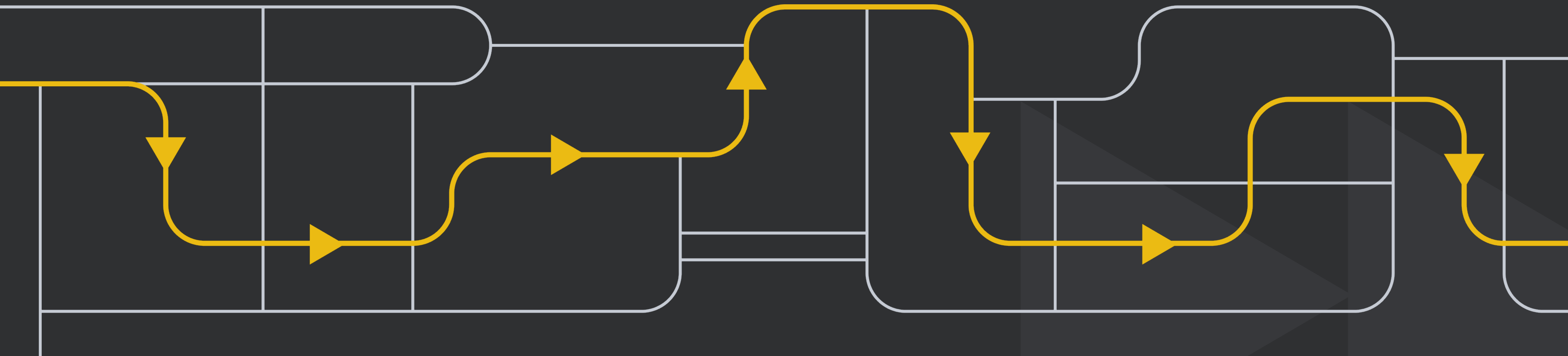


^{RT} Protect EDR

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.

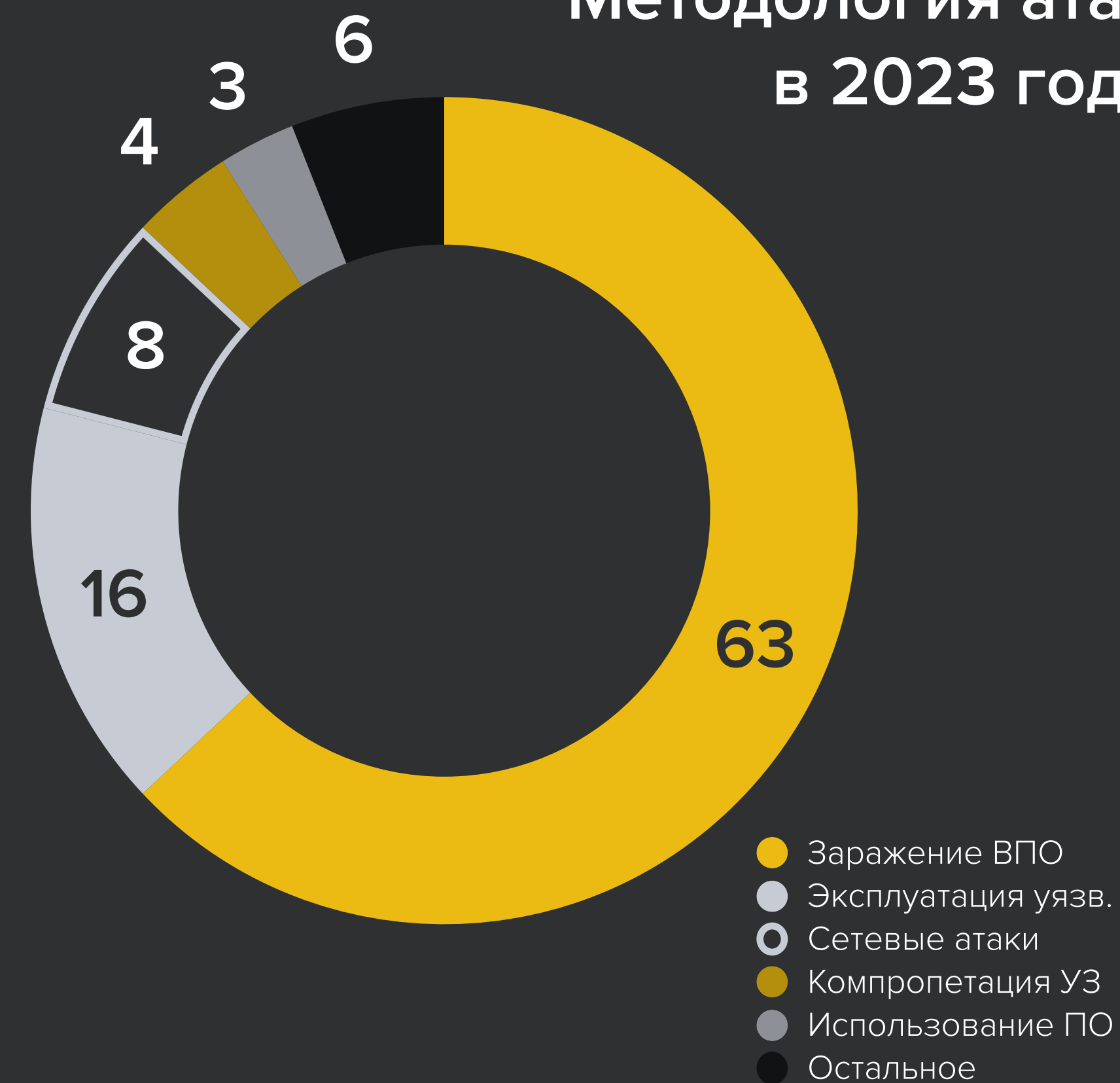
Увеличение количества атак на
госучреждения практически

в 2,5 раза

по сравнению с данными 2022 года.

