Autopentest LAB

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Платформы Autopentest iSTEM 2.0

Благодарим за интерес к Платформе Autopentest iSTEM 2.0!

Настоящее руководство содержит описание работы с платформой: создание, настройку, мониторинг и управление проектами автопентеста, анализ результатов тестирования. Отдельный раздел посвящён справочнику по интерфейсу: описание окон, панелей и интерактивных элементов.

По вопросам технической поддержки обращайтесь, пожалуйста, к вашему поставщику, либо в службу технической поддержки АВТОПЕНТЕСТ ЛАБ - support@autopentest.ru.

Будем рады вам помочь!

С уважением,

Команда ООО «АВТОПЕНТЕСТ ЛАБ»

Лицензионное соглашение с конечным пользователем Платформы Autopentest iSTEM 2.0: http://autopentest.ru/eula

ОГЛАВЛЕНИЕ

1 Введение 4
1.1 Назначение документа 4
1.2 О платформе 4
1.2.1 Модель этичной атаки 4
1.2.2 Объектная модель платформы 5

2 Создание, запуск, пауза и остановка проектов 6
2.1 Создание нового проекта 6
2.2 Настройка параметров проекта 7
2.3 Настройка границ автопентеста 7
2.4 Запуск проекта 8
2.5 Приостановка проекта (Пауза) 8
2.6 Остановка проекта 9

3 Мониторинг хода проекта 10
3.1 Как понять, что проект запущен, как долго идёт и когда остановится? 10
3.2 Как понять, в каких границах выполняется автопентест? 10
3.3 Как увидеть общую оценку риска? 11
3.4 Как увидеть общую статистику по фактам? 11
3.5 Как увидеть общую статистику по артефактам? 11
3.6 Как увидеть, какие активы система нашла в заданных границах? 11
3.7 Как увидеть статистику по найденным слабостям? 12
3.8 Как увидеть наиболее ценные находки? 12
3.9 Как отслеживать статистику и прогресс действий? 12

4 Управление действиями проекта 13
4.1 Как увидеть предложенные действия? 13
4.2 Как одобрить или отклонить действие? 15
4.3 Как остановить выполняемое действие? 15
4.4 Как запустить действие вручную? 15
4.5 Какие действия выполняются автоматически, а какие требуют одобрения? 15

5 Анализ результатов проекта 16
5.1 Как посмотреть все действия в рамках проекта? 16
5.2 Как посмотреть все факты в рамках проекта? 16
5.3 Как перейти к нужным фактам и действиям с Панели управления? 16
5.4 Как понять, как система получила конкретный трофей (любой факт)? 16
5.4.1 Через связанные действия в карточках фактов в окне Список фактов (Fact List) 16
5.4.2 Через ретроспективный анализ в Киллчейне (Kill Chain) 16
5.5 Как понять возможные последствия конкретного действия или факта? 17
5.5.1 Через карточки действий в Журнале действий (Action Log) 18
5.6 Как взглянуть на инфраструктуру глазами атакующего? 18
5.7 Как увидеть описание конкретной слабости? 19
5.8 Как увидеть описание любых действий? 19
5.8.1 В Журнале действий (Action Log) 19
5.8.2 В Базе знаний (Knowledge Base) 20
5.9 Как сформировать отчёт по проекту? 20
5.9.1 Подразделы отчёта 20
5.9.2 Настройка отчёта 20
5.9.3 Экспорт отчёта 21

6 Справочник по интерфейсу 22
6.1 Навигация по интерфейсу 22
6.1.1 Боковое меню навигации по проекту 22
6.1.2 Глобальная навигационная цепочка (Breadcrumbs) 22
6.1.3 Карточки фактов и действий 23
6.2 Работа с проектами 23
6.2.1 Список проектов (Autopentest Projects) 23
6.2.2 Конфигуратор проекта (Project Configurator) 24
6.3 Основные окна 25

6.3.1 Панель управления (Dashboard) 25
6.3.2 Журнал действий (Action Log) 26
6.3.3 Список фактов (Fact List) 27
6.4 Инструменты анализа 28
6.4.1 Киллчейн (Kill Chain) 28
6.4.2 Инспектор структуры (Structure) 29
6.4.3 Расследование (Investigation) 30
6.5 Вспомогательные окна 30
6.5.1 База знаний (Knowledge Base) 30
6.5.2 Конфигуратор отчёта (Report Builder) 31
6.6 Ручное управление данными 32
6.6.1 Пользовательские факты (User Input) 32
6.6.2 Создать действие (Create Action) 33

1 ВВЕДЕНИЕ

1.1 Назначение документа

Настоящее Руководство пользователя предназначено для операторов Платформы Autopentest iSTEM 2.0. Документ содержит информацию, необходимую для работы с веб-интерфейсом платформы: управление проектами, мониторинг выполнения задач, анализ результатов тестирования и формирование отчётов.

Инструкции по установке, настройке и администрированию платформы см. в отдельных документах:

- Руководство по быстрому запуску.

1.2 О платформе

Платформа Autopentest iSTEM 2.0 выполняет автоматизированную проверку киберзащиты ИТ-инфраструктуры организации (автопентест) с учётом всех внедрённых в ней средств защиты и процессов. Система имитирует поведение реального злоумышленника в сети, безопасно выполняет контролируемые действия, фиксирует подтверждённые результаты и предоставляет рекомендации по устранению выявленных слабых мест, релевантных конкретной среде в конкретный момент времени.

1.2.1 Модель этичной атаки

Платформа моделирует цепочки атак в анализируемой инфраструктуре с помощью универсальной и расширяемой объектной модели. Основной принцип модели – разделение *фактов* и *действий*:

- **Факт (Fact)** – фрагмент информации об анализируемом ИТ-окружении. Факты попадают в систему либо от пользователя, либо становятся известными или подтверждаются действиями системы.
- **Действие (Action)** – операция, выполняемая с целью поиска новых фактов. Одни действия используют известные факты в качестве входных параметров, а другие – выполняются без них.

Вместе факты и действия образуют единый граф, отражающий последовательность цепочки атаки (Kill Chain). Цепочка атаки наглядно демонстрирует причинно-следственные связи фактов с действиями: известные факты используются как параметры для действий, действия подтверждают известные или находят новые факты, те открывают возможность выполнить следующие действия, и так далее…:

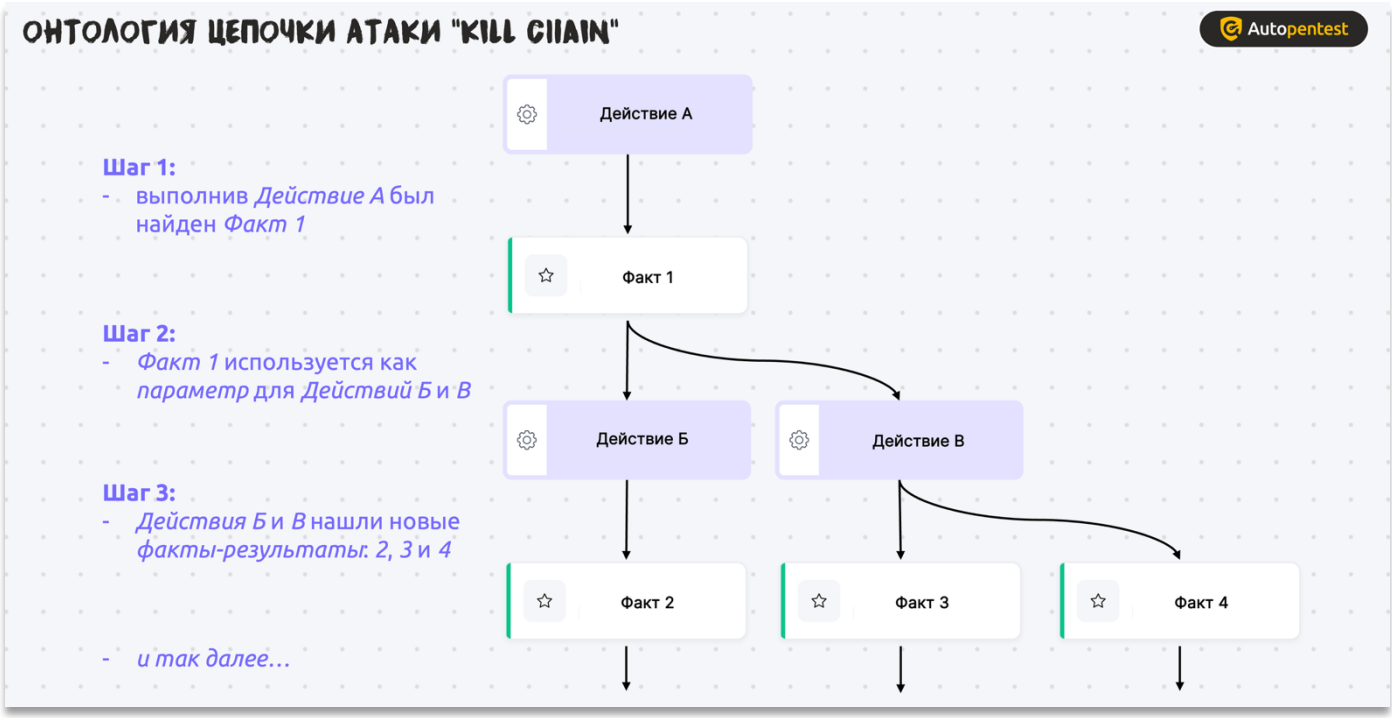


Рисунок 1: Пример схемы цепочки атаки с действиями и фактами

1.2.2 Объектная модель платформы

Факт (Fact)

Фрагмент информации об анализируемой ИТ-среде. Факты описывают найденные сущности и их свойства: IP-диапазоны, хосты, порты, учётные данные, уязвимости, сессии, файлы, права доступа и др. Факты образуют агрегированную базу знаний системы об окружении. Факты по отношению к действиям в цепочке атаки могут быть:

- **Аргументами (Arguments)** – фактами, которые те или иные действия используют в своей работе в качестве входящих параметров;
- **Результатами (Results)** – фактами, которые те или иные действия подтверждают или находят в результате выполнения.

Большинство найденных системой фактов классифицируется как «Трофеи» (Trophies) и ранжируется по уровню ценности (weight). Любые факты могут быть добавлены в систему пользователем вручную через веб-интерфейс или API (например: IP-диапазоны для определения границ пентеста, учётные данные для автопентеста в модели «серый ящик» и пр.).

Действие (Action)

Операция, выполняемая системой в роли условного злоумышленника для сбора новых или проверки известных фактов. Некоторые действия требуют входные факты-аргументы в качестве параметров. В отношении фактов в цепочке атаки действия выполняют:

- **Подтверждения (Verifications)** – любое результативное действие подтверждает существование тех или иных фактов (например: обнаружен компьютер (хост), обнаружена уязвимость на хосте и пр.);
- **Использование (Usage)** – для работы некоторых действий требуются входящие факты-аргументы (например: для проверки уязвимости на хосте действию нужен его адрес).

Действия могут быть предложены системой, одобрены пользователем, выполнены автоматически или запущены вручную через веб-интерфейс или API (например, если на хосте была устранена уязвимость и теперь нужно выполнить конкретное действие для повторной проверки и подтверждения).

Цепочка атаки (Kill Chain)

Показывает, как исходные условия могут привести потенциального злоумышленника к результату через последовательность выполненных действий и обнаруженных фактов. В интерфейсе платформы любые факты и действия могут быть отправной точкой для автоматического построения цепочки атаки в ретроспективу или перспективу:

- **Ретроспективный анализ** помогает выявить «корневые» слабые места, благодаря которым становится возможна реализация всех последующих этапов моделируемой атаки.
- **Перспективный анализ** демонстрирует возможные последствия от успешного выполнения того или иного действия атакующего и как может развиваться цепочка атаки в глубину и ширину.

Проект (Project)

Отдельная сессия автопентеста со своей конфигурацией, границами (Pentest Scope), статусом, набором фактов, действий и отчётными данными.

Границы пентеста (Pentest Scope)

IP-диапазоны (IPRange), определяющие, какие хосты и подсети включены в конкретный проект. Границы настраиваются пользователем через веб-интерфейс или API.

Глоссарий (Glossary)

Вспомогательная статичная информация, не зависящая от конкретной анализируемой среды (например: описание сервисов, протоколов, записи базы знаний, теги и другие повторно используемые справочные данные).

2 СОЗДАНИЕ, ЗАПУСК, ПАУЗА И ОСТАНОВКА ПРОЕКТОВ

2.1 Создание нового проекта

Откройте веб-интерфейс[1] в браузере с рабочей станции, где импортирован клиентский сертификат:

```
https://<autopentest_host>:8443/
```

При открытии веб-интерфейса отображается страница выбора проекта «Проекты автопентеста».

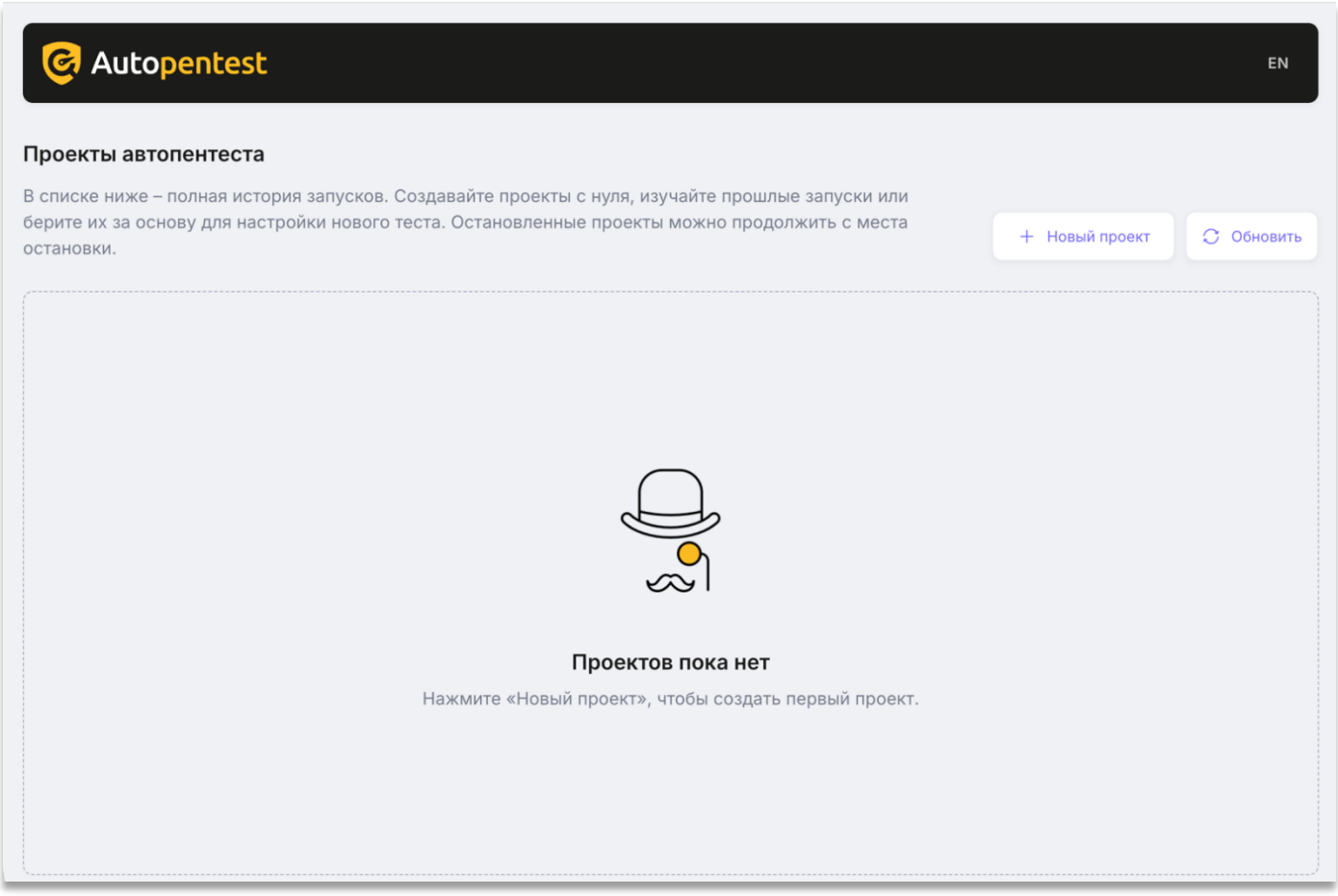


Рисунок 2: Окно выбора проекта при отсутствии проектов

Если проекты уже создавались ранее, список будет содержать их:

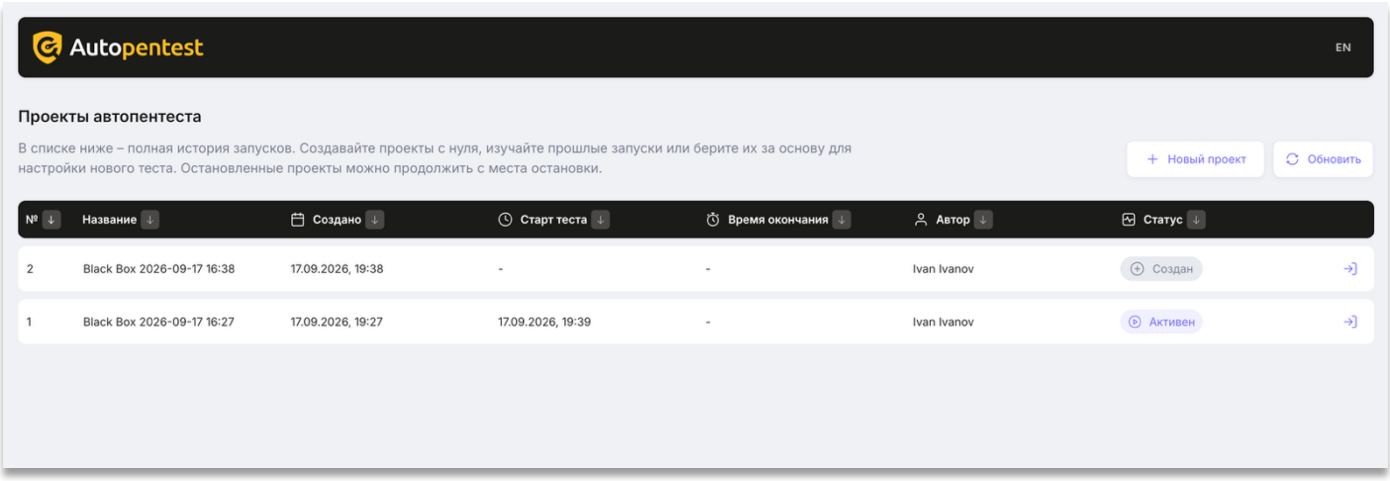


Рисунок 3: Окно выбора проекта с существующими проектами

[1] *Используйте адрес, настроенный при установке системы (см.* ***Руководство по быстрому запуску****).*

Для создания нового проекта нажмите кнопку + Новый проект (New Project) в правой верхней части экрана. Откроется окно конфигурации проекта с параметрами только что созданного проекта в статусе «Создан» (Created):

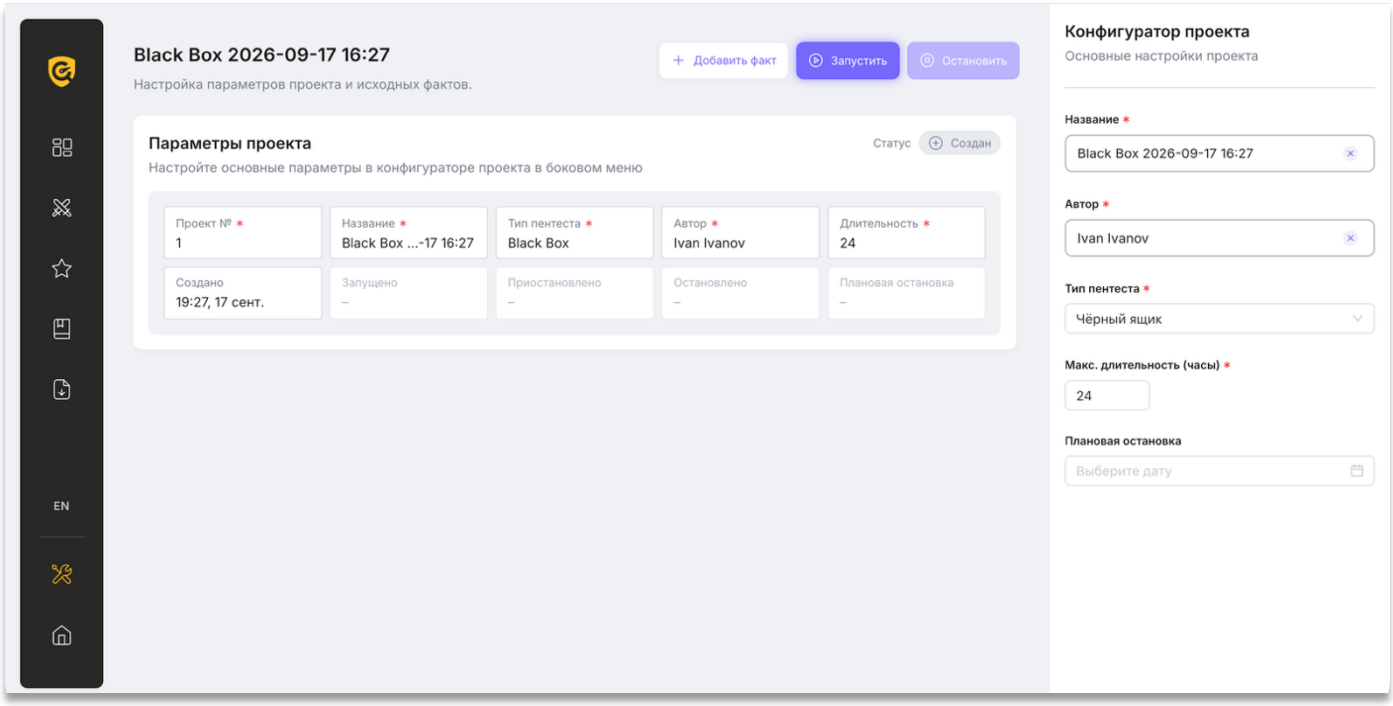


Рисунок 4: Окно конфигурации проекта

2.2 Настройка параметров проекта

В рабочей области окна отображаются параметры проекта:

- название проекта;
- порядковый номер (ID);
- длительность;
- автор (имя пользователя);
- тип пентеста (например, «Чёрный ящик»);
- временные метки.

Параметры редактируются в боковом меню конфигуратора справа в любое время – как до, так и после запуска проекта. Часть параметров недоступна для ручного редактирования (ID, временные метки).

При создании проекта редактируемые поля автоматически заполняются значениями по умолчанию:

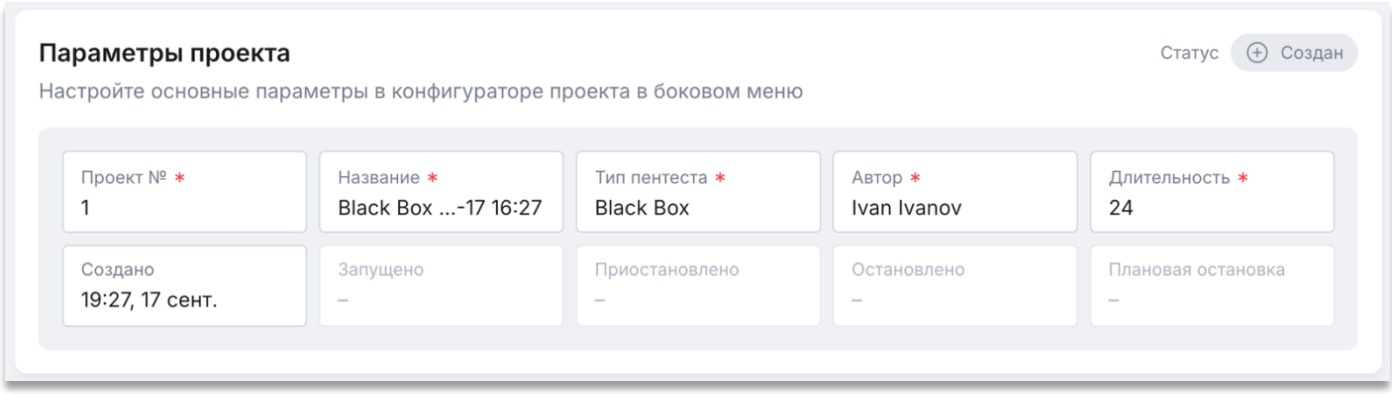


Рисунок 5: Параметры проекта со значениями по умолчанию

После установки параметров можно переходить к настройке границ автопентеста.

2.3 Настройка границ автопентеста

Для настройки границ автопентеста используется меню добавления пользовательских фактов. Любые факты можно добавлять в проект в любом статусе: «Создан» (Created), «Активен» (Running), «Пауза» (Paused) или «Окончен» (Stopped). Если не добавить границы автопентеста в созданный проект, то

после его запуска система не сможет эффективно работать, так как не получит целевую сеть для анализа.

Нажмите на кнопку + Добавить факт (+ Add fact) в верхней части экрана – откроется меню ручного добавления пользовательских фактов. Введите один или несколько фактов типа «Диапазон IP» (IPRange) либо через поле JSON, либо через поля формы ручного ввода.

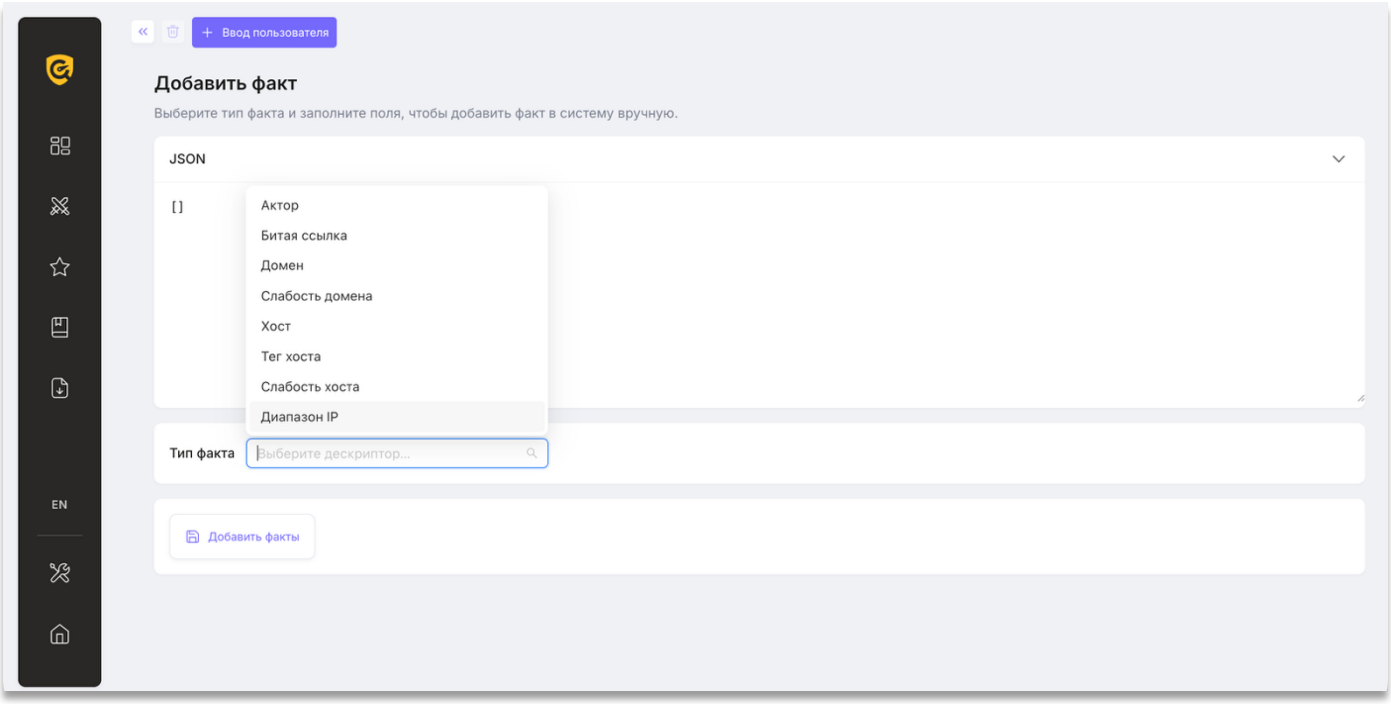


Рисунок 6: Меню добавления фактов вручную

После ввода диапазонов IP-адресов нажмите кнопку Добавить факты (+Add facts), после чего можно переходить к запуску проекта.

2.4 Запуск проекта

Запустить проект можно двумя способами: из окна «Конфигуратор проекта» или в «Панели управления» (Dashboard). Оба окна открываются через боковое меню навигации.

- **В окне «Конфигуратор проекта»:** нажмите кнопку Запустить (Run) в правой верхней части экрана.
- **В окне «Панель управления»:** нажмите иконку «Запустить проект» в верхней левой панели – ▷.

После запуска статус проекта изменится на «Активен» (Running).

2.5 Приостановка проекта (Пауза)

Активный проект можно поставить на паузу. Для этого в верхней правой части окна конфигуратора проекта нажмите кнопку Пауза (Pause), либо используйте кнопку «Поставить проект на паузу» в верхней левой панели окна «Панель управления» – ⏸.

После постановки проекта на паузу статус проекта изменится на «Пауза» (Paused).

Постановка проекта на паузу останавливает только координатор – механизм предложения новых действий к запуску. Ранее запущенные действия продолжают работу до штатного завершения.

В частности, сохраняют активность NTLMRelay, MITMResponder; остаются доступными для последующего использования все активные сессии (RelayedSession).

Во время паузы отсчёт времени до запланированной остановки проекта не приостанавливается.

Для снятия проекта с паузы используются кнопки Продолжить (Resume) в тех же местах интерфейса. Статус вернётся в «Активен», система продолжит работу с использованием ранее накопленных фактов.

2.6 Остановка проекта

При достижении временного лимита теста проект останавливается автоматически, его статус меняется на «Окончен» (Stopped). В этом статусе система завершает всю активность в рамках проекта.

Проекты в статусах «Активен» (Running) и «Пауза» (Paused) можно останавливать вручную. Для этого используйте кнопку Остановить (Stop) в окне конфигуратора проекта или в верхней левой панели окна «Панель управления» - .

Для возобновления остановленных проектов используются кнопки Перезапустить (Rerun) в тех же местах. После перезапуска статус проекта возвращается в «Активен» (Running). Проект запускается заново, но использует все факты, накопленные до остановки.

3 МОНИТОРИНГ ХОДА ПРОЕКТА

После запуска проекта отслеживать его состояние можно на Панели управления (Dashboard). Окно состоит из группы панелей, отображающих основные параметры и результаты проекта. Ниже приведены типовые задачи мониторинга.

