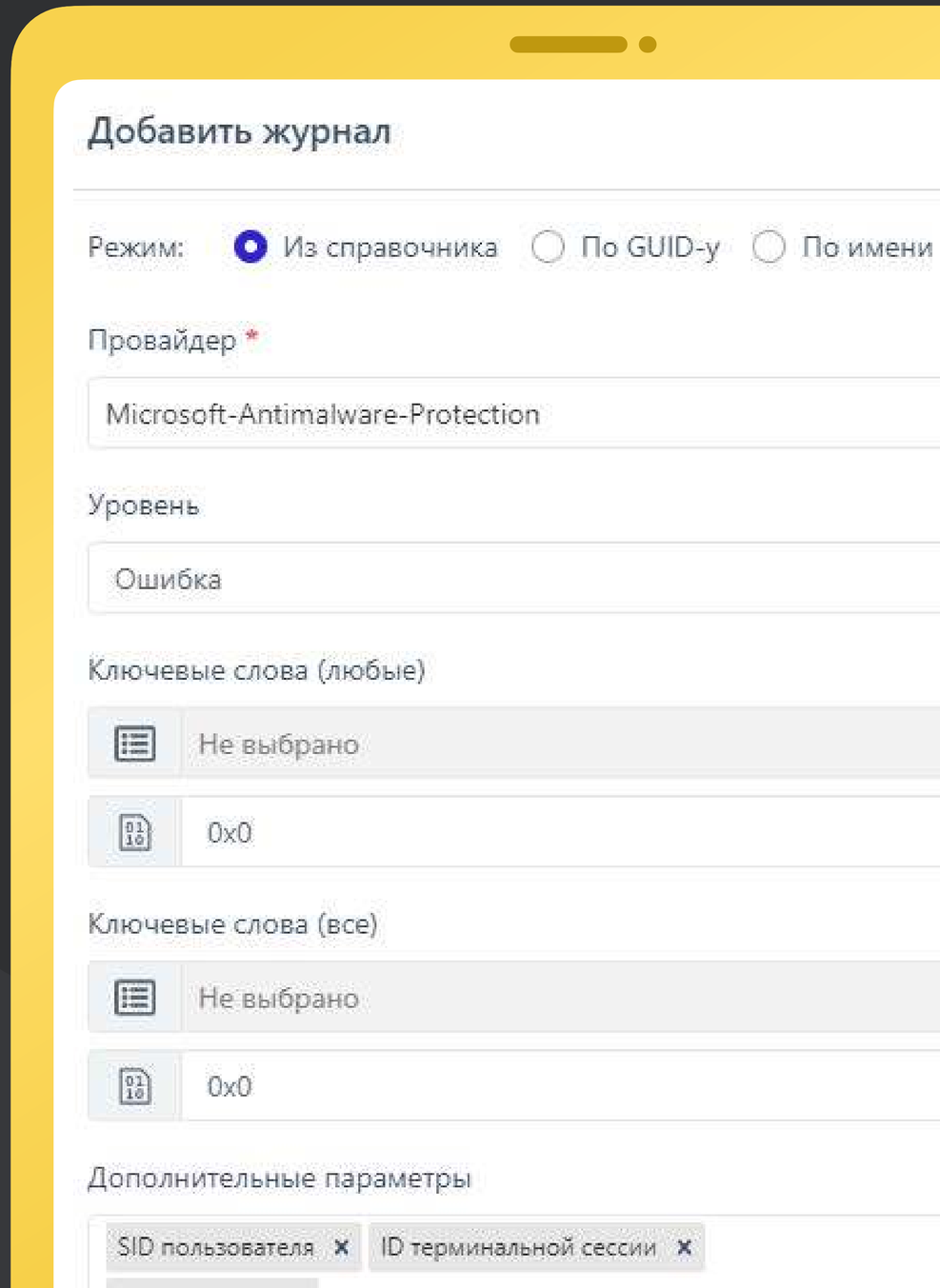


PT
Информационная безопасность

Сбор данных журналов

Взаимодействие с любыми провайдерами журналов Windows

Возможность сбора журналов со средств защиты информации заказчика

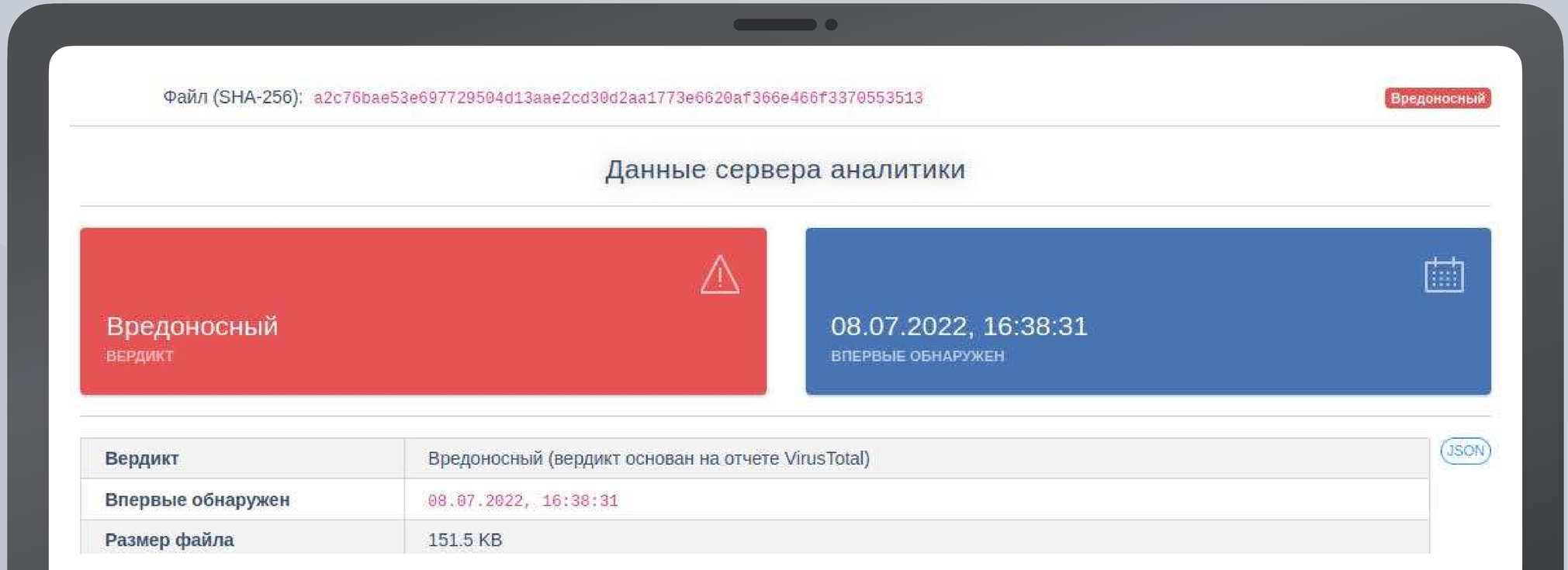


PT
Информационная безопасность

Сервер аналитики (TI portal)