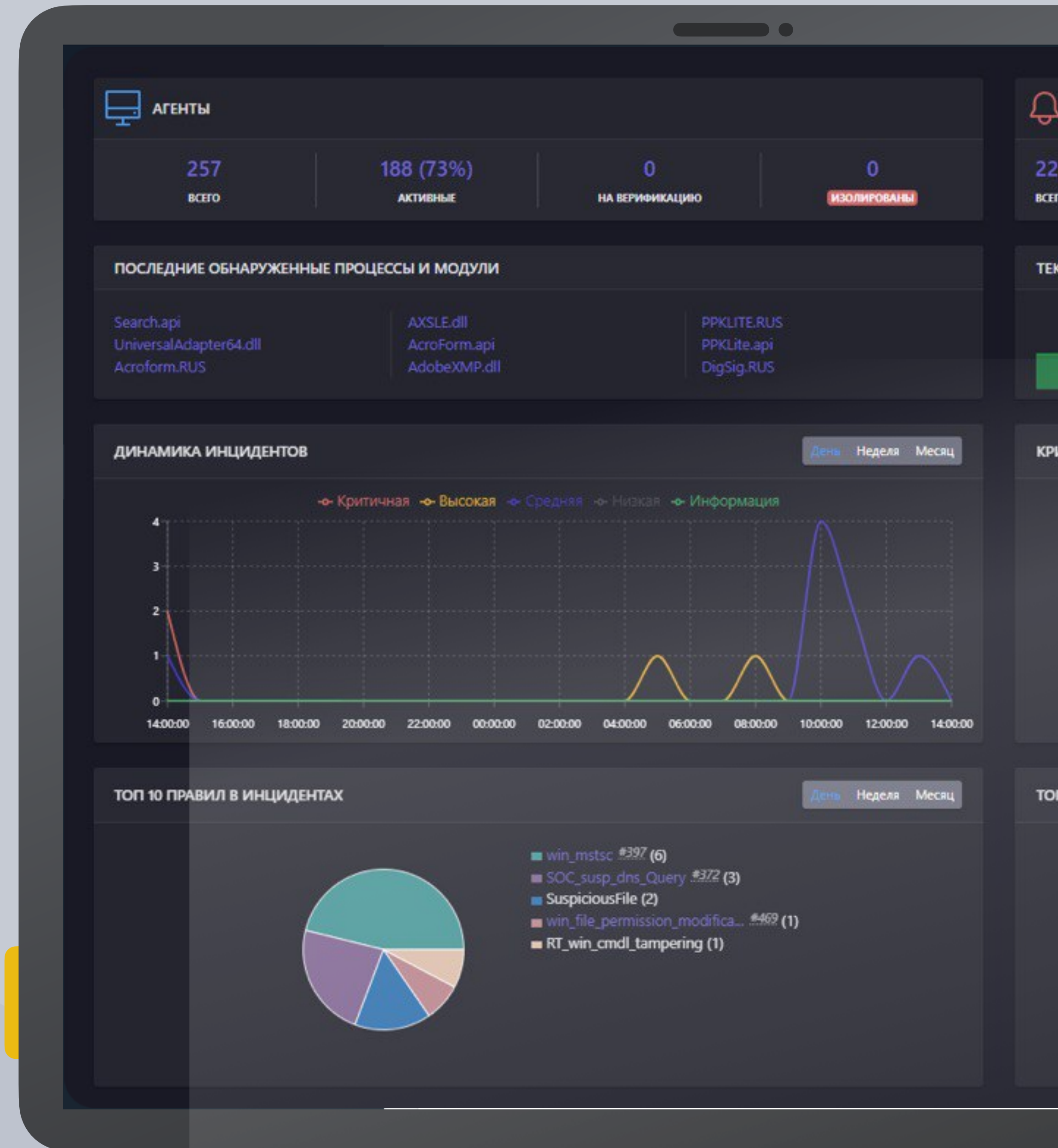
RT Protect EDR - актуальное
средство защиты ИБ,
отразившее 100% атак на
Киберполигоне 2022

Методология атак
в 2023 году



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.