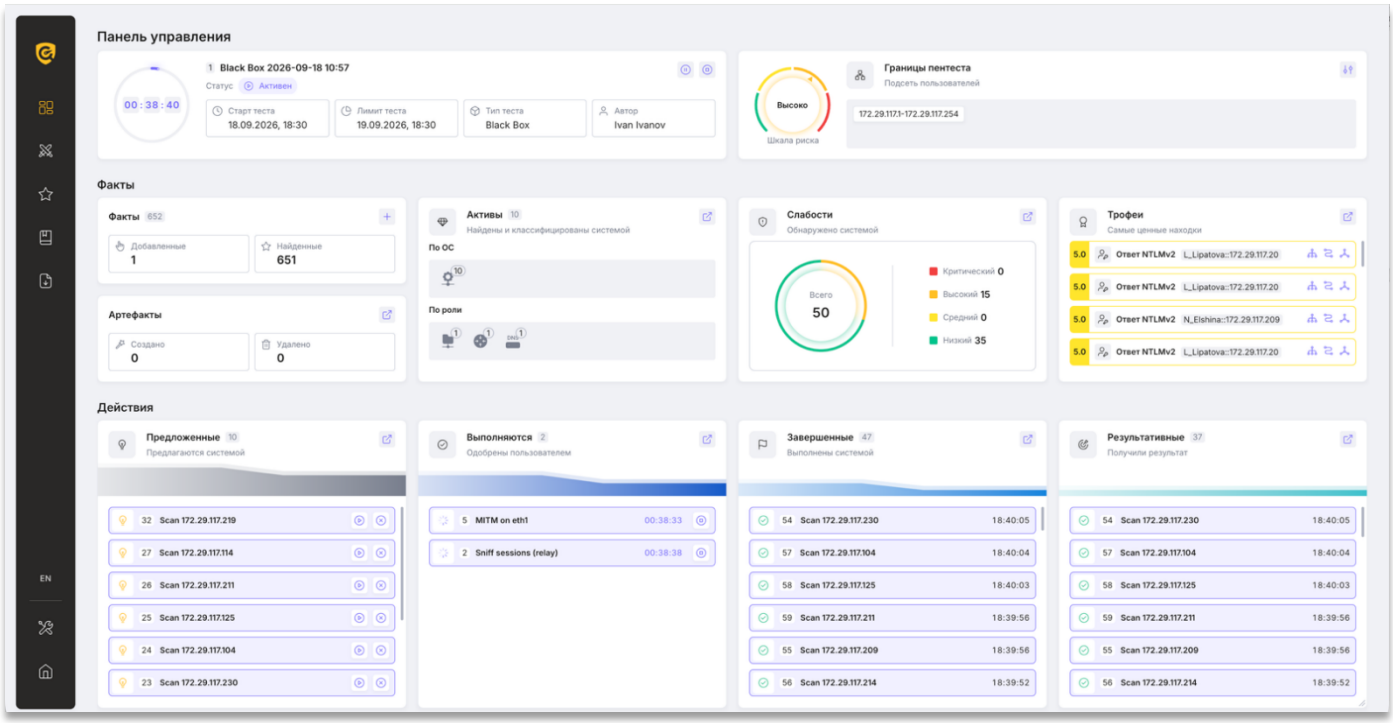


Рисунок 7: Общий вид панели управления (Dashboard)

3.1 Как понять, что проект запущен, как долго идёт и когда остановится?

В верхней левой панели отображаются:

- таймер: время, прошедшее с момента запуска;
- номер (ID) и название проекта;
- статус проекта (например, «Активен»);
- дата и время старта теста;
- лимит теста: дата и время плановой остановки;
- тип теста (например, Black Box);
- автор проекта.

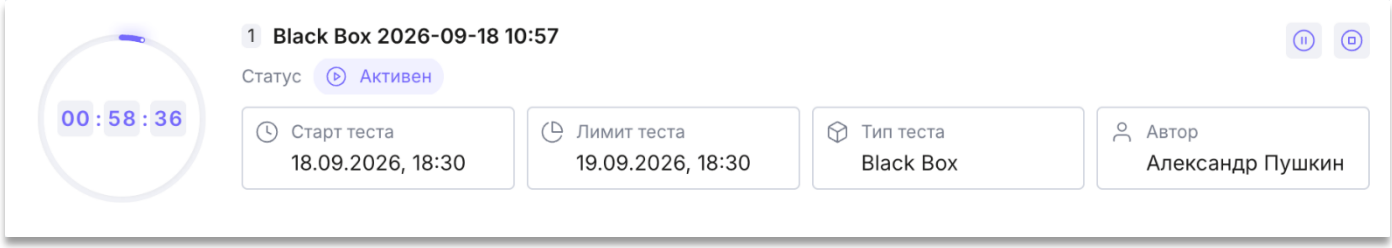


Рисунок 8: Верхняя левая панель - параметры проекта

3.2 Как понять, в каких границах выполняется автопентест?

В верхней правой панели отображается блок «Границы пентеста» с перечнем IP-диапазонов и адресов, установленных в качестве границ. Для добавления новых границ нажмите кнопку + в панели «Факты» – откроется меню добавления пользовательских фактов (то же, что и в конфигураторе проекта, через кнопку + Добавить факт).

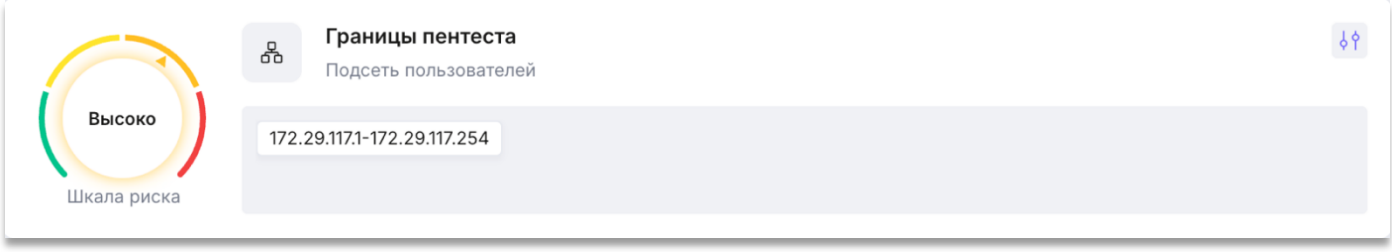


Рисунок 9: Верхняя правая панель - границы автопентеста и шкала риска

3.3 Как увидеть общую оценку риска?

В верхней правой панели расположена Шкала риска (Risk Score). Значение рассчитывается по наиболее ценному трофею, обнаруженному системой. Трофеи, добавленные пользователем через User Input, в расчёте не участвуют.

3.4 Как увидеть общую статистику по фактам?

В центральной части окна, в панели «Факты», отображается:

- общее число фактов;
- число фактов, добавленных пользователем (User Input);
- число фактов, найденных системой.

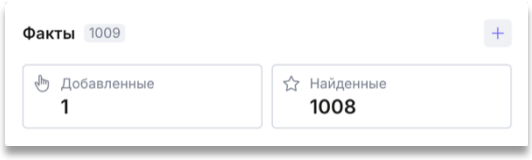


Рисунок 10: Панель "Факты"

3.5 Как увидеть общую статистику по артефактам?

В центральной части окна, в панели «Артефакты», отображается:

- число артефактов, созданных системой;
- число артефактов, удалённых системой.

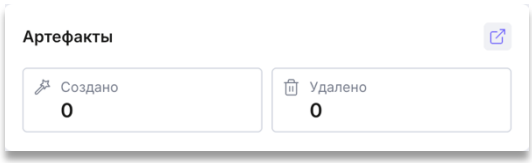


Рисунок 11: Панель "Артефакты"

3.6 Как увидеть, какие активы система нашла в заданных границах?

В центральной части окна, в панели «Активы», отображается сводка по обнаруженным активам с разбивкой:

- по операционной системе (By OS);
- по роли (By Role).

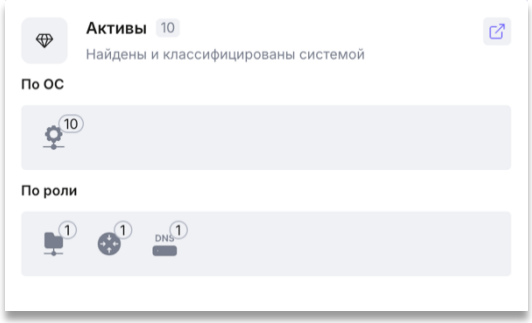


Рисунок 12: Панель "Активы"

3.7 Как увидеть статистику по найденным слабостям?

В центральной части окна, в панели «Слабости», отображается общее число выявленных слабостей с разбивкой по уровням критичности: низкий (Low), средний (Medium), высокий (High), критический (Critical).

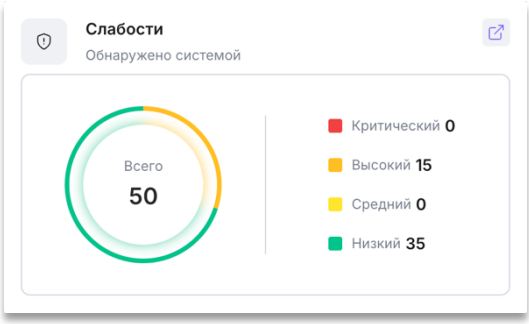


Рисунок 13: Панель "Слабости"

3.8 Как увидеть наиболее ценные находки?

В центральной части окна, в панели «Трофеи», отображается список наиболее ценных находок, отсортированный по уровню ценности (weight) с точки зрения атакующего. Список прокручивается.

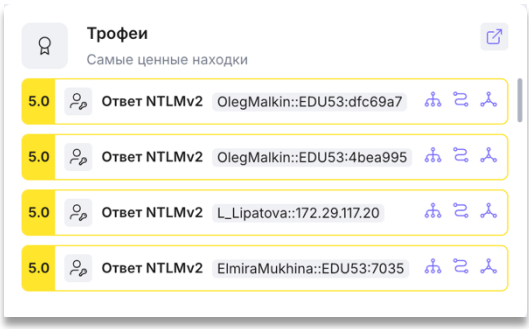


Рисунок 14: Панель "Трофеи"

3.9 Как отслеживать статистику и прогресс действий?

В нижней части окна отображается сводка по действиям системы, разбитая по статусам:

- **Предложенные (Suggested)** – действия, которые система предлагает выполнить;
- **Выполняются (Running)** – действия, выполняемые в данный момент;
- **Завершённые (Completed)** – действия, которые система уже выполнила;
- **Результативные (Fruitful)** – действия, которые привели к обнаружению новых фактов.

Списки прокручиваются. Каждая панель содержит ссылку на журнал действий (Action Log).

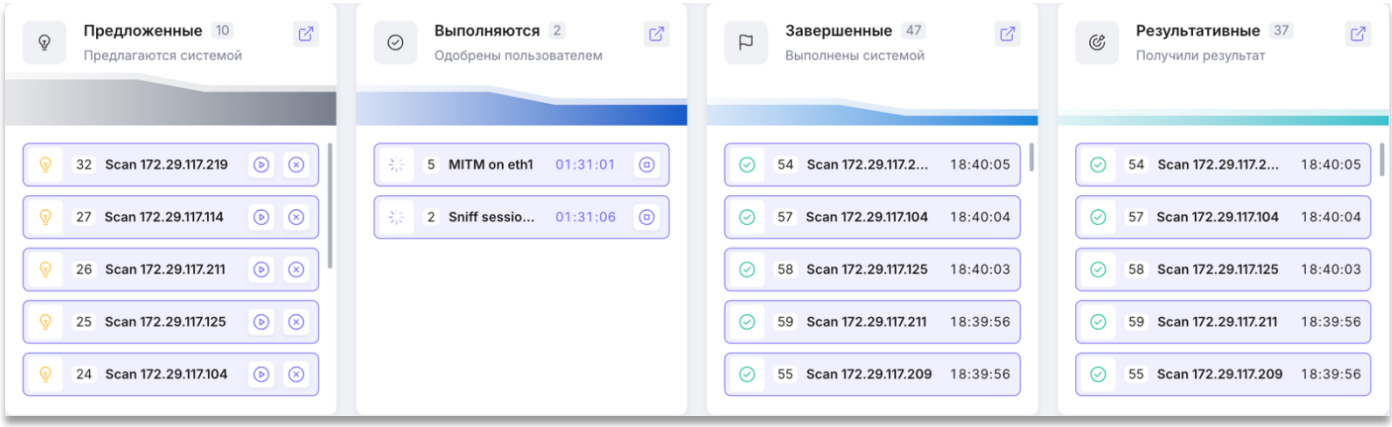


Рисунок 15: Сводная статистика по действиям

4 УПРАВЛЕНИЕ ДЕЙСТВИЯМИ ПРОЕКТА

Действиями можно управлять из любого окна интерфейса, где отображаются их карточки: Панель управления (Dashboard), Журнал действий (Action Log), Список фактов (Fact List), Киллчейн (Kill Chain).

4.1 Как увидеть предложенные действия?

Предложенные действия отображаются во всех окнах интерфейса, где отображаются действия:

- **Панель управления (Dashboard)** – в панели действий «Предложенные»:

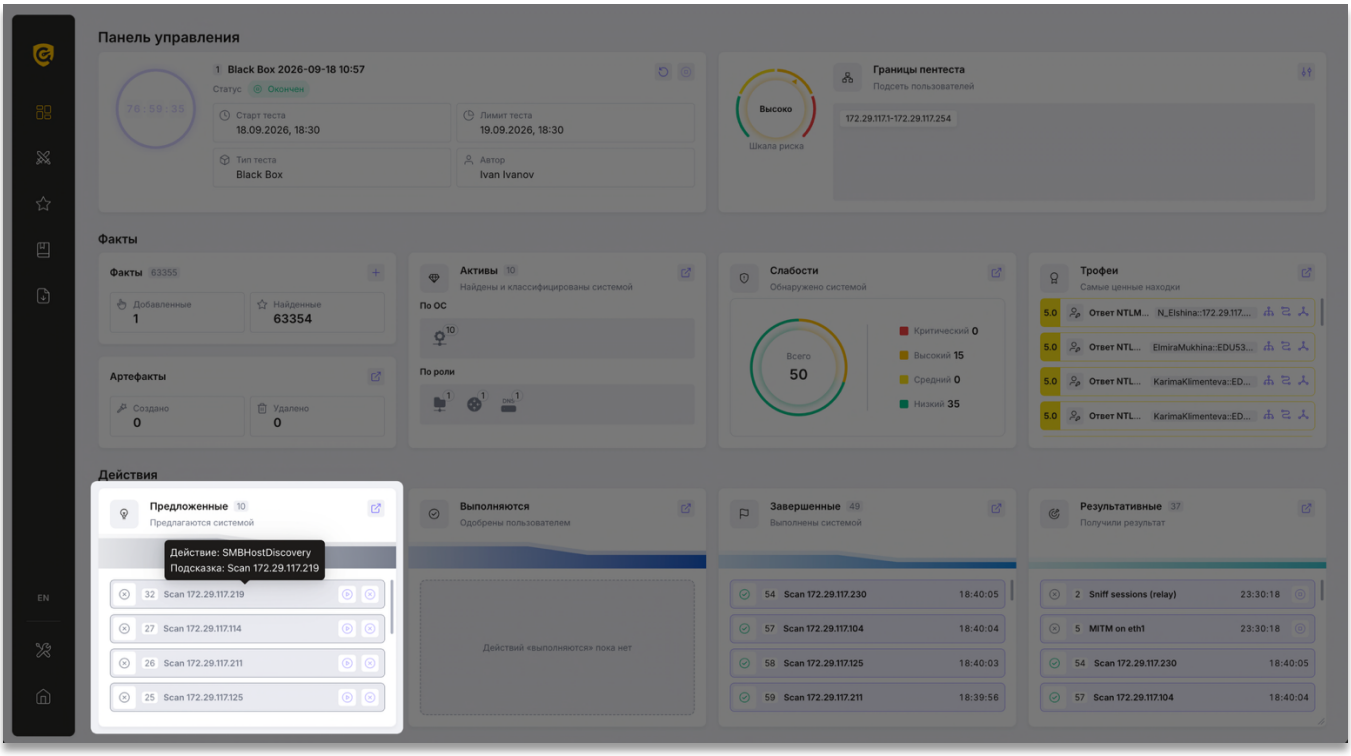


Рисунок 16: Панель «Предложенные» на Панели управления

В Панели управления представлен отфильтрованный список всех предлагаемых системой действий. При наведении курсора на карточку действия появляется краткое описание, содержащее:

- название типа действия (например, «Действие: SMBHostDiscovery»);
- подсказку (например, «Подсказка: Scan 172.29.117.219»).