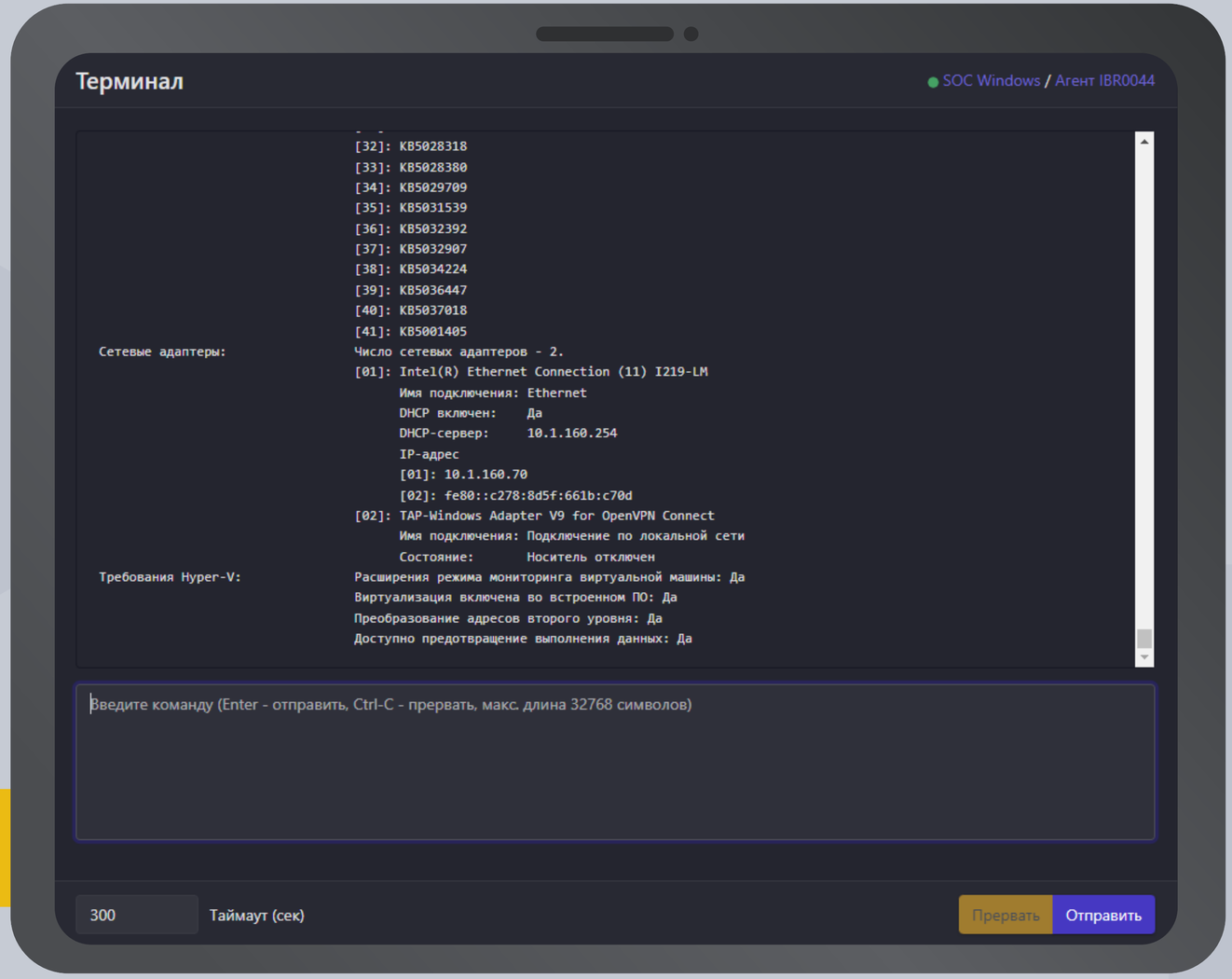
Интеграция с популярными TI решениями

Регулярное обновление наборов индикаторов компрометации



PT