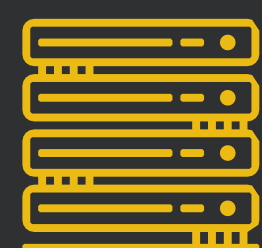


Защита от вирусов-вымогателей

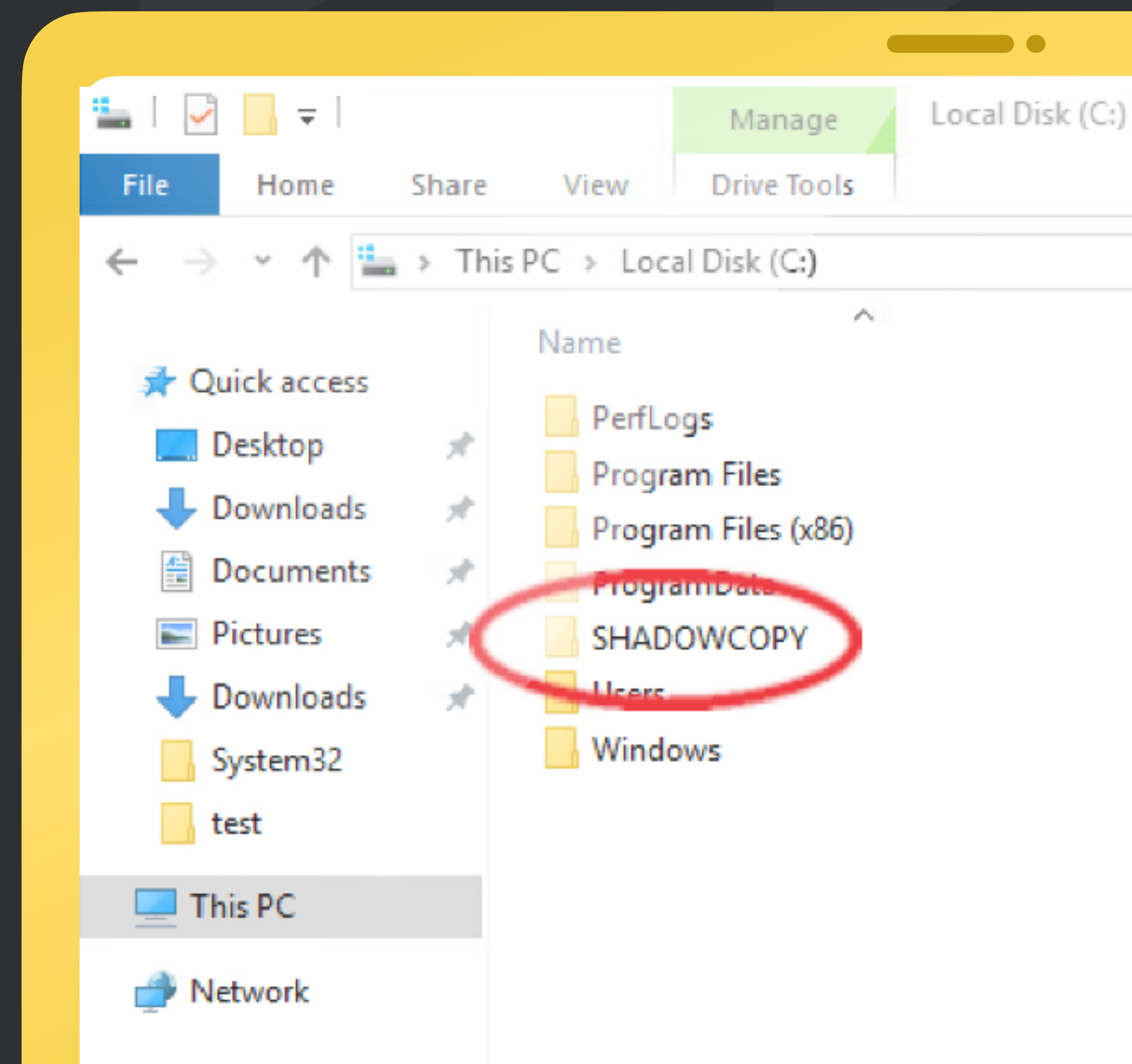
Отдельный модуль на базе эвристического анализа поведения программ:



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



осуществляет прозрачное резервирование пользовательских файлов



Защита от вирусов-вымогателей



восстанавливает резервируемые файлы в случае утраты



поддерживает все типы файлов и предоставляет возможность гибкой настройки резервирования



PT

Информационная
безопасность

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

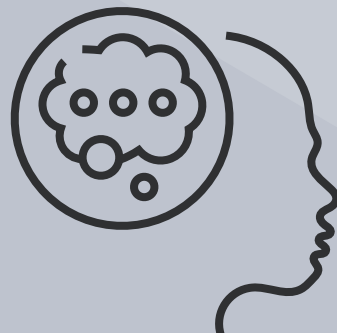
Исходные коды x

Анализ запускаемых файлов и загружаемых модулей

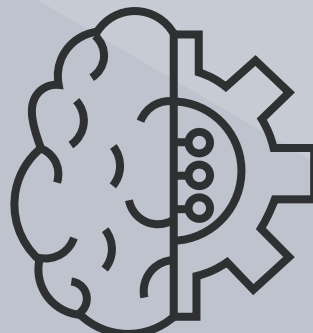
Анализ всех исполняемых модулей перед загрузкой:



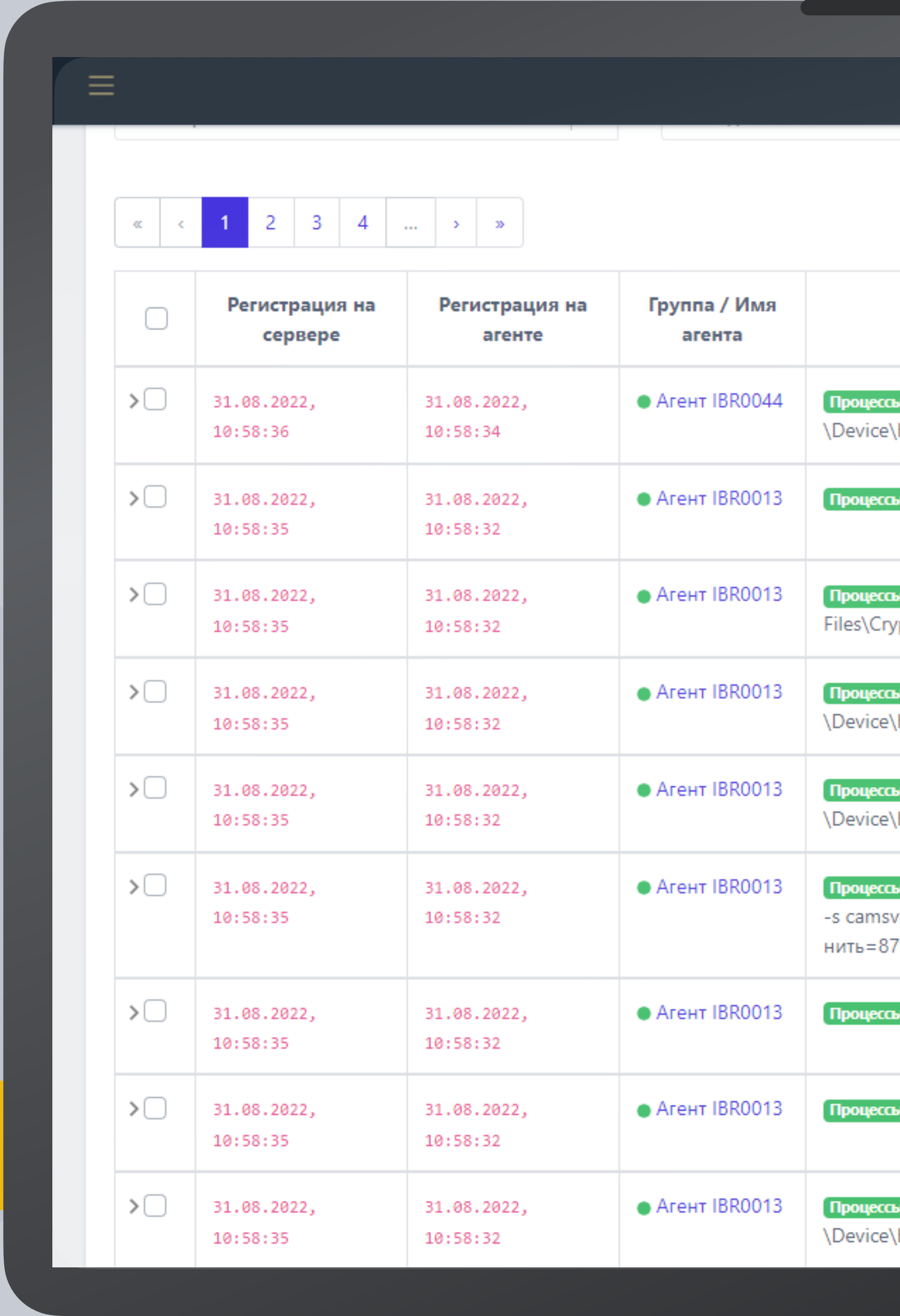
сигнатурный анализ



эвристика



легковесная модель машинного обучения



☐	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	
> ☐	31.08.2022, 10:58:36	31.08.2022, 10:58:34	● Агент IBR0044	Процесс \Device\
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс Files\Cry
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс \Device\
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс \Device\
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс -s camsv нить=87
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс
> ☐	31.08.2022, 10:58:35	31.08.2022, 10:58:32	● Агент IBR0013	Процесс \Device\

Индикаторы компрометации

 Многообразие типов индикаторов компрометации

 Удобная система управления индикаторами компрометации и их наборами

Индикаторы компрометации							
« < 1 > »				Выбрано: 0 из 1			
☐	Имя индикатора ↑↓	Тип артефакта ↑↓	Артефакт ↑↓	Действие ↑↓	Комментарий ↑↓	Дата создания / Автор ↑	Последнее изменение / Пользователь
☐	NotPetya	SHA-1	40132ae21a76d7c142b3ce571e97e86eecc1d01c 	Блокировать	Ransomware	30.08.2022, 10:49:40 Аналитик L1	30.08.2022, 12:52:40 Аналитик

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

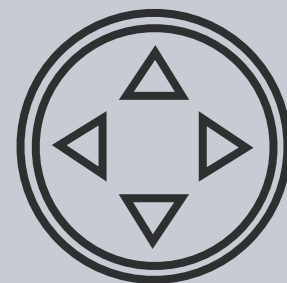
Ransomware

Индикаторы атак

Работающие в режиме реального времени



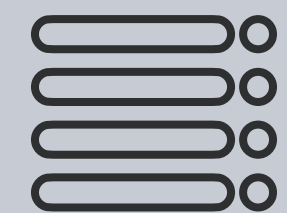
Классификация по матрице MITRE ATT&CK



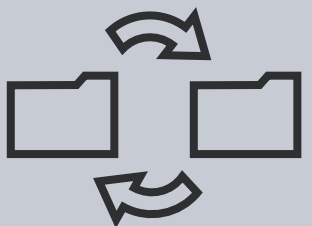
Удобная система управления индикаторами атак и их наборами



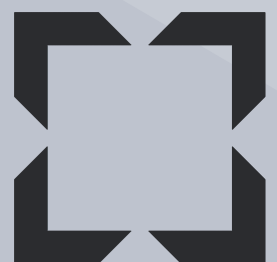
Регулярное обновление специалистами TI



Собственные правила выявления угроз с интуитивно понятным механизмом написания IOA



Конвертер Sigma правил



PT
Информационная
безопасность

> ☐	fake_svchost	Процессы Старт процесса	Высокая
> ☐	win_mmc20_lateral_movement	Процессы Старт процесса	Высокая
> ☐	win_malware_emotet	Процессы Старт процесса	Высокая

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)

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
(exclcf.Cmd or
exclcf.PowerShell or
exclcf.ScriptEngine or
exclcf.Wmic or exclcf.Vssadmin or exclcf.Wbadmin or exclcf.BcdEdit or exclcf.DiskShadow or
exclcf.MsHta or exclcf.MsiExec or exclcf.TaskScheduler or exclcf.Regsvr32 or exclcf.Verclsid o