- **Журнал действий (Action Log)** – в списке действий в рабочей области окна:



Рисунок 17: Предложенные действия в Журнале действий

- **Список фактов (Fact List)** – в развёрнутых карточках фактов:

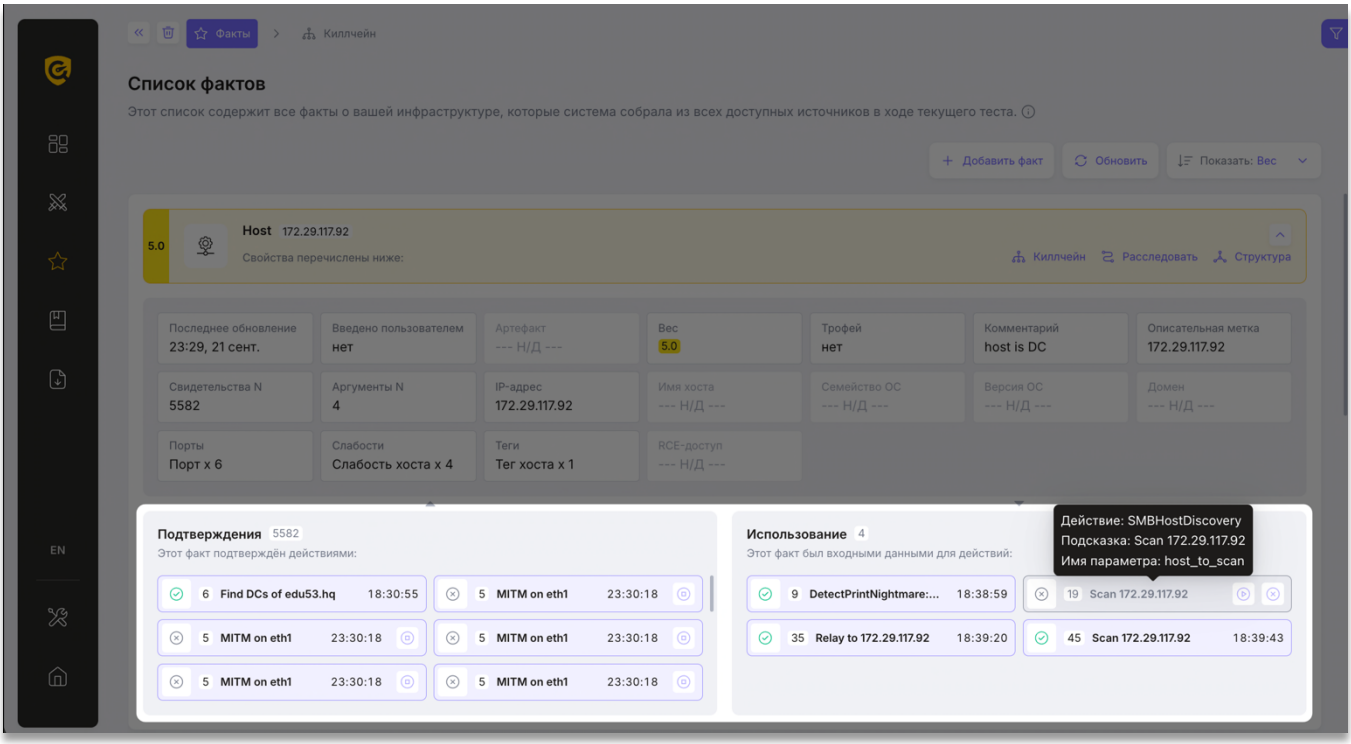


Рисунок 18: Связанные действия в карточке факта (Список фактов)

Раскрытая карточка факта включает все связанные с ним действия: подтвердившие этот факт и использовавшие его в качестве параметра. При наведении курсора на действие появляется краткое описание с названием типа и подсказкой; для действий, использующих факт как параметр, дополнительно отображается имя параметра.

- **Киллчейн (Kill Chain)** – в боковой панели с описанием выбранных узлов графа:

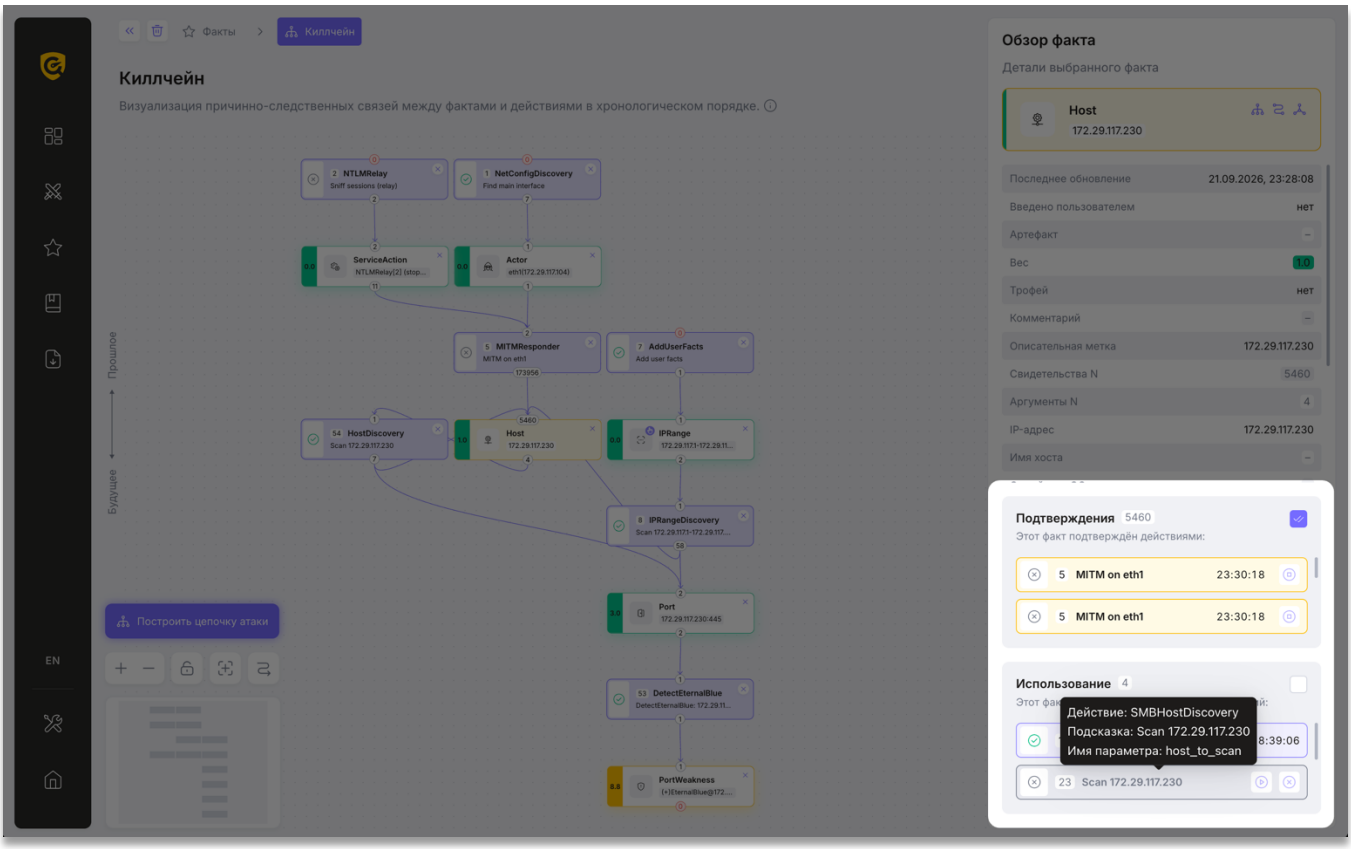


Рисунок 19: Связанные действия в боковой панели окна Киллчейн

При выборе на графе факта в боковой панели появляются все связанные с ним действия. Поведение при наведении курсора аналогично описанному выше.

4.2 Как одобрить или отклонить действие?

Одобрение и отклонение доступны прямо на карточках действий. Кнопки расположены в карточке действия в любом окне, где она отображается:

- **Одобрить**: кнопка с иконкой ⊙;
- **Отклонить**: кнопка с иконкой ⊗.

4.3 Как остановить выполняемое действие?

Остановка доступна прямо на карточке выполняющегося действия:

- **Остановить**: кнопка с иконкой ⊙.

4.4 Как запустить действие вручную?

Если требуется запустить действие, не дожидаясь предложения системы, используйте кнопку + Запустить действия (+ Run actions) в верхней части Журнала действий (Action Log). Откроется окно «Создать действие» (Create Action), где нужно выбрать тип действия и заполнить параметры запуска.

Подробнее см. раздел 6.6.2.

4.5 Какие действия выполняются автоматически, а какие требуют одобрения?

Система разделяет действия на две категории по признаку потенциального риска:

- **Безопасные** – выполняются автоматически сразу после того, как система предлагает их к запуску;
- **Потенциально небезопасные** – требуют ручного одобрения оператором. Система предлагает их к запуску, но не выполняет до подтверждения пользователем.

К потенциально небезопасным относятся действия, которые теоретически могут повлиять на работу инфраструктуры или привести к нежелательным последствиям.

Потенциально небезопасные действия отображаются в интерфейсе со статусом «Предложенные» (Suggested) до тех пор, пока оператор не одобрит их. Управление такими действиями описано в подразделах 4.2 и 4.3.

5 АНАЛИЗ РЕЗУЛЬТАТОВ ПРОЕКТА

Все собранные в ходе проекта факты и выполненные действия доступны для просмотра и анализа. Ниже приведены типовые задачи анализа.

5.1 Как посмотреть все действия в рамках проекта?

Откройте Журнал действий (Action Log) через боковое меню навигации – иконка . В окне отображается список всех действий текущего проекта. Список отсортирован: сверху – самые последние действия.

Для отображения конкретных типов действий используйте боковой фильтр справа.

5.2 Как посмотреть все факты в рамках проекта?

Откройте Список фактов (Fact List) через боковое меню навигации – иконка ☆. В окне отображается список всех фактов текущего проекта. По умолчанию факты отсортированы по уровню ценности (сверху – наиболее ценные). Порядок сортировки можно изменить с помощью кнопки-сортировщика в верхней части окна: по уровню ценности или времени обновления, по возрастанию или убыванию.

Для отображения конкретных типов фактов используйте боковой фильтр справа.

5.3 Как перейти к нужным фактам и действиям с Панели управления?

Панели в окне Панель управления (Dashboard) содержат ссылки, которые открывают Журнал действий (см. 6.3.2) или Список фактов (см. 6.3.3) с уже применённым фильтром:

- панель «Границы пентеста» → Список фактов с фильтром по типу «Диапазон IP» (IPRange);
- панель «Активы» → Список фактов с фильтром по типу «Хост» (Host);
- панель «Слабости» → Список фактов со всеми выявленными слабостями всех типов;
- панель «Трофеи» → Список фактов, отсортированный по уровню ценности (weight).

Ссылки на панелях действий ведут в Журнал действий.

5.4 Как понять, как система получила конкретный трофей (любой факт)?

Есть несколько способов узнать, откуда в системе появился факт любого типа. Ниже приведены основные:

5.4.1 Через связанные действия в карточках фактов в окне Список фактов (Fact List)

Источник получения факта отображается прямо в карточке факта в окне Список фактов (Fact List). Карточки фактов можно раскрывать для детального изучения их свойств:

- временные метки создания или обновления фактов;
- отметки об источниках: найден системой, создан системой как артефакт, добавлен пользователем;
- описательные метки и прочее.

Состав полей зависит от типа факта.

Ниже блока со свойствами расположен блок со связанными действиями:

- **«Подтверждение» (Verifications)** – список действий, подтвердивших наличие этого факта;
- **«Использование» (Usage)** – действия, использовавшие этот факт в качестве входного параметра.

У каждого связанного действия отображается уникальный номер (UID), который можно использовать для идентификации и дальнейшего изучения источников факта.

5.4.2 Через ретроспективный анализ в Киллчейне (Kill Chain)

Полный ретроспективный пошаговый путь, по которому система получила факт любого типа (включая трофеи и слабости), можно увидеть через инструмент построения цепочек атаки в виде интерактивного графа – Киллчейн (Kill Chain).

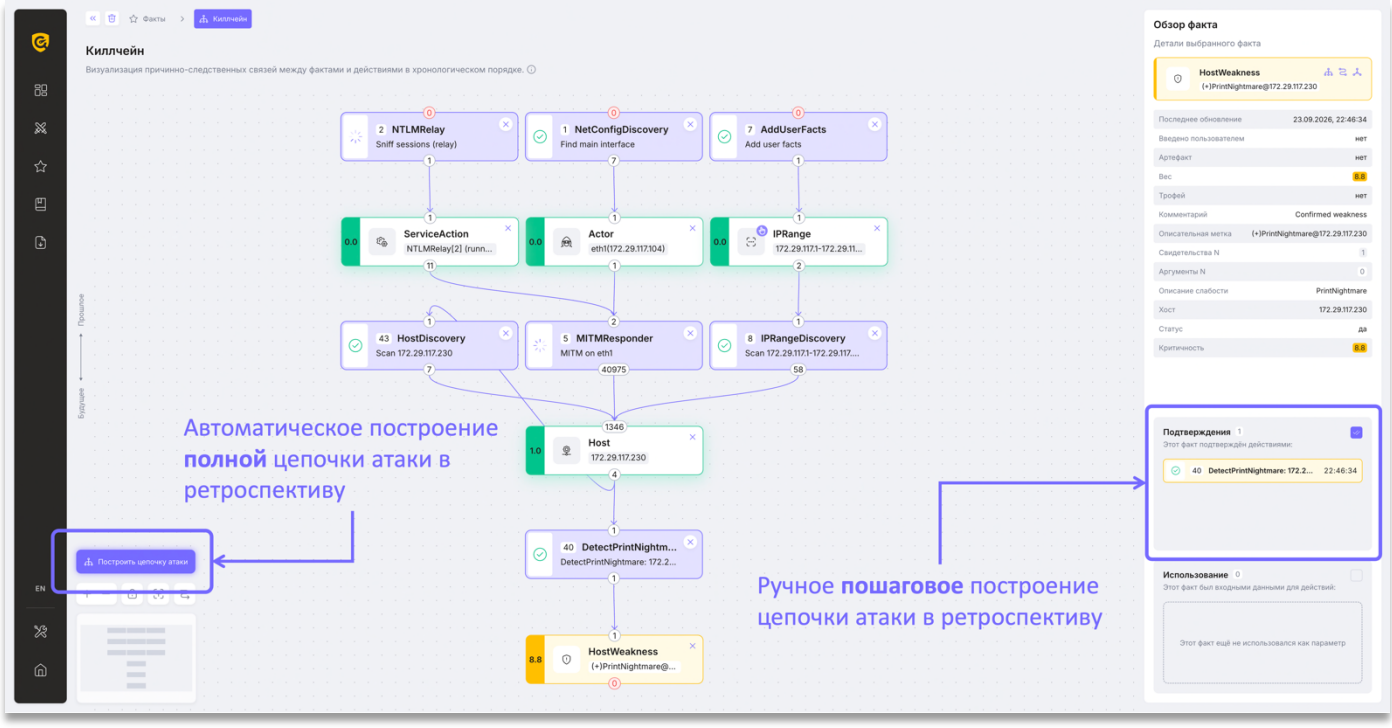


Рисунок 20: Киллчейн (Kill Chain) с примером ретроспективного анализа

В карточках фактов есть специальная ссылка – иконка . При нажатии открывается окно Киллчейн с выбранным фактом. В нём можно:

- добавлять шаги в ретроспективную цепочку вручную;
- построить полную цепочку атаки до самых первых действий системы в проекте – автоматически, используя кнопку Построить цепочку атаки (Generate Full Attack Vector) внизу слева.

5.5 Как понять возможные последствия конкретного действия или факта?

Результаты работы любого действия или использования любого факта доступны в тех же инструментах, что и для ретроспективного анализа (см. 5.4).