Информационная безопасность

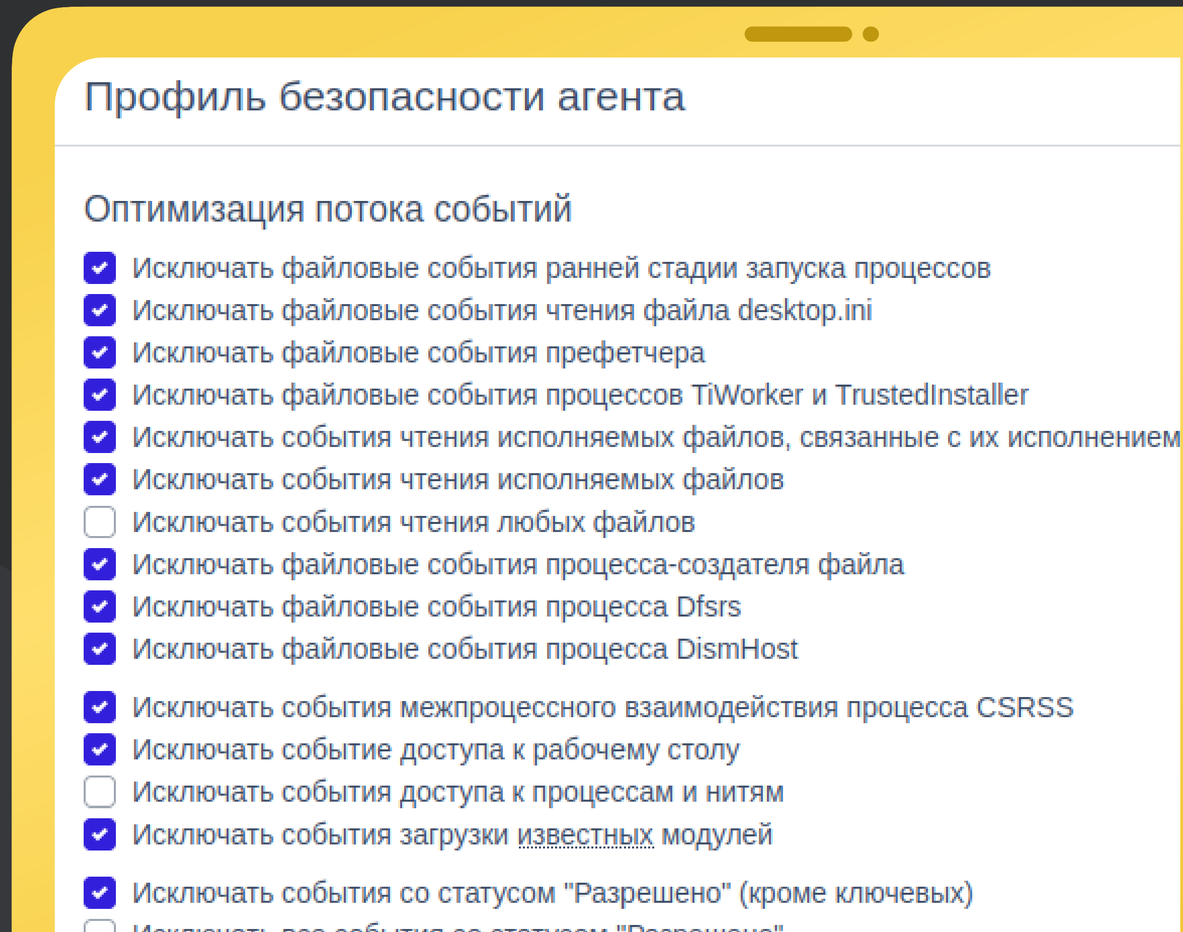
Терминал удалённого доступа



Профиль безопасности агента

Гибкая настройка сбора событий