Тип индикатора

Процессы: Старт проце
Сеть: Исходящее подкл
Сеть: Входящее подкл
Сеть: SSL HELLO
Сеть: Открытие локаль
Сеть: DNS-ответ
Файлы: Создан новый
Файлы: Файл переимен
Файлы: Удален файл
Файлы: Доступ к файлу
Реестр: В значение кл
Журналы: Событие жу
Процессы: Загрузка др
Процессы: Старт проце
Процессы: Загрузка об
Процессы: Загрузка об

Режим ▾

Обычный

Threat Hunting



Гибкий поиск угроз по событиям EDR



Аналитика по поведенческим признакам

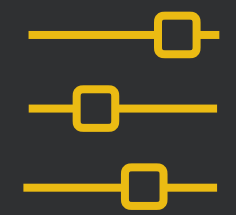
Время регистрации события (UTC)	29.08.2022, 18:47:05
Тип события	Файлы
Подтип события	Удален файл
Критичность (уровень важности) события	Информация
Агент	Агент IBR0038
Уникальный идентификатор агента	1d7e14463ec2fb8e10b931fa07e9ff517e
Полное имя исполняемого модуля процесса	\\Device\\HarddiskVolume3\\Program 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



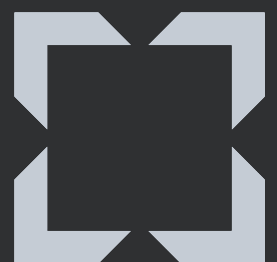
Быстрый и удобный поиск угроз в корпоративной сети по событиям EDR



Настраиваемая фильтрация событий по различным параметрам



Возможность использования языка DSL для продвинутой фильтрации



PT
Информационная
безопасность

Активность

Показывать по

50

Группа

Не выбрана

Период регистрации (на сервере)

1 день

☒ Список ☐ Календарь

Поля для отображения

Не выбраны

Запрос на языке DSL

cmdl: *chrome*

Агент

Не выбран

Критичность (не менее)

Не задана

« < 1 2 3 4 ... > »

☐	Регистрация на сервере	Регистрация на агенте	Группа / Имя агента	
☒	29.08.2022, 18:53:22	29.08.2022, 18:53:13	● Агент IBR0043	Файлы Создан новый файл \\Device\\HarddiskVolume3\\ Data\\Local State~RF3dc25

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

Имя модуля

Хеш модуля (SHA-256)

50

Введите имя модуля

Введите хеш

Период регистрации (на сервере)

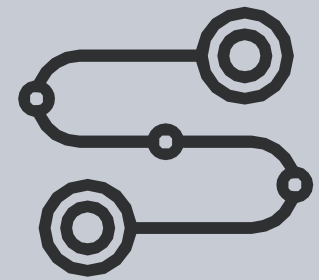
Список Календарь

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	fff797e284cc21447515c478d1f97b89efb2a49a6cce7d7f94b4df76b5789df	vcrun...
>	03.06.2022, 13:47:37	03.06.2022, 13:47:32	● Агент IBR0046	d0105566bc22ef92204e163428e5feda866f8a9b2be19be3b95e6327fff3f8c6	ngen...
>	03.06.2022, 13:56:23	03.06.2022, 13:56:19	● Агент IBR0046	b564df9c84b48bcc0ce9db733deda5fd35c22b06e09759bff3427e75d14b77af	Unity...
>	03.06.2022, 13:56:23	03.06.2022, 13:56:19	● Агент IBR0046	fb0ffe934cf7d574c5958b1889b0925430e04523f12122384d2c3322b1884f0c	concr...
>	03.06.2022, 13:47:31	03.06.2022, 13:47:31	● Агент IBR0046	21cfa6bbc96779923e21ca05f14a32ab24cf45eb0c448aa0c4f60b71635924d8	ngen...
>	03.06.2022, 13:56:23	03.06.2022, 13:56:19	● Агент IBR0046	594bab5ed05826aaf2aec0750be135eff2876c9b941d2e99b6b1e278073c96a	vccor...
>	09.06.2022, 09:48:20	09.06.2022, 09:48:20	● Агент IBR0043	9cac8297b2fcdcfb8886ce9e4282f0720119d3235fe91b344052e27153325d325	OneS...er.dll