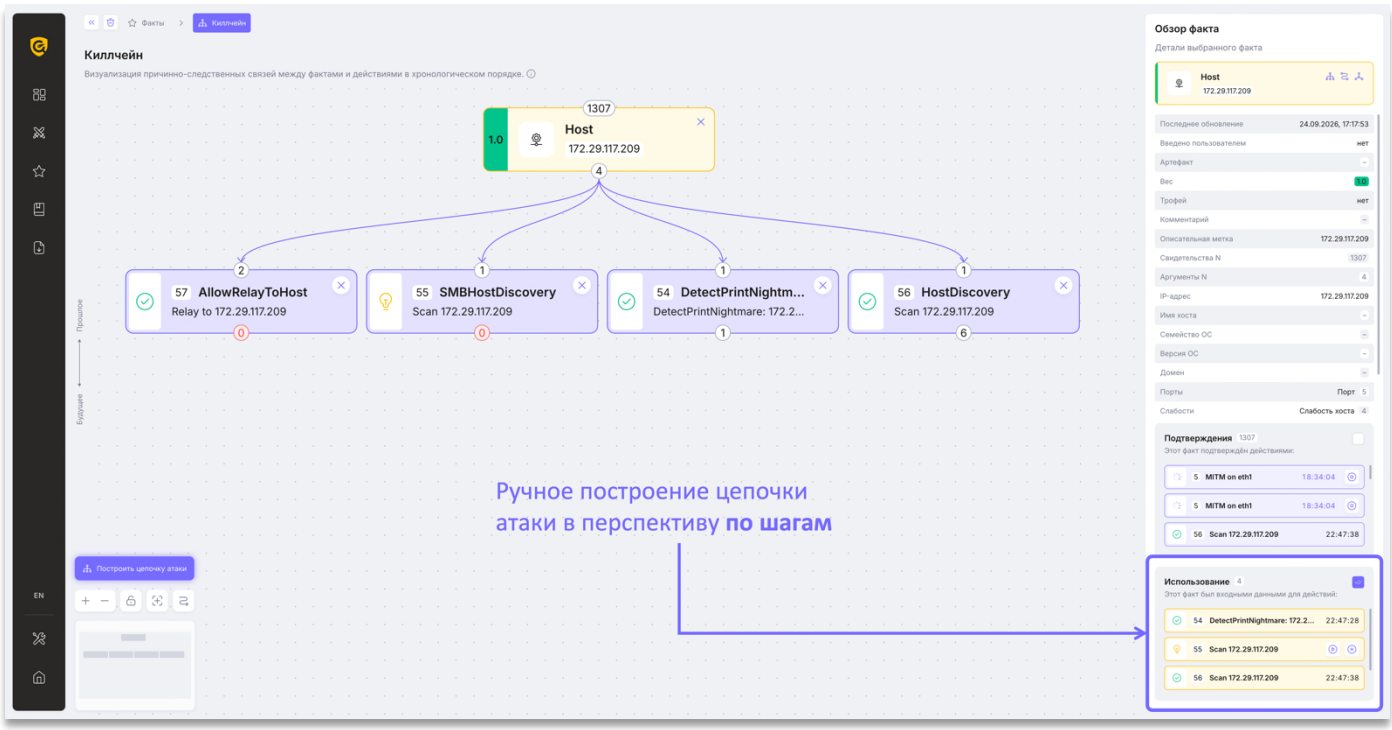


Рисунок 21: Киллчейн (Kill Chain) с примером перспективного анализа

При анализе последствий (*перспективы*) в Киллчейне выстраивайте продолжение цепочки атаки на любую доступную глубину, добавляя на граф уже не *предыдущие* (сверху), а *следующие* шаги (снизу):

- в карточках фактов используйте блок действий «Использование» (Usage) – внизу справа;
- в карточках действий используйте блок фактов «Результаты» (Results) – внизу справа.

5.5.1 Через карточки действий в Журнале действий (Action Log)

В Журнале действий карточки действий также можно раскрывать для детального изучения их свойств. Раскрытая карточка действия включает блок со связанными фактами:

- **«Аргументы» (Arguments)** – список фактов, которые действие использовало как входные параметры;
- **«Результаты» (Results)** – список фактов, которые действие получило в результате выполнения.

У каждого связанного факта есть описательная метка (descriptive label), по которой его можно идентифицировать для дальнейшего изучения.

Как и у фактов, в карточках действий тоже есть специальная ссылка – иконка . При нажатии открывается окно Киллчейн с выбранным действием. В нём также можно выстраивать цепочку атаки как в ретроспективу, так и в перспективу – на любую доступную глубину, автоматически и вручную.

5.6 Как взглянуть на инфраструктуру глазами атакующего?

Все факты в рамках проекта взаимосвязаны. Например, у факта типа «Хост» есть IP-адрес, который тоже является отдельным фактом; у IP-адреса могут быть порты, у портов – сервисы, уязвимости и так далее. По мере появления в проекте новых фактов система выстраивает единую модель окружения, проясняя связи и детализируя инфраструктуру.

Это позволяет взглянуть на сеть с позиции атакующего и увидеть не плоский список несвязанных фактов, а структурированную модель окружения, построенную на основе доступных данных.

В окнах интерфейса, где отображаются карточки фактов, есть специальная ссылка – иконка . При нажатии открывается окно «Инспектор структуры» (Structure) с выбранным фактом. В нём можно не только увидеть свойства выбранного факта, но и использовать интерактивные поля-ссылки, позволяющие выстраивать граф из карточек взаимосвязанных фактов на любую доступную глубину.

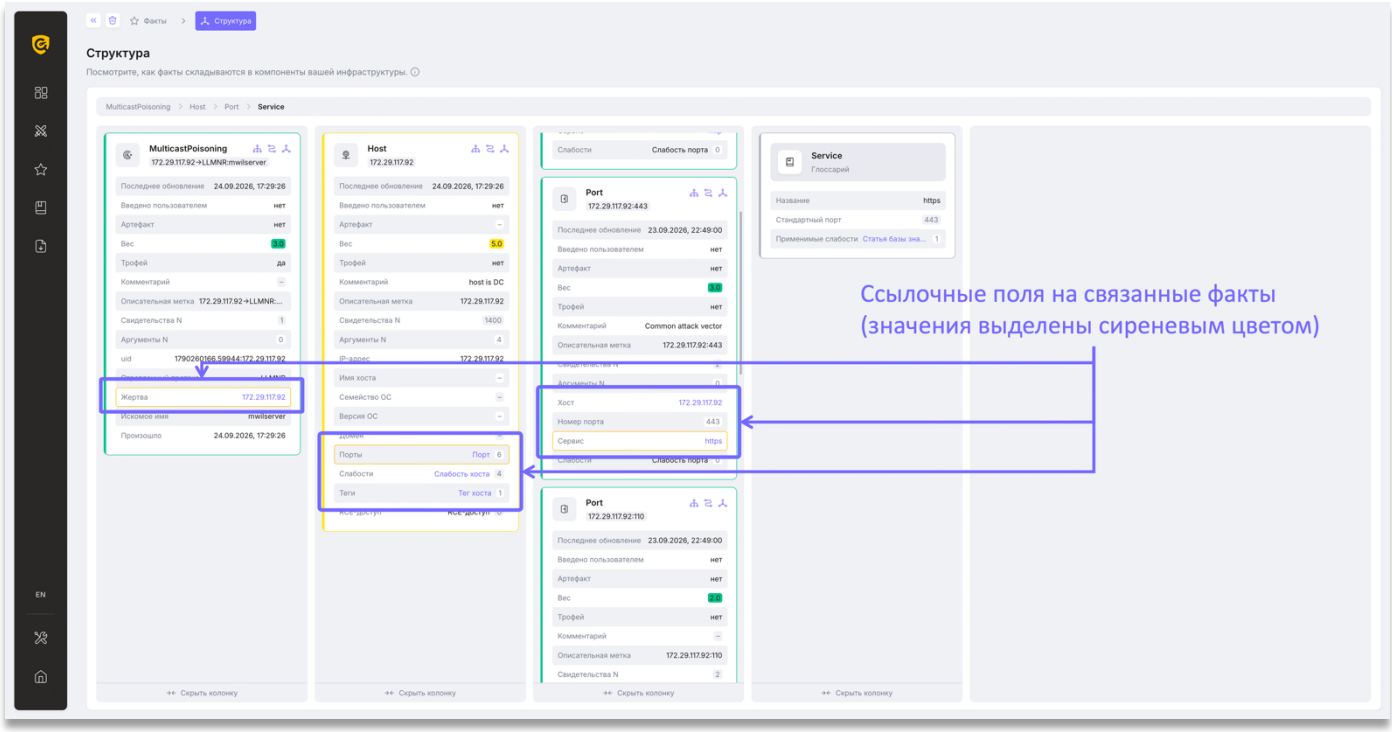


Рисунок 22: Инспектор структуры (Structure) с примером графа взаимосвязанных фактов

5.7 Как увидеть описание конкретной слабости?

Помимо общих свойств факта, Инспектор структуры позволяет раскрывать карточки из Базы знаний (БЗ) с описанием слабостей (Weakness Knowledge Base, Weakness KB). Это удобно, когда при анализе инфраструктуры требуется быстро понять суть обнаруженной слабости, не покидая текущее окно.

Чтобы открыть описание, щёлкните по соответствующему полю-ссылке «Weakness KB» в карточке факта типа «Слабость» – откроется карточка из базы знаний с описанием.

Слабости бывают двух типов: «Уязвимости» (Vulnerability) и «Слабая конфигурация» (Misconfiguration).

Карточка слабости содержит:

- **Основные метрики:** UID, название, тип слабости (уязвимость или слабая конфигурация), идентификаторы CVE и Vendor ID, уровень критичности (Base severity) и вектор CVSS;
- **Влияние (Impact):** описание возможного влияния слабости на инфраструктуру;
- **Рекомендации по устранению (Remediation):** рекомендации по устранению;
- **Подробности (More info):** ссылки на внешние источники с дополнительной информацией.

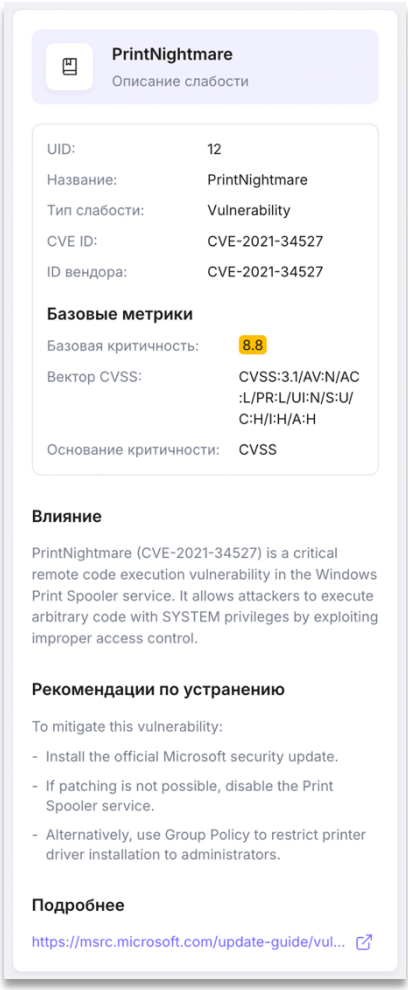


Рисунок 23: Карточка слабости из БЗ

5.8 Как увидеть описание любых действий?

Подробную информацию о *конкретном* действии в проекте можно получить в Журнале действий (Action Log), а статьи с описанием разных *типов* действий доступны в Базе знаний (Knowledge Base).

5.8.1 В Журнале действий (Action Log)

Раскройте карточку *конкретного* действия, чтобы изучить его свойства и результаты:

- краткое описание типа действия;
- статус, оценка безопасности, временные метки, UID и другие свойства;
- **«Arguments» (Arguments)** – факты, использованные действием как входные параметры;
- **«Результаты» (Results)** – факты, которые действие обнаружило или подтвердило в результате выполнения.

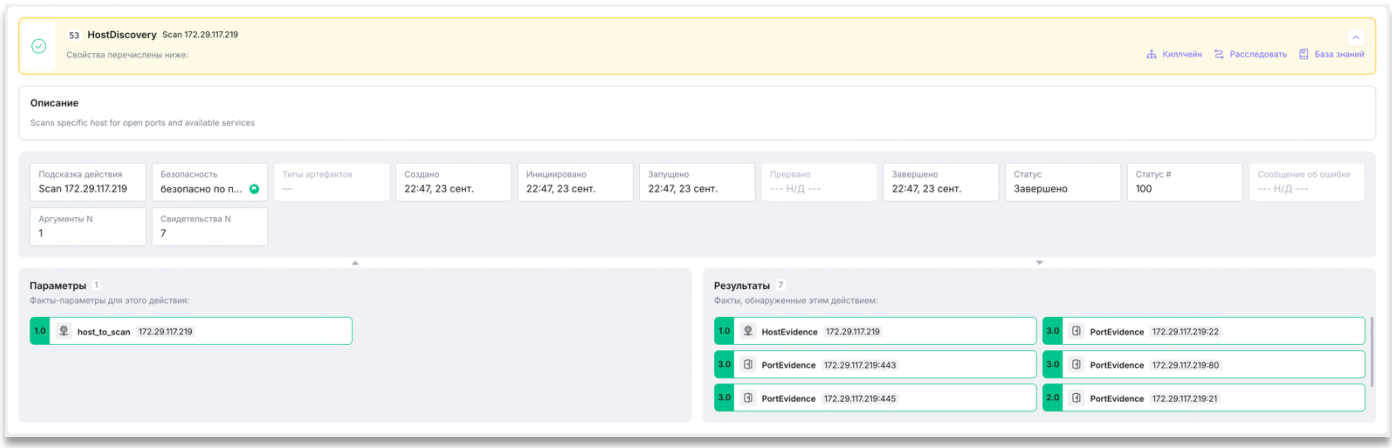


*Рисунок 24: Описание **конкретного** действия в рамках проекта в раскрытой карточке Журнала действий (Action Log)*

5.8.2 В Базе знаний (Knowledge Base)

База знаний содержит статьи с описанием *типов* действий. Статья может включать:

- общее описание;
- оценку безопасности применения действия в сети организации;
- ссылку на GitHub с техниками, встроенными в систему;
- создаваемые артефакты;
- рекомендации по обнаружению и предотвращению;
- ссылки на MITRE ATT&CK.

Открыть статью можно из бокового меню навигации или по ссылке в карточке действия – иконка .

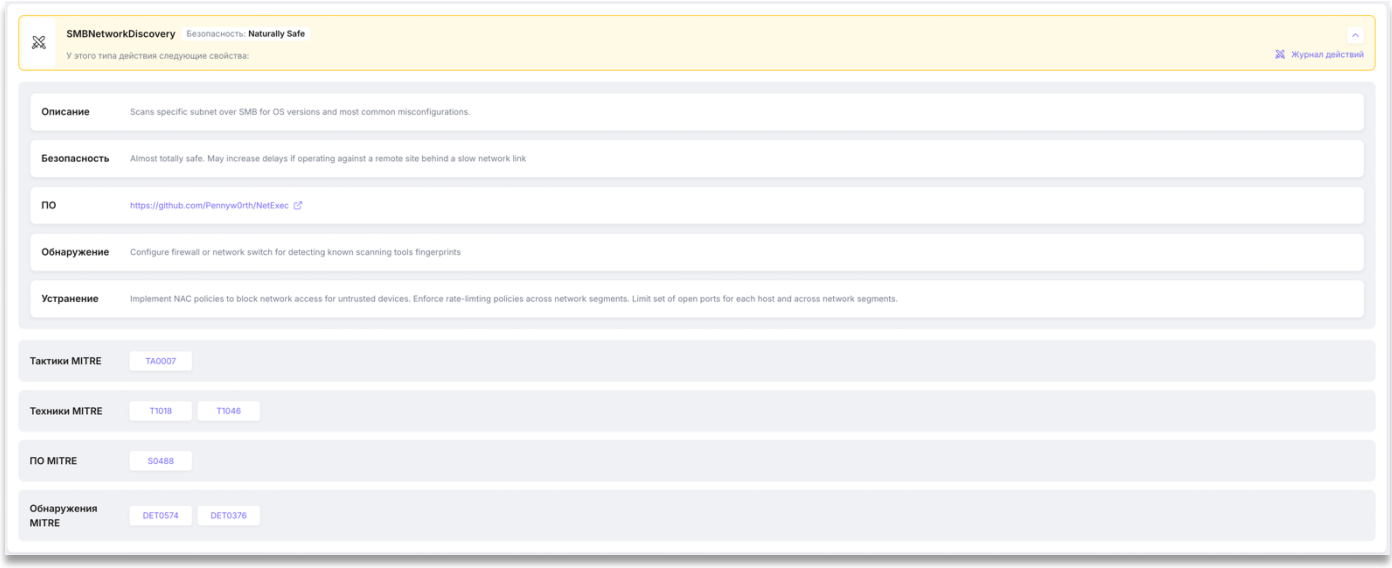


*Рисунок 25: Карточка с описанием отдельного **типа** действия в Базе знаний (Knowledge Base)*

5.9 Как сформировать отчёт по проекту?