для отправки на сервер

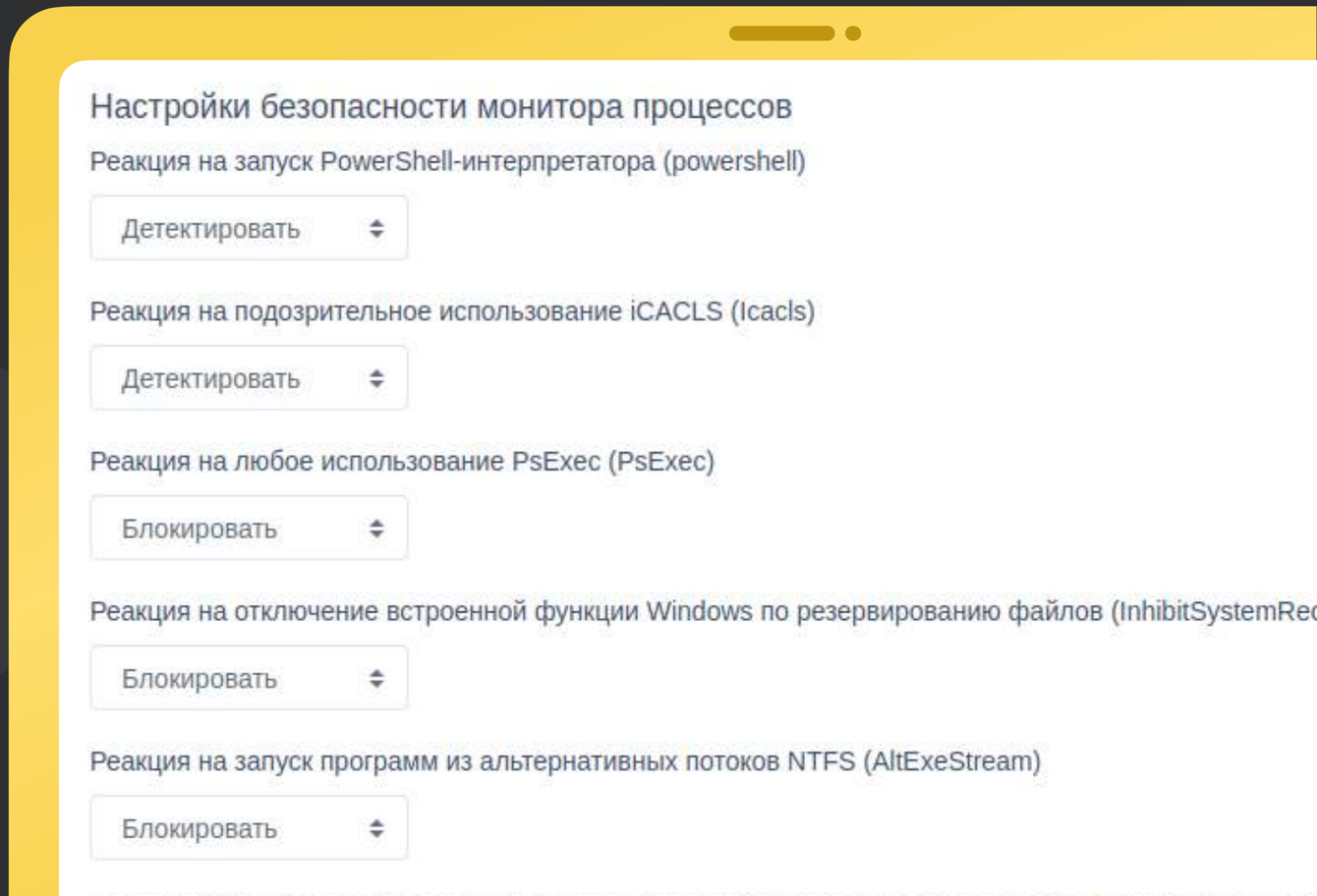
Персонализированный подход конфигурирования агентов для разных типов профилей защиты