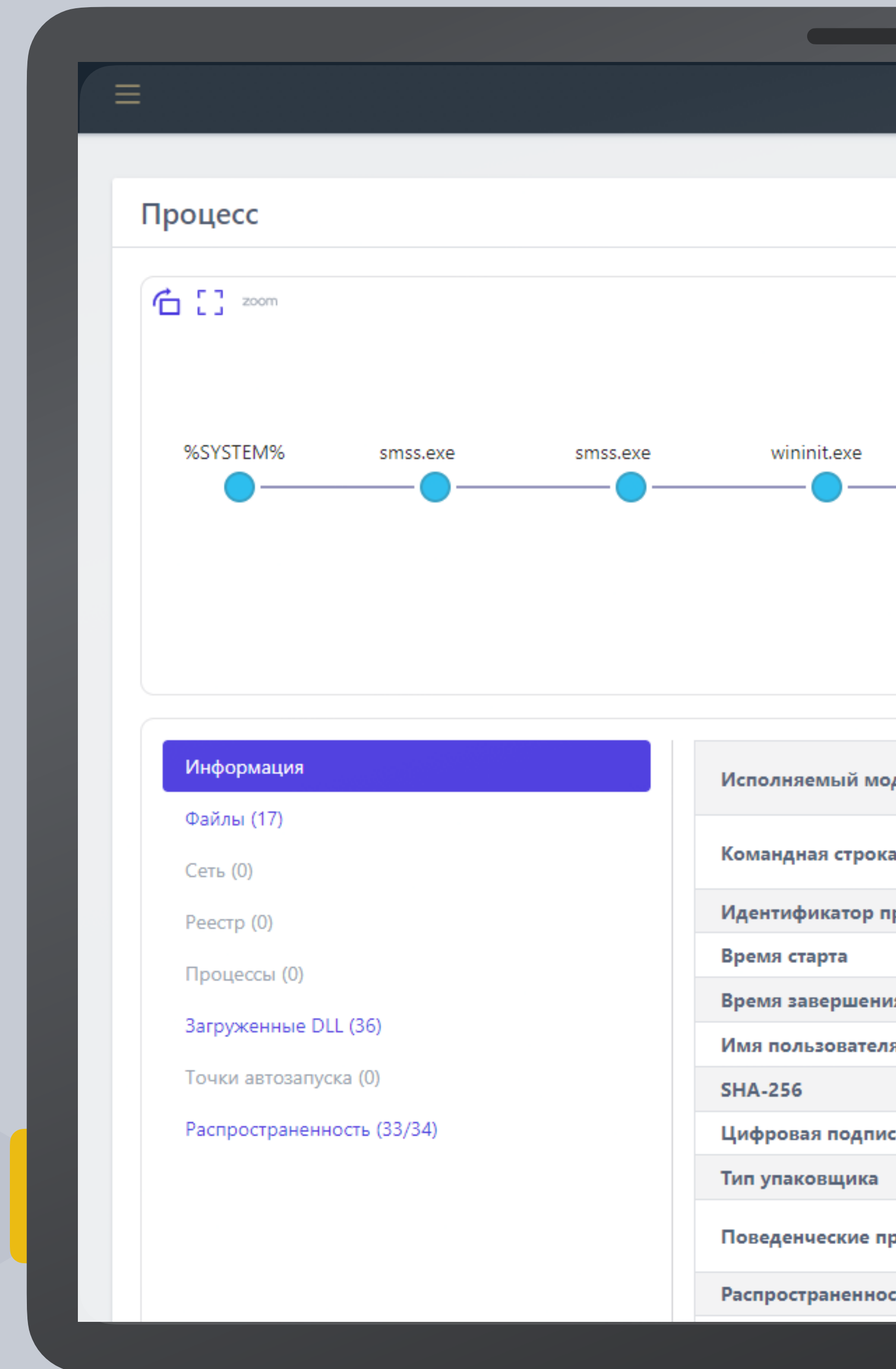
Богатый инструментарий расследований инцидентов



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



сведения о распространенности подозрительных исполняемых модулей в агентской сети



Сбор данных журналов



Взаимодействие с любыми провайдерами журналов Windows



Возможность сбора журналов со средств защиты информации заказчика

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)

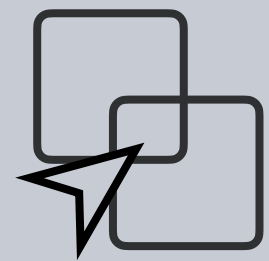
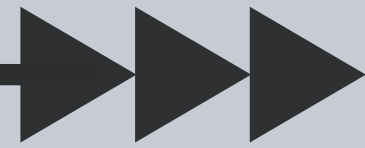
 Не выбрано

 0x0

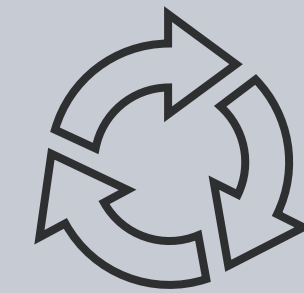
Дополнительные параметры

SID пользователя x ID терминальной сессии x

Сервер аналитики (TI portal)



Интеграция с популярными TI решениями



Регулярное обновление наборов индикаторов компрометации



PT
Информационная
безопасность

Файл (SHA-256): `a2c76bae53e697729504d13aae2cd30d2aa1773e6620af366e466f3370553513`

Вредоносный

Данные сервера аналитики

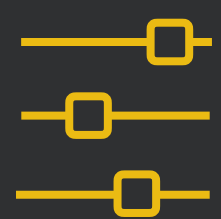
Вредоносный
ВЕРДИКТ

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
SHA-256	a2c76bae53e697729504d13aae2cd30d2aa1773e6620af366e466f3370553513

JSON

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 (Icacs)

Детектировать

Реакция на любое использование PsExec (PsExec)

Блокировать

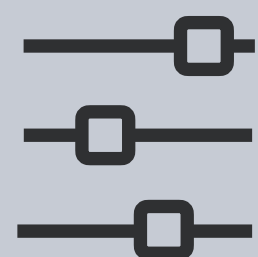
Реакция на отключение встроенной функции Windows по резервированию файлов (InhibitSystemReco