Для формирования отчёта используется Конфигуратор отчёта (Report Builder). Отчёт можно составить в любое время – как в ходе проекта, так и по его завершении.

Откройте Конфигуратор отчёта через боковое меню навигации – иконка . При открытии окна сразу начинается создание отчёта: в шаблон загружаются данные и статистика проекта.

5.9.1 Подразделы отчёта

- Обзор (Overview): общая статистическая информация о проекте;
- Слабости (Weaknesses): выявленные слабости с разбивкой по критичности;
- Трофеи (Trophies): наиболее ценные находки системы;
- Действия (Actions): общая статистика по действиям проекта во всех статусах: Предложенные (Suggested), Выполняются (Running), Завершённые (Completed), Результативные (Fruitful).

В ходе настройки в рабочей области окна отображается прокручиваемый макет отчёта с учётом всех внесённых изменений.

5.9.2 Настройка отчёта

В боковой панели справа находится конфигуратор, позволяющий настроить итоговый документ:

- включать или выключать отдельные подразделы (Report Sections);
- настраивать пороги критичности для отображения слабостей (Weakness Thresholds);
- настраивать пороги ценности для отображения трофеев (Trophy Thresholds);
- ограничивать количество отображаемых трофеев;

- для подраздела «Действия» (Actions) – оставлять в отчёте только те типы действий, которые были результативными в рамках проекта.

5.9.3 Экспорт отчёта

Для печати или сохранения отчёта в PDF используйте кнопку с иконкой принтера в левом нижнем углу.

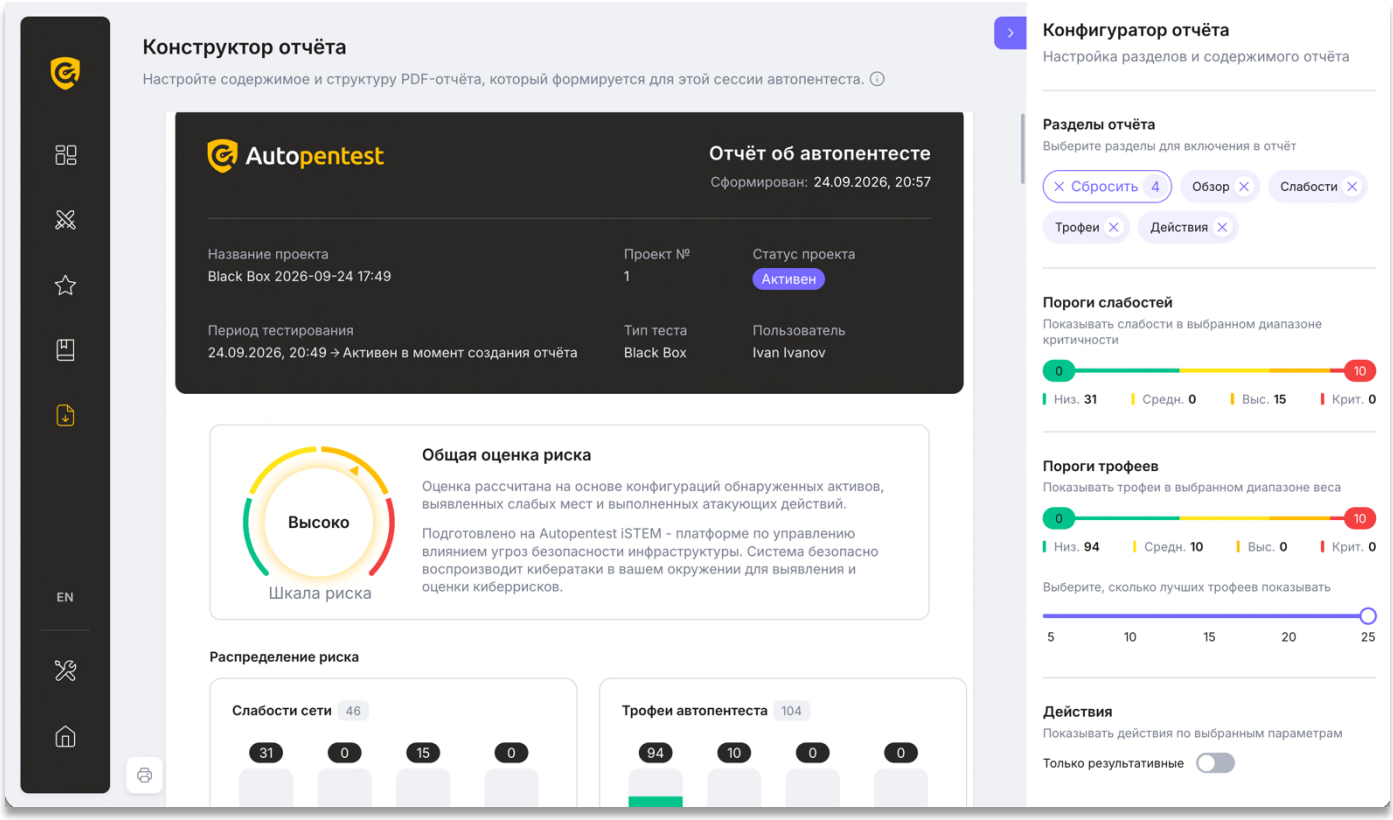


Рисунок 26: Конфигуратор отчёта (Report Builder)

6 СПРАВОЧНИК ПО ИНТЕРФЕЙСУ

Веб-интерфейс – основной инструмент работы оператора с Платформой, через который доступны: настройка и управление проектами, мониторинг хода тестирования, просмотр фактов и выполненных действий, анализ цепочек атак, формирование отчётов.

Все операции, доступные в веб-интерфейсе, могут выполняться и через API Платформы, а некоторые возможности доступны только через API. API поставляется с автоматическим документированием. Документацию по API можно получить по адресу:

```
https://<autopentest_host>:8443/api/docs#
```

Справочник по интерфейсу сгруппирован по тематическим подразделам:

- Навигация по интерфейсу;
- Работа с проектами;
- Основные окна;
- Инструменты анализа;
- Вспомогательные окна;
- Ручное управление данными.

6.1 Навигация по интерфейсу

6.1.1 Боковое меню навигации по проекту

Боковое меню используется для переключения между функциональными окнами внутри проекта. В нём доступны основные окна:

- Панель управления (Dashboard) – ;
- Журнал действий (Action Log) – ;
- Список фактов (Fact List) – ;
- База знаний (Knowledge Base) – ;
- Конфигуратор отчёта (Report Builder) – ;
- Конфигуратор проекта (Project Configurator) - .

Помимо этого, в меню есть иконка «Выйти из проекта», возвращающая к списку проектов - .

Окна специального назначения

Часть окон не вынесена в боковое меню, поскольку они открываются в контексте конкретного факта или действия:

- Пользовательские факты (User Input) – открывается по кнопке + в панели «Факты» или + Добавить факт (+ Add fact) в конфигураторе проекта;
- Создать действие (Create Action) – открывается по кнопке + Запустить действия (+ Run actions) в верхней части Журнала действий (Action Log);
- Киллчейн (Kill Chain) – , Инспектор структуры (Structure) – , Расследование (Investigation) – – открываются по ссылкам-иконкам на карточках фактов и действий.

Такой подход позволяет работать с окнами в контексте: например, построить цепочку атаки именно для выбранного факта или действия.

6.1.2 Глобальная навигационная цепочка (Breadcrumbs)

В интерфейсе реализован компонент навигации, сохраняющий контекст расследования при переключении между окнами. Пример маршрута:

- Панель управления → Киллчейн (анализ трофея) → База знаний (изучение действия) → Журнал действий (фильтр по типу) → Расследование (детальный анализ) → Инспектор структуры (контекст инфраструктуры).

Система запоминает шаги и строит цепочку «хлебных крошек», по которым можно перемещаться.

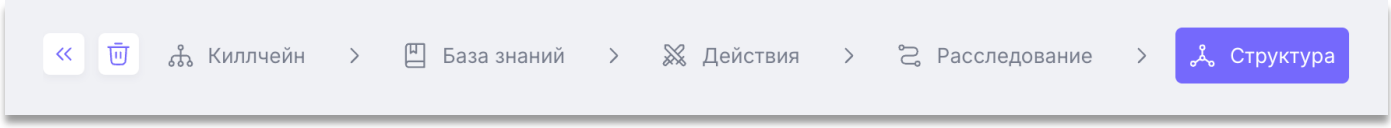


Рисунок 27: Глобальные хлебные крошки (Breadcrumbs)

Интерактив

- Состояния всех промежуточных страниц сохраняются. Если вернуться на любой шаг назад, страница восстановится в прежнем виде (например, построенный граф в Киллчейне не сбросится);
- Если вернуться на один из предыдущих шагов и начать новую ветку расследования, система с этого момента построит новую последовательность «хлебных крошек».

6.1.3 Карточки фактов и действий

В окнах интерфейса факты и действия представлены в виде карточек. Карточки имеют единый цветовой код, помогающий быстро различать типы объектов:

- действия — сиреневые;
- факты — белые, с цветовыми элементами, отражающими уровень критичности или ценности конкретного факта с точки зрения атакующего.

Цветовой код един для всех окон интерфейса: Панели управления (Dashboard), Журнала действий (Action Log), Списка фактов (Fact List), Киллчейна (Kill Chain), Инспектора структуры (Structure) и других.

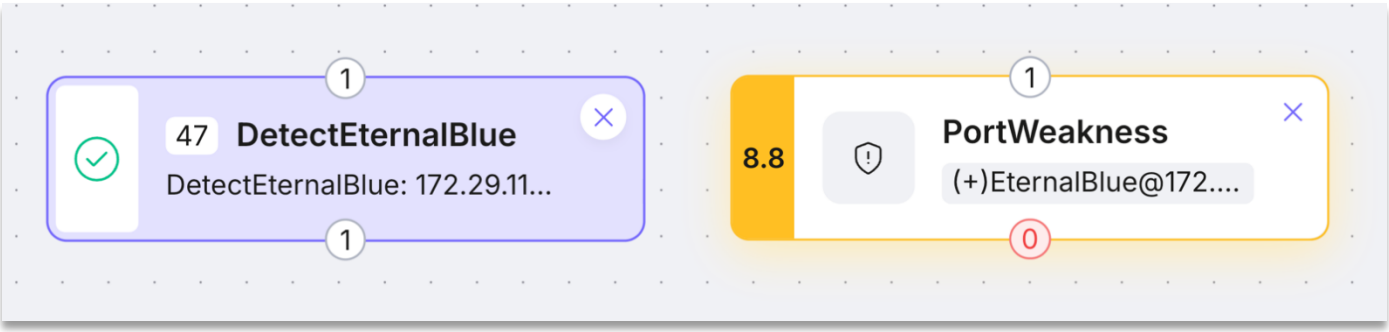


Рисунок 28: Пример карточек фактов и действий

6.2 Работа с проектами

6.2.1 Список проектов (Autopentest Projects)

При входе в систему отображается окно со списком проектов. Оно содержит все существующие проекты с указанием их идентификаторов, названий, временных меток и статусов.

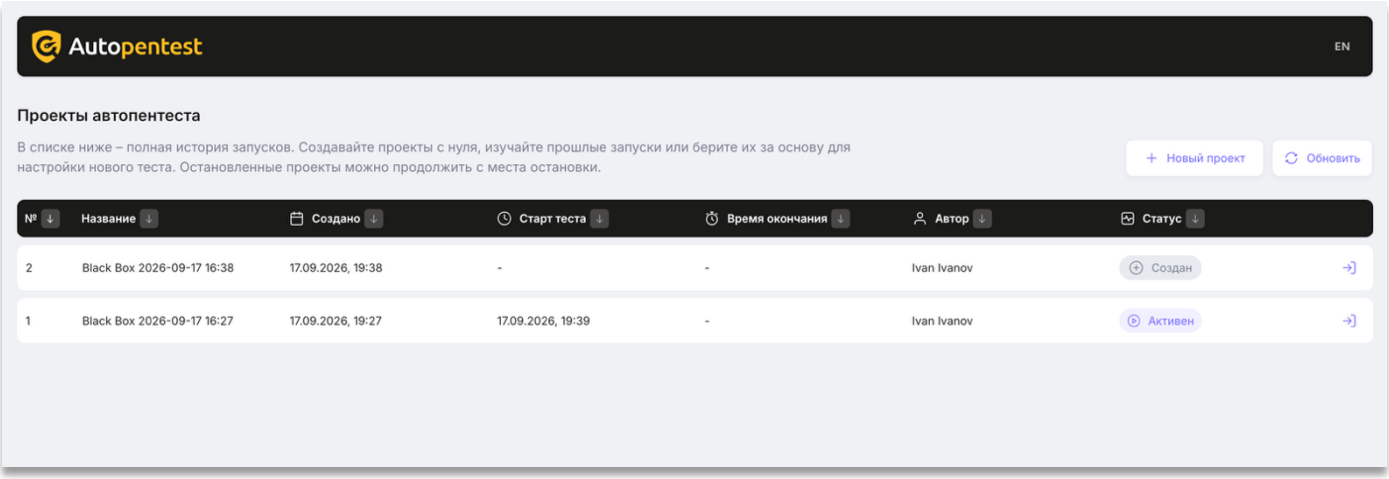


Рисунок 29: Список проектов (Autopentest Projects)

Интерактив

- **Создать новый проект**: нажмите кнопку + Новый проект (+ New Project). Будет создан проект со статусом «Создан» (Created).
- **Перейти в существующий проект**: щёлкните по строке выбранного проекта.

- **Вернуться к списку проектов**: находясь внутри проекта, нажмите иконку (Выйти из проекта) в боковом меню навигации.

6.2.2 Конфигуратор проекта (Project Configurator)

Используется для настройки параметров проекта. Редактируемые параметры можно изменять в любое время – как до, так и после запуска проекта.

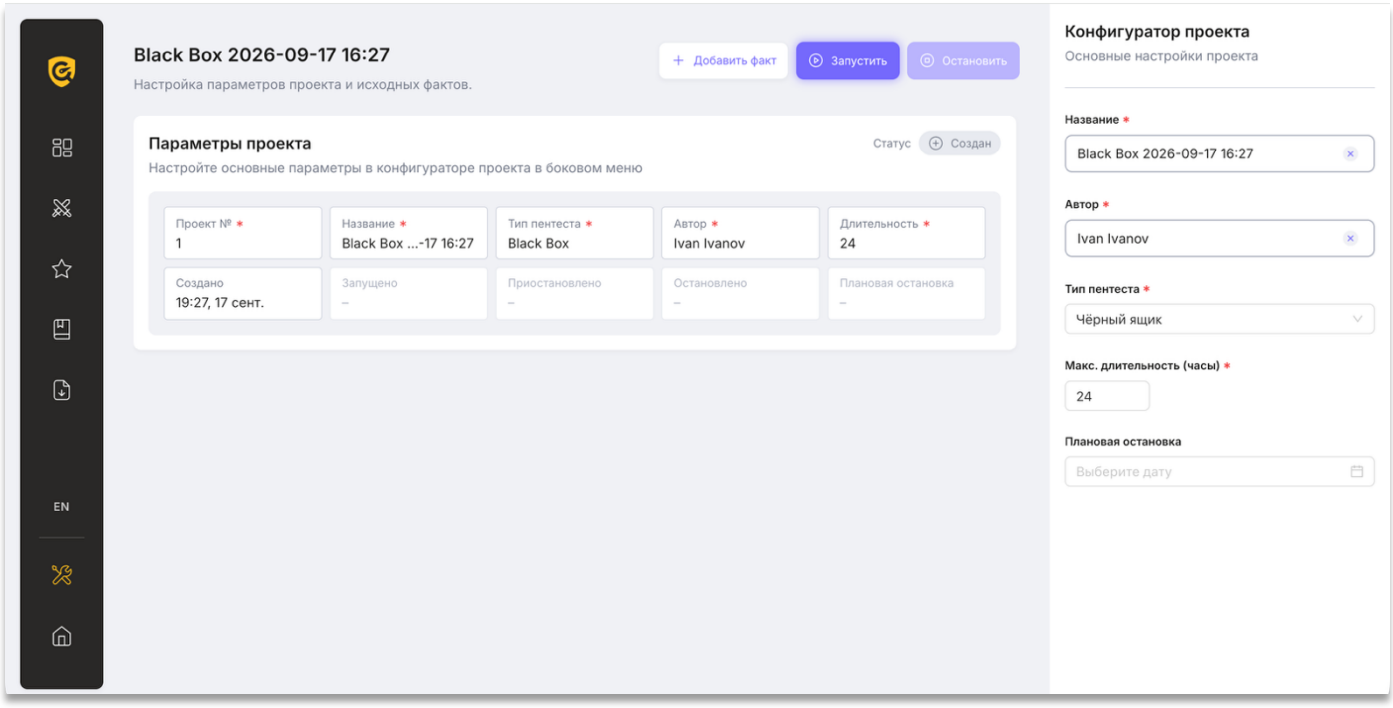


Рисунок 30: Конфигуратор проекта (Project Configurator)

Окно открывается при создании нового проекта. Чтобы открыть его изнутри текущего проекта, нажмите иконку «Конфигуратор проекта» (Project Configurator) в боковом меню навигации – .