PT
Информационная безопасность

Профиль безопасности агента

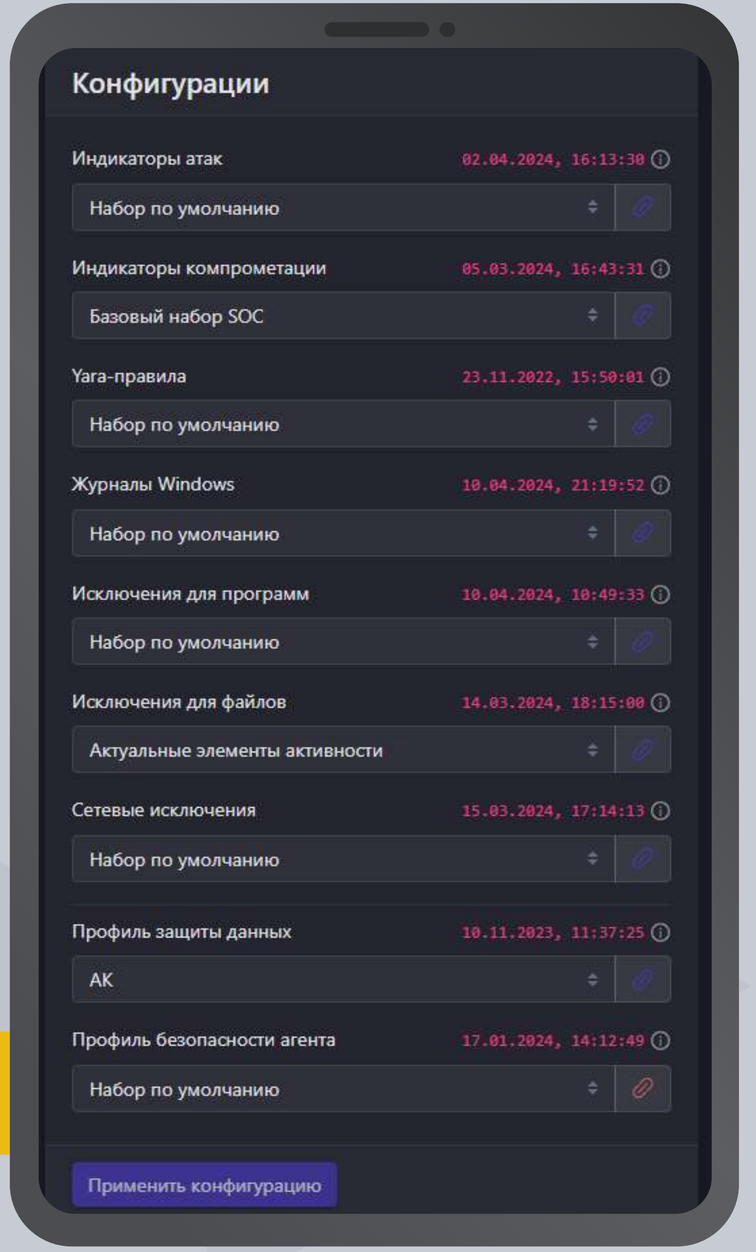
Удобная система распространения профилей безопасности агентов