Блокировать

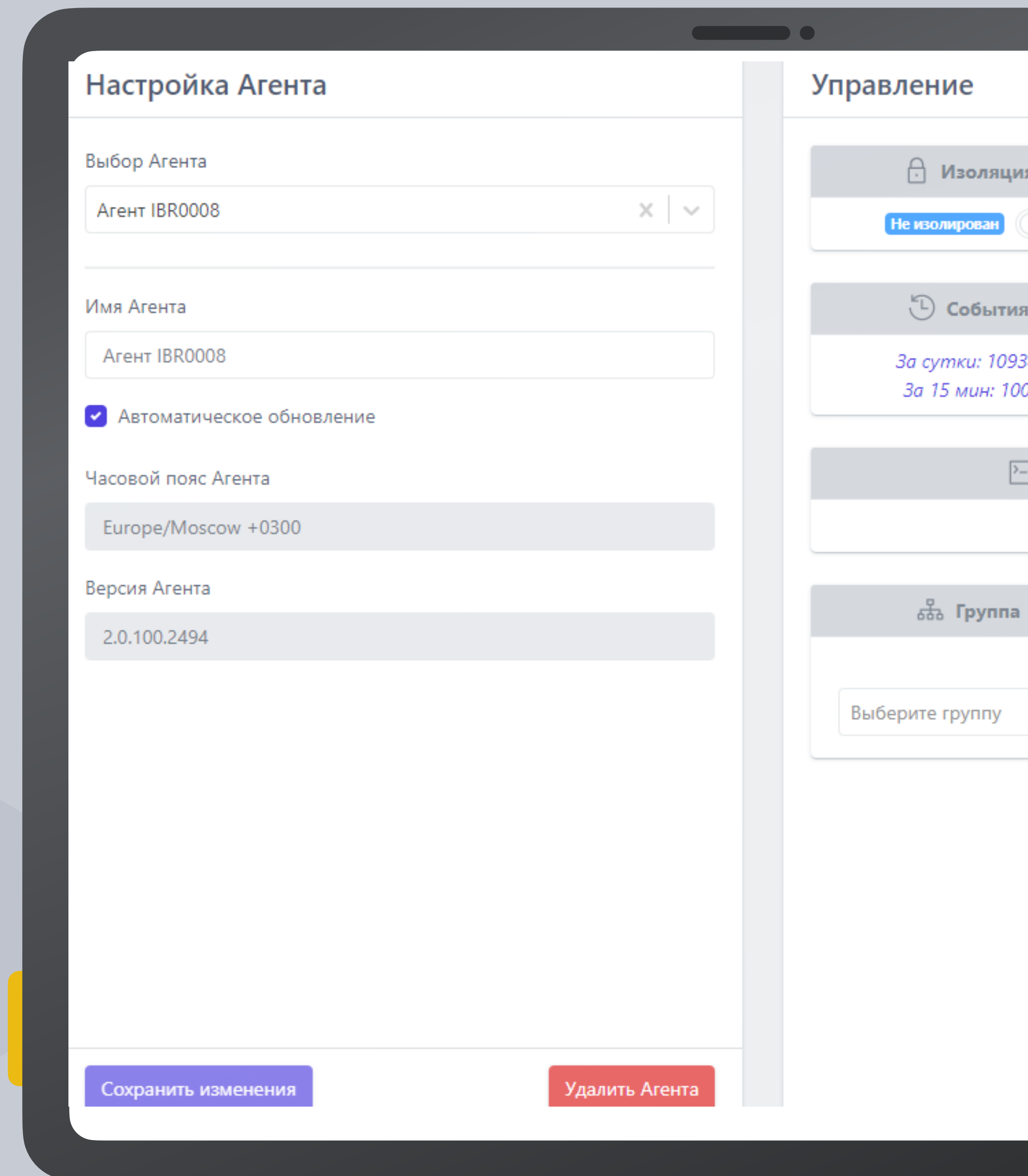
Реакция на запуск программ из альтернативных потоков NTFS (AltExeStream)