Управление проектом

В окне конфигуратора доступно управление проектом (запуск, остановка, пауза, возобновление). Управление осуществляется кнопками в верхней части окна. Доступные действия зависят от текущего статуса проекта:

- Проект в статусе «Создан» (Created) или «Окончен» (Stopped) можно запустить ;
- Проект в статусе «Активен» (Running) можно поставить на паузу или остановить ;
- Проект в статусе «Пауза» (Paused) можно возобновить или остановить .

Одновременно может быть запущен только один проект.

Базовые параметры

Базовые параметры редактируются в боковом меню конфигуратора справа:

- название проекта;
- имя автора;
- продолжительность проекта.

Дополнительные параметры

Для настройки нового проекта необходимо задать как минимум:

- **IP-диапазоны (IPRange)** – определяют границы пентеста (Pentest Scope). Минимальное требование для запуска проекта;
- **учётные данные** – факты типа NTAccount, NTPassword и другие. Добавляются для тестирования в модели «серый ящик».

В проект могут быть добавлены и любые другие типы фактов. Подробнее см. раздел 6.6.1.

6.3 Основные окна

6.3.1 Панель управления (Dashboard)

Окно «Панель управления» используется для наблюдения за ходом проекта и его основными показателями, а также для изучения уже завершённых проектов. Ключевая задача окна – дать пользователю возможность одним взглядом определить начальные условия, базовые настройки проекта и оценить его ключевые результаты.

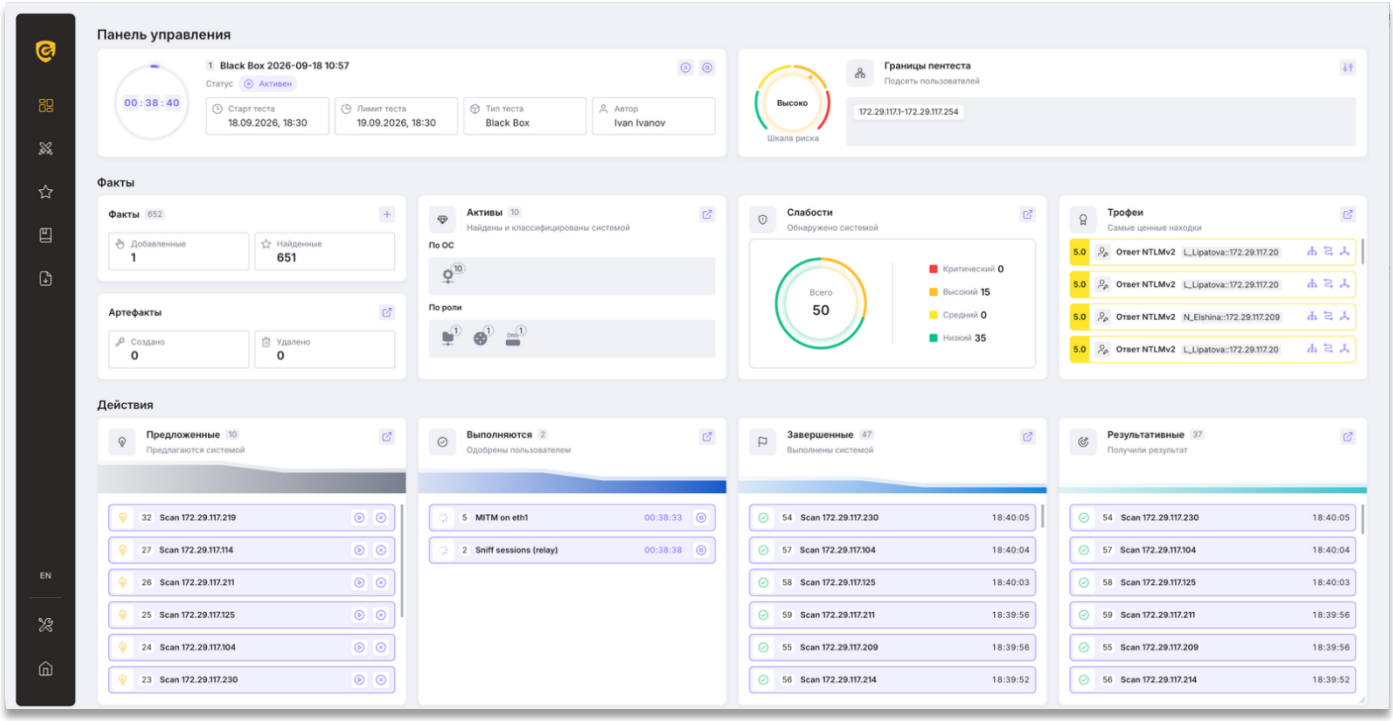


Рисунок 31: Панель управления (Dashboard)

Для открытия панели управления перейдите по ссылке в боковом меню навигации – иконка .

Окно состоит из трёх «этажей», каждый из которых включает информационные панели, разбитые по категориям: параметры и границы проекта сверху, статистика по фактам посередине и сводка по действиям внизу.

Параметры проекта

Верхняя левая панель включает базовые настройки проекта:

- таймер, показывающий время, прошедшее с момента запуска проекта;
- идентификатор и название проекта;
- текущий статус проекта;
- время запуска и время планируемой остановки проекта;
- модель теста («Чёрный ящик» или «Серый ящик»);
- имя автора проекта.

Также панель включает кнопки управления проектом, дублирующие функции кнопок управления в окне «Конфигуратор проекта».

Границы пентеста

Верхняя правая панель включает шкалу оценки риска и описание границ пентеста:

- **Шкала риска (Risk Score)** – отображает общую оценку риска в рамках проекта, рассчитываемую исходя из текущих находок и достижений системы;
- **Границы пентеста (Pentest Scope)** – перечень IP-диапазонов и адресов, установленных пользователем перед запуском и в ходе проекта.

Факты (Facts)

В центральной части представлены панели со статистикой по фактам проекта, разбитой по категориям:

- **Факты (Facts)** – общее число фактов, число добавленных пользователем (User Input), число фактов, обнаруженных системой. Панель включает кнопку-ссылку + для перехода в меню добавления пользовательских фактов;
- **Артефакты (Artifacts)** – число артефактов, созданных системой (Created), и число артефактов, удалённых системой (Deleted). Панель включает ссылку на список фактов (Fact List);
- **Активы (Assets)** – сводка по обнаруженным активам в сети, отсортированным по операционной системе (By OS) и по роли (By Role). Панель включает ссылку на список фактов (Fact List) с фильтром по активам (хостам);
- **Слабости (Weaknesses)** – сводка по выявленным слабостям окружения (уязвимостям и небезопасным конфигурациям), разбитым по уровням критичности: низкий (Low), средний (Medium), высокий (High), критический (Critical). Панель включает ссылку на список фактов (Fact List) с фильтром по слабостям;
- **Трофеи (Trophies)** – сводка по наиболее ценным находкам системы. Включает список трофеев, отсортированный по уровню ценности (weight) с точки зрения атакующего (отображаются наиболее ценные, список прокручивается).

Действия (Actions)

В нижней части представлена сводка по действиям системы в рамках проекта, разбитым по статусам:

- **Предложенные (Suggested)** – действия, которые система предлагает пользователю выполнить. Ручное одобрение или отклонение предлагаемых действий доступно прямо в панели управления, либо в других окнах интерфейса, отображающих действия;
- **Выполняемые (Running)** – действия, которые система выполняет в данный момент. Доступна ручная остановка действий – прямо в панели управления, либо в других окнах интерфейса, отображающих действия;
- **Выполненные (Completed)** – действия, которые система уже выполнила;
- **Результативные (Fruitful)** – действия, которые позволили системе обнаружить новые факты (включая как уже выполненные, так и ещё выполняемые действия).

Панели действий отсортированы по времени обновления (сверху – последние), содержат счётчики действий и обновляются в реальном времени. Списки действий на панелях можно прокручивать. Для детального изучения действий используется окно «Журнал действий» (Action Log). Панели имеют ссылки на Журнал действий.

6.3.2 Журнал действий (Action Log)

Окно «Журнал действий» содержит журнал всех действий текущего проекта и используется для детального изучения выполняемых, уже выполненных либо предлагаемых системой действий. Действия представлены в виде интерактивного списка. Карточки действий можно раскрывать, чтобы увидеть описание, свойства, а также связанные факты-аргументы (Arguments) и факты-результаты (Results).

Для открытия журнала перейдите по ссылке в боковом меню навигации – .

Интерактив

- Список действий отсортирован по времени обновления (сверху – последние), прокручивается;
- В боковой панели справа доступна фильтрация списка по типам действий;
- Доступно управление действиями: одобрение или отклонение предложенных действий, остановка выполняемых;
- У действий есть ссылка на «Базу знаний» (Knowledge Base) с подробным описанием – ;
- У действий есть ссылка на «Киллчейн» (Kill Chain), показывающую действия в контексте текущего проекта с учётом взаимосвязей с другими действиями и фактами – ;

- У действий есть ссылка на окно «Расследование» (Investigation) – ;
- В верхней части окна находится кнопка + Запустить действия (+ Run actions) для ручного запуска действия без ожидания предложения от системы. Подробнее см. раздел 6.6.2.

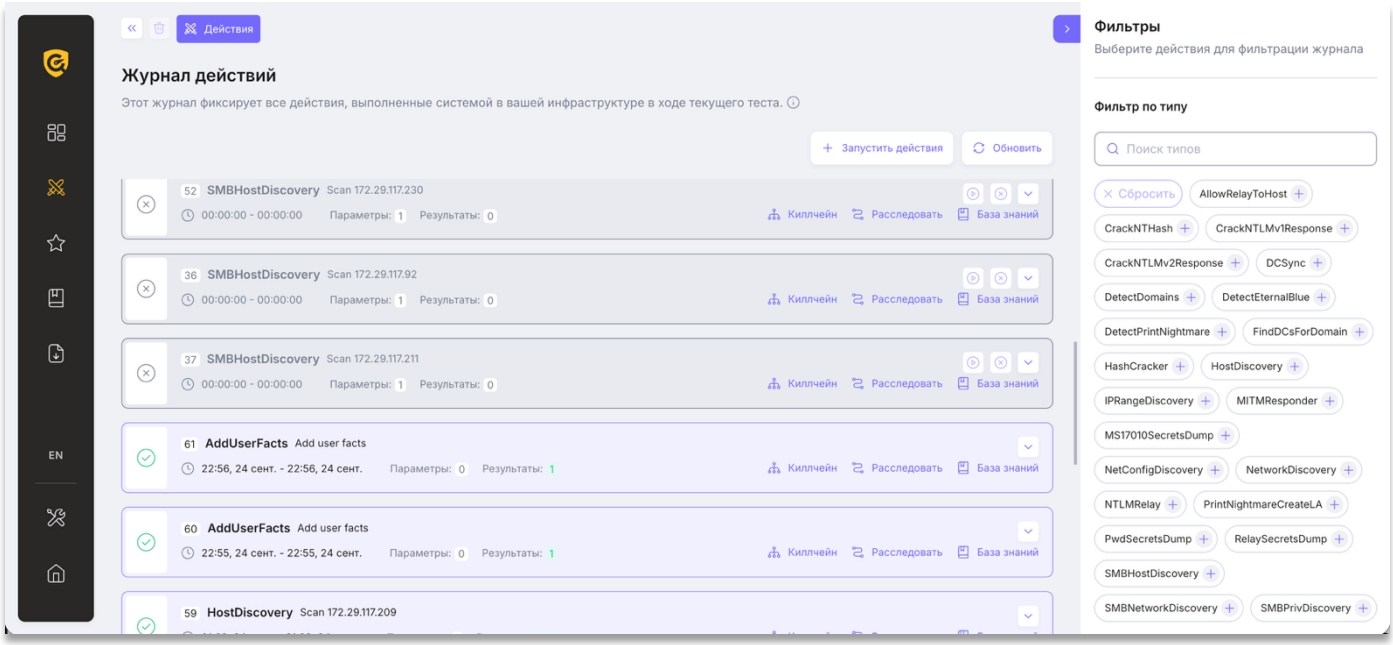


Рисунок 32: Журнал действий (Action Log)

6.3.3 Список фактов (Fact List)

Окно «Список фактов» содержит все факты текущего проекта: как добавленные пользователем, так и найденные системой автоматически. Артефакты (факты, созданные системой, например, учётные записи, сессии и пр.) также отображаются в этом окне. Факты представлены в виде интерактивного списка. Карточки фактов можно раскрывать, чтобы увидеть описание, свойства, а также связанные с ними подтверждающие действия (Verifications) и действия, использовавшие эти факты в работе (Usage).

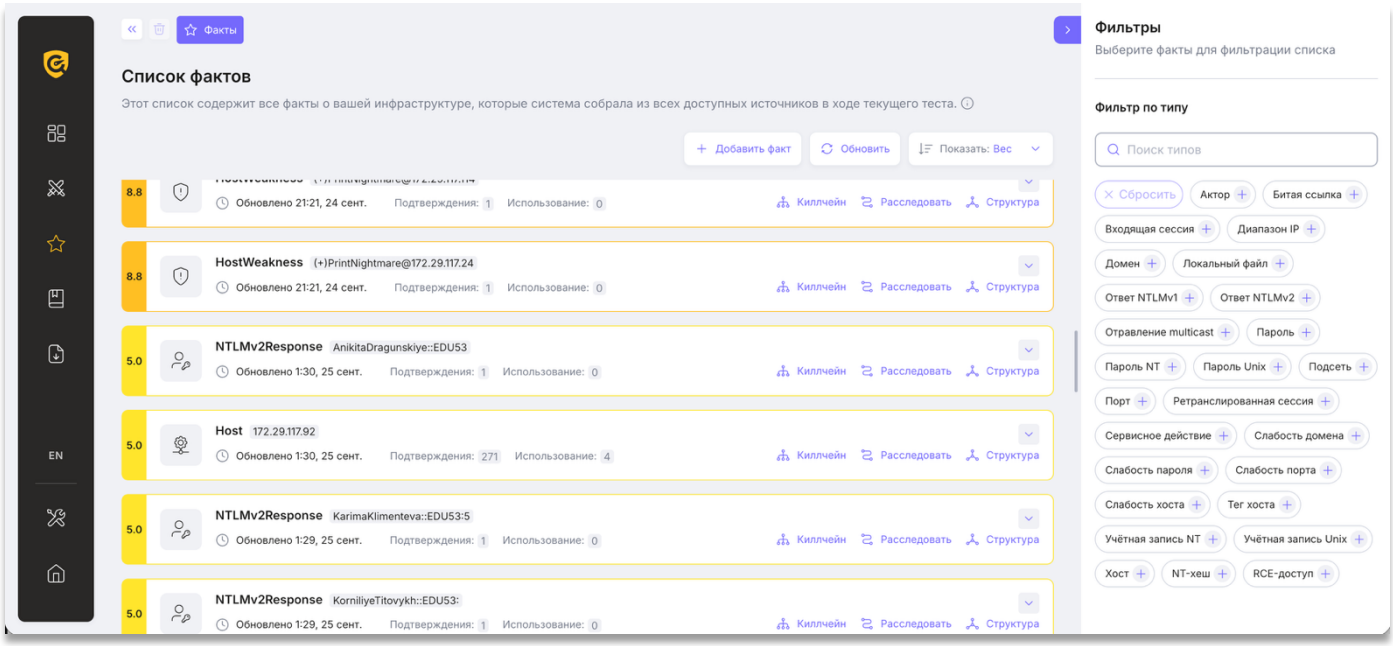


Рисунок 33: Список фактов (Fact List)

Для открытия списка фактов перейдите по ссылке в боковом меню навигации – .