PT
Информационная безопасность

Настройка профиля безопасности агента

Обилие тонких настроек позволяет создавать эффективные профили безопасности



PT
Информационная безопасность

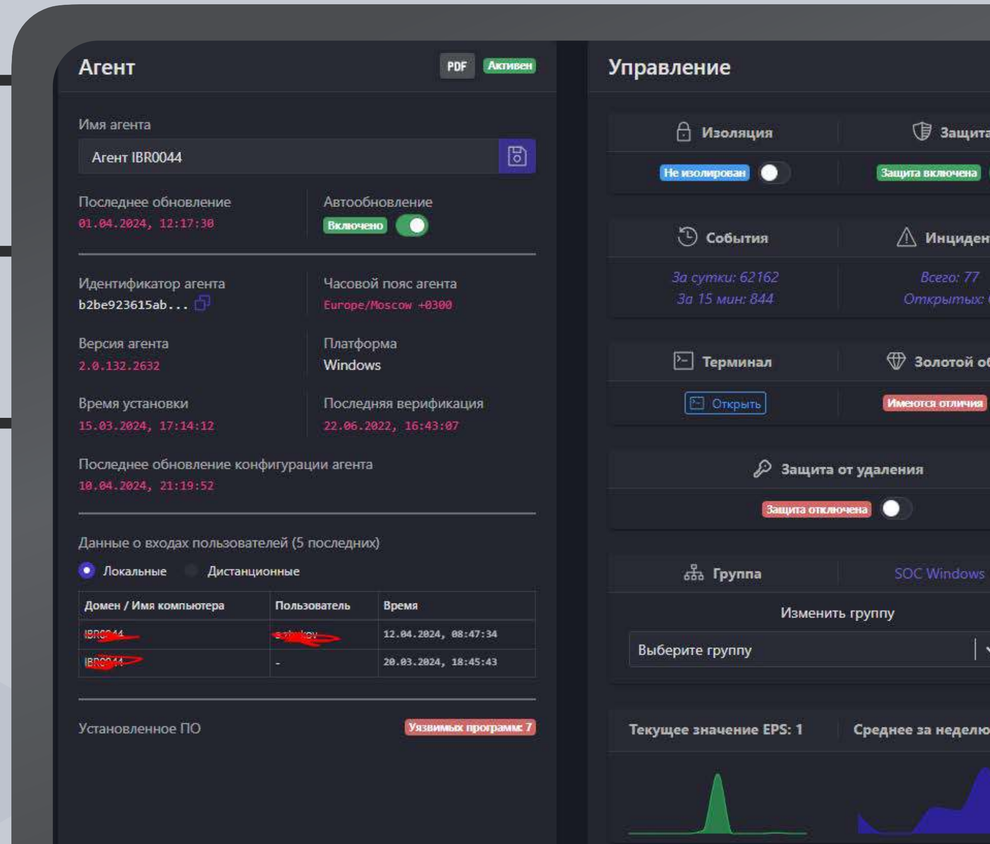
Удаленное управление агентами

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



Модуль управления уязвимостями

PT
Информационная безопасность

Планы развития на 2024 год

Апрель 2024

- Поддержка новых версий ядра ОС Linux
- Добавлен новый тип IoC - URL

Май 2024

- Сканирование памяти и дампы интересующих образов

Июнь 2024

- Поддержка ОС CentOS
- Расширение встроенных правил атак на DC

Сентябрь 2024

- Контроль USB устройств
- Поддержка хэша типа Imphash

Ноябрь 2024

- Расширение механизма файловых исключений, добавления возможности управления телеметрией

Декабрь 2024

- Интеграция с дополнительными решениями класса SandBOX
- Реализация технологии «File Vantage»

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