Блокировать

Настройка профиля безопасности агента



Обилие тонких настроек позволяет создавать эффективные профили безопасности



Настройка Агента

Выбор Агента

Агент IBR0008

Имя Агента

Агент IBR0008

☒ Автоматическое обновление

Часовой пояс Агента

Europe/Moscow +0300

Версия Агента

2.0.100.2494

Сохранить изменения

Удалить Агента

Управление

Изоляция

Не изолирован

События

За сутки: 1093

За 15 мин: 100

Группа

Выберите группу

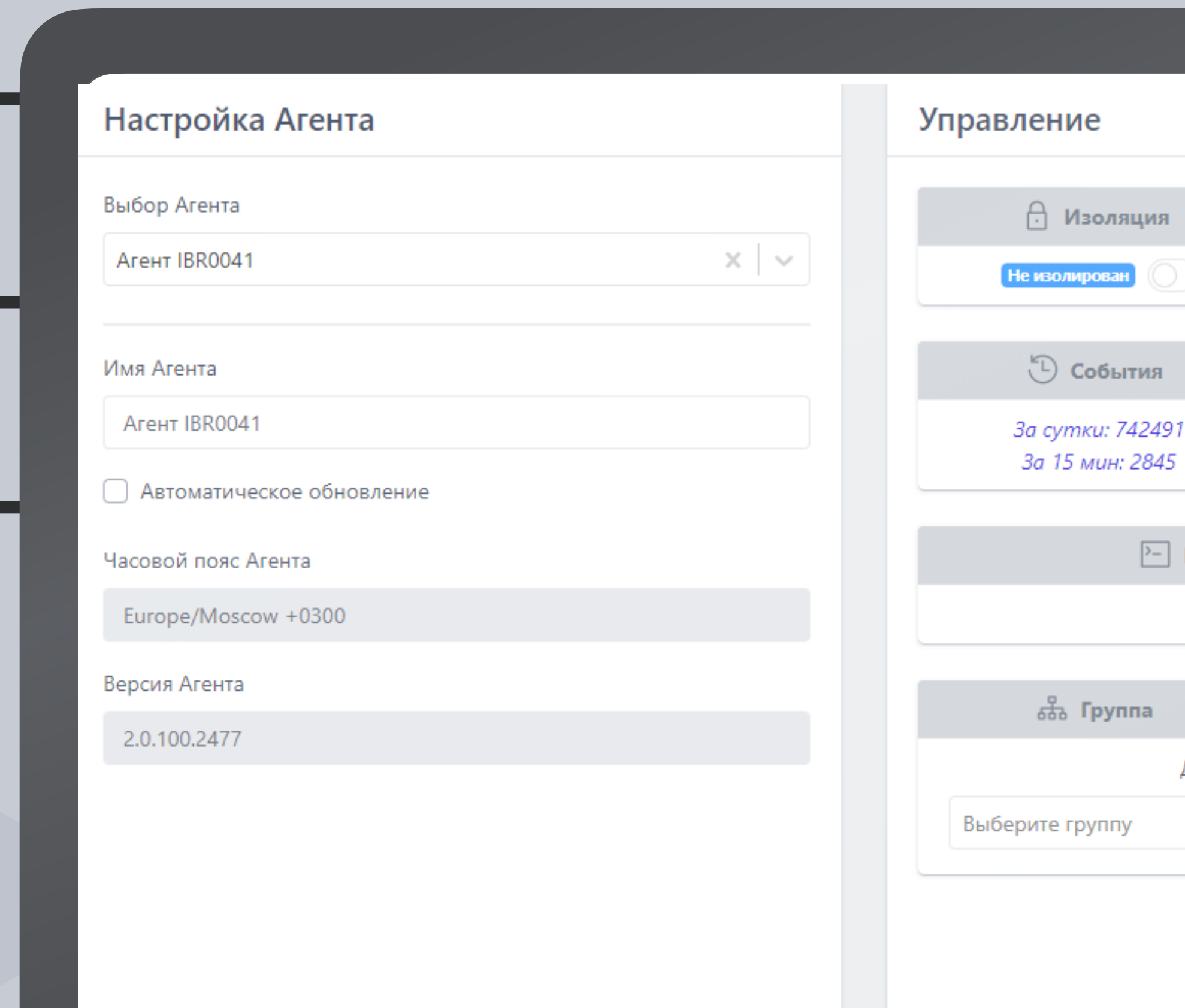
Удаленное управление агентами

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



Планы развития



Linux-агент

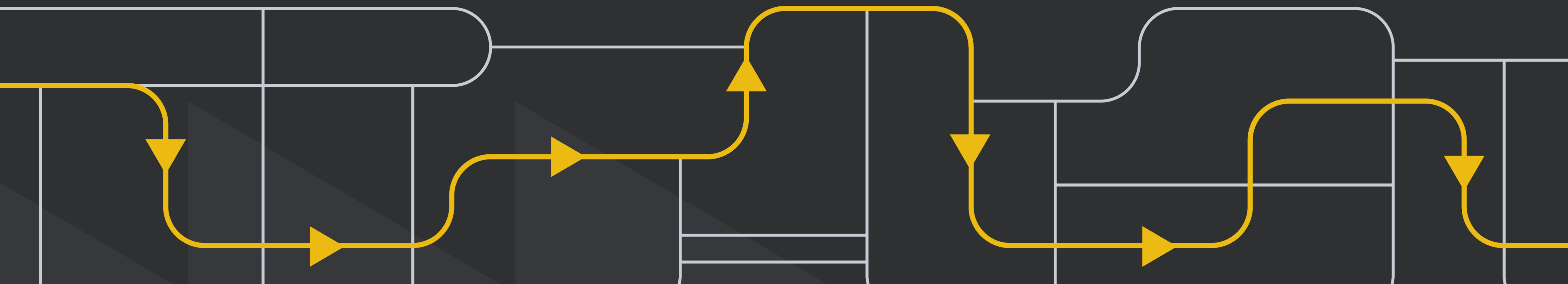
Автоматическое устранение последствий атак

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)

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 Protect AV — Центр управления

 RT Protect AV



Файловый сканер

Состояние: **норма**
Фоновое сканирование: усиленное
Время запуска: 10:48 18.03.2022
Проверено: 5760
Угроз: **4**
Ошибок: 0

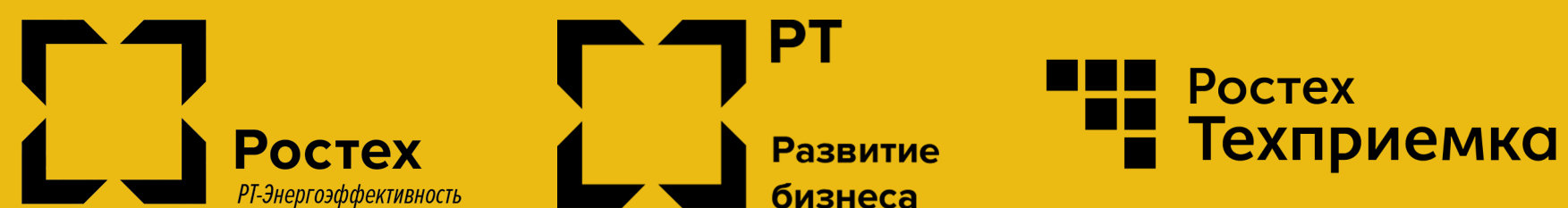
Антивирусные базы

Версия: 2.0.3
Угроз: 36012
Статус: **загружены**
Обновлено: 14:43 31.01.2022

Сетевой агент:

Состояние: **норма**
Сервер обновлений: доступен

Нам доверяют



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