Интерактив

- Список прокручивается, отсортирован по уровню ценности (сверху – наиболее ценные);
- Можно менять порядок сортировки (по уровню ценности или времени обновления, по возрастанию или убыванию) с помощью кнопки-сортировщика в верхней части окна;
- В боковой панели справа доступна фильтрация списка по типам фактов;
- У фактов есть ссылка на «Киллчейн» (Kill Chain), позволяющую увидеть факты в контексте текущего проекта с учётом взаимосвязей с другими фактами и действиями – ;
- У фактов есть ссылка на «Инспектор структуры» (Structure), позволяющий взглянуть на факты в контексте текущего окружения и увидеть инфраструктуру глазами атакующего – ;
- У фактов есть ссылка на окно «Расследование» (Investigation) – ;

В верхней части окна есть кнопка-ссылка + Добавить факт (+ Add fact) для ручного добавления любых типов фактов в окне «Пользовательские факты» (User Input).

6.4 Инструменты анализа

6.4.1 Киллчейн (Kill Chain)

В окне «Киллчейн» автоматически или вручную генерируется интерактивная визуализация цепочек атаки в виде графа. В качестве начальной точки для построения графа используются любые факты или действия проекта. Киллчейн демонстрирует причинно-следственные связи между действиями и фактами в контексте цепочки атаки. Граф позволяет пошагово анализировать развитие атаки на любую доступную глубину как в перспективу (вперёд по цепочке), так и в ретроспективу (назад к корневым причинам).

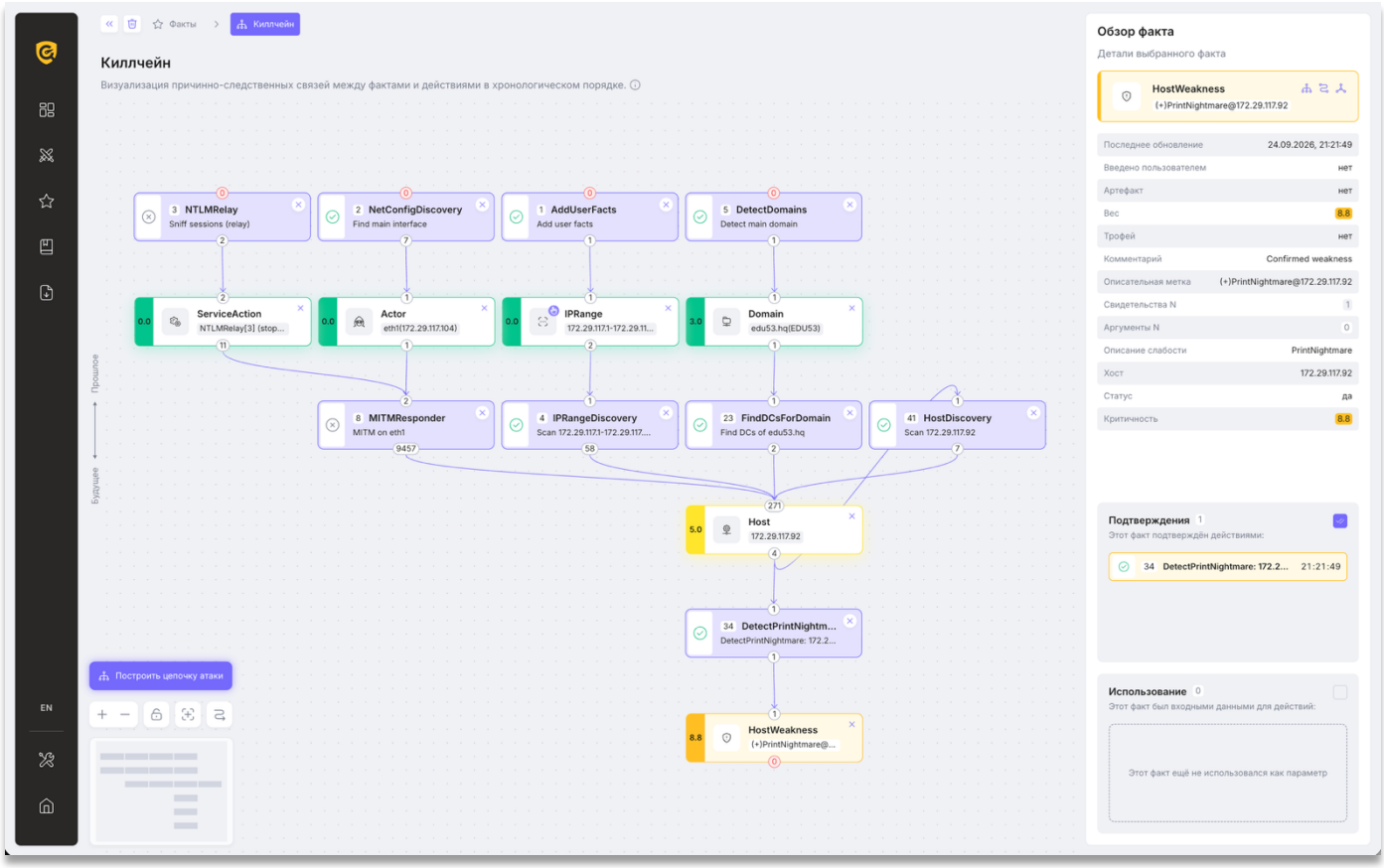


Рисунок 34: Киллчейн (Kill Chain)

Интерактив

- При открытии в рабочей области отображается карточка того факта или действия, с которого был инициирован переход в Киллчейн, а на панели справа приводится детализация:

  - для фактов: свойства факта и связанные с ним интерактивные списки подтверждающих и использующих действий;
  - для действий: свойства действия и связанные с ним интерактивные списки фактов-аргументов и фактов-результатов;
- Для автоматического построения цепочки атаки в ретроспективу используется кнопка Построить цепочку атаки (Generate Full Attack Vector) на панели управления слева внизу;
- Используя вспомогательные элементы управления на панели графа (внизу слева), можно увеличивать/уменьшать граф, блокировать ручное перетаскивание вершин, центрировать изображение, анимировать стрелки графа;
- Внизу слева также отображается миниатюра графа для быстрой навигации;
- Для ручного построения графа в ретроспективу или перспективу выбираются взаимосвязанные факты и действия в интерактивных списках на панели справа;
- Любые элементы графа можно перетягивать, удалять или открывать в других окнах проекта (инструментах анализа), используя ссылки на них в панели справа (, , ,).

6.4.2 Инспектор структуры (Structure)

Платформа формирует и отображает интерактивную модель инфраструктуры на основе фактов, полученных системой в ходе тестирования, либо добавленных пользователем из внешних источников (через «Пользовательские факты» (User Input) или API). Модель включает сведения об обнаруженных объектах, их свойствах и взаимосвязях, значимых с точки зрения развития атаки.

Это позволяет анализировать инфраструктуру с позиции атакующего и понимать, какие возможности доступа и перемещения возникают в сети в результате выполненных действий.

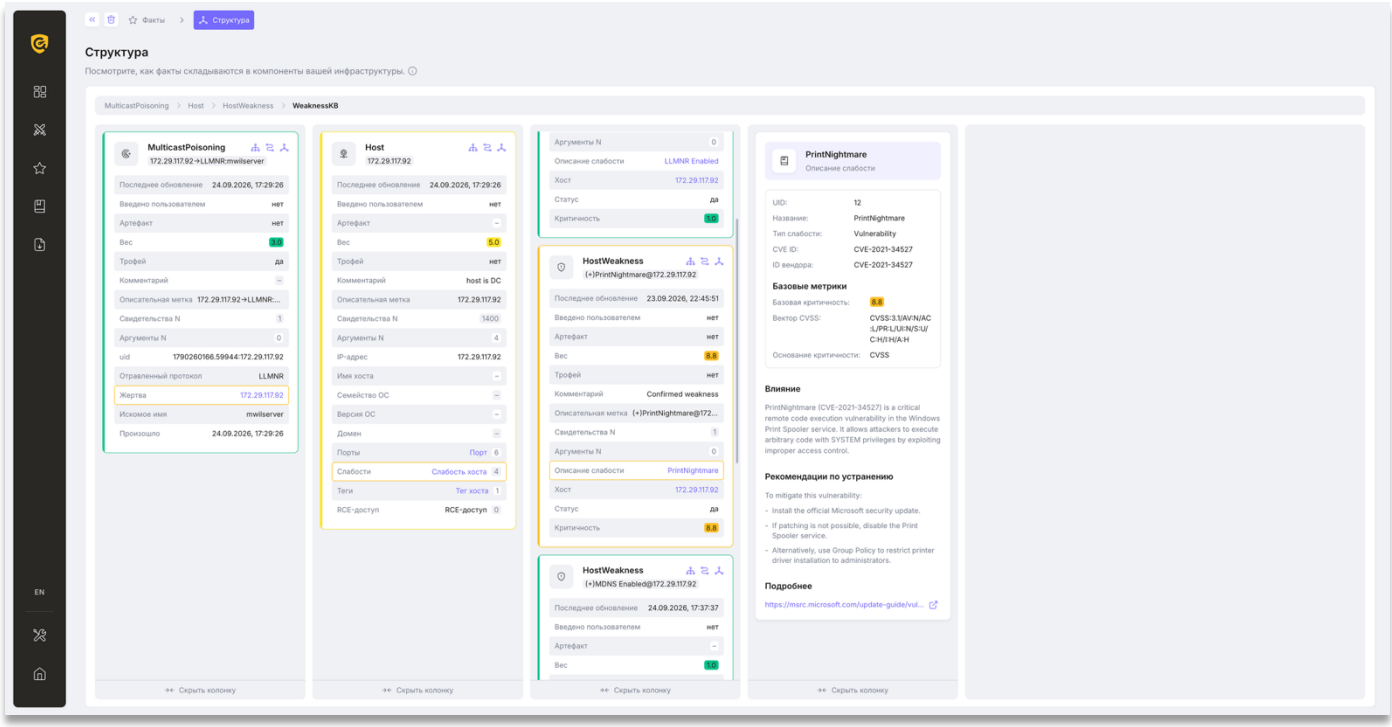


Рисунок 35: Инспектор структуры (Structure)

Для открытия Инспектора структуры перейдите по ссылке, доступной в окнах, где отображаются карточки фактов — .

Интерактив

- При открытии в рабочей области отображается карточка того факта, с которого был инициирован переход в Инспектор структуры. Карточки представленных фактов отображаются в вертикальном виде вместе с их параметрами;
- Для ручного построения таблицы связей фактов щёлкните по полям-ссылкам;

- Отдельные столбцы с данными можно сворачивать или разворачивать для фокуса на наиболее ценной информации;
- Таблица имеет горизонтальную прокрутку. Для быстрого перемещения между столбцами используйте «хлебные крошки» в верхней части таблицы;
- В Инспекторе структуры доступны карточки из базы знаний с описанием слабостей (Weakness Knowledge Base, Weakness KB);
- Факт любого типа можно раскрыть для анализа в других окнах проекта (инструментах анализа), используя ссылки в заголовках карточек (, ,).

6.4.3 Расследование (Investigation)

Окно «Расследование» позволяет выстраивать цепочки взаимосвязанных фактов и действий на линии времени.

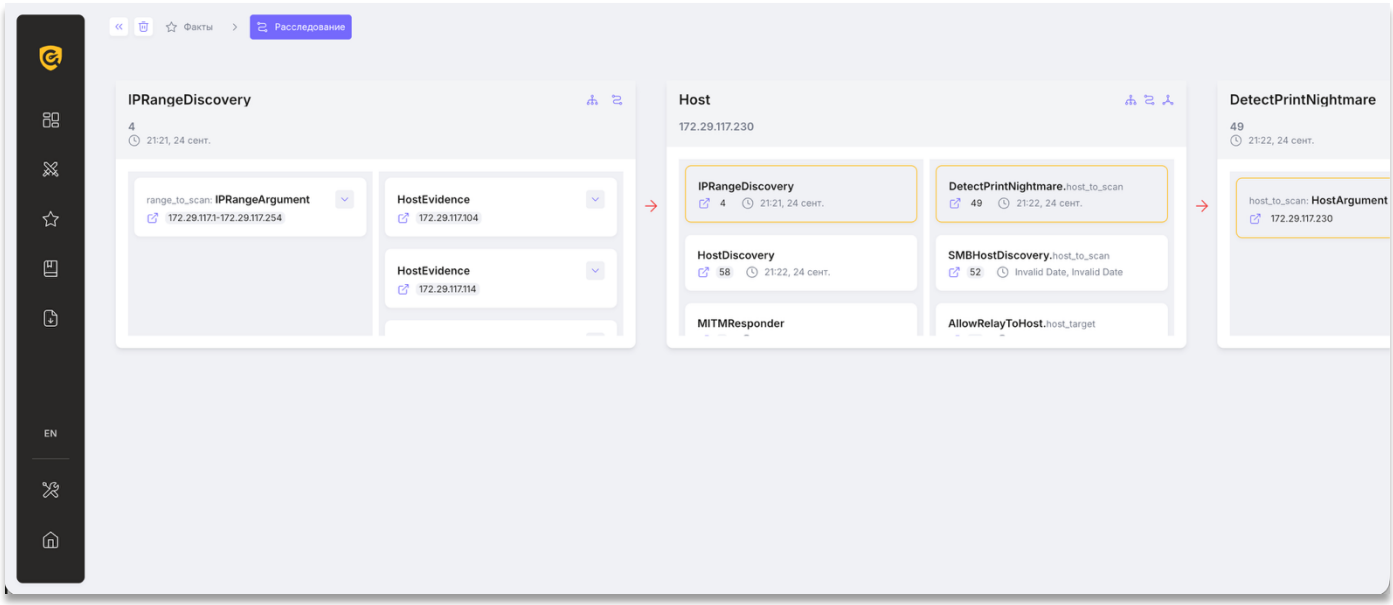


Рисунок 36: Расследование (Investigation)

Для открытия Расследования перейдите по ссылке, доступной в окнах, где отображаются карточки фактов и действий — .

Интерактив

- При открытии в рабочей области отображается карточка того факта или действия, с которого был инициирован переход в Расследование. В карточке приводится детализация:
  - для фактов: связанные с ними интерактивные списки подтверждающих и использующих действий;
  - для действий: связанные с ними интерактивные списки фактов-параметров и фактов-результатов;
- Для построения таблицы связей в текущей версии щёлкните по вложенным карточкам.

6.5 Вспомогательные окна

6.5.1 База знаний (Knowledge Base)

База знаний содержит статьи с описанием встроенных в систему действий. Каждая статья включает набор полей в зависимости от типа действия. Статья может содержать:

- общее описание;
- оценку безопасности применения действия в сети организации;
- ссылку на конкретное ПО, используемое системой для данного действия;

- создаваемые артефакты;
- рекомендации по обнаружению и предотвращению;
- ссылки на MITRE ATT&CK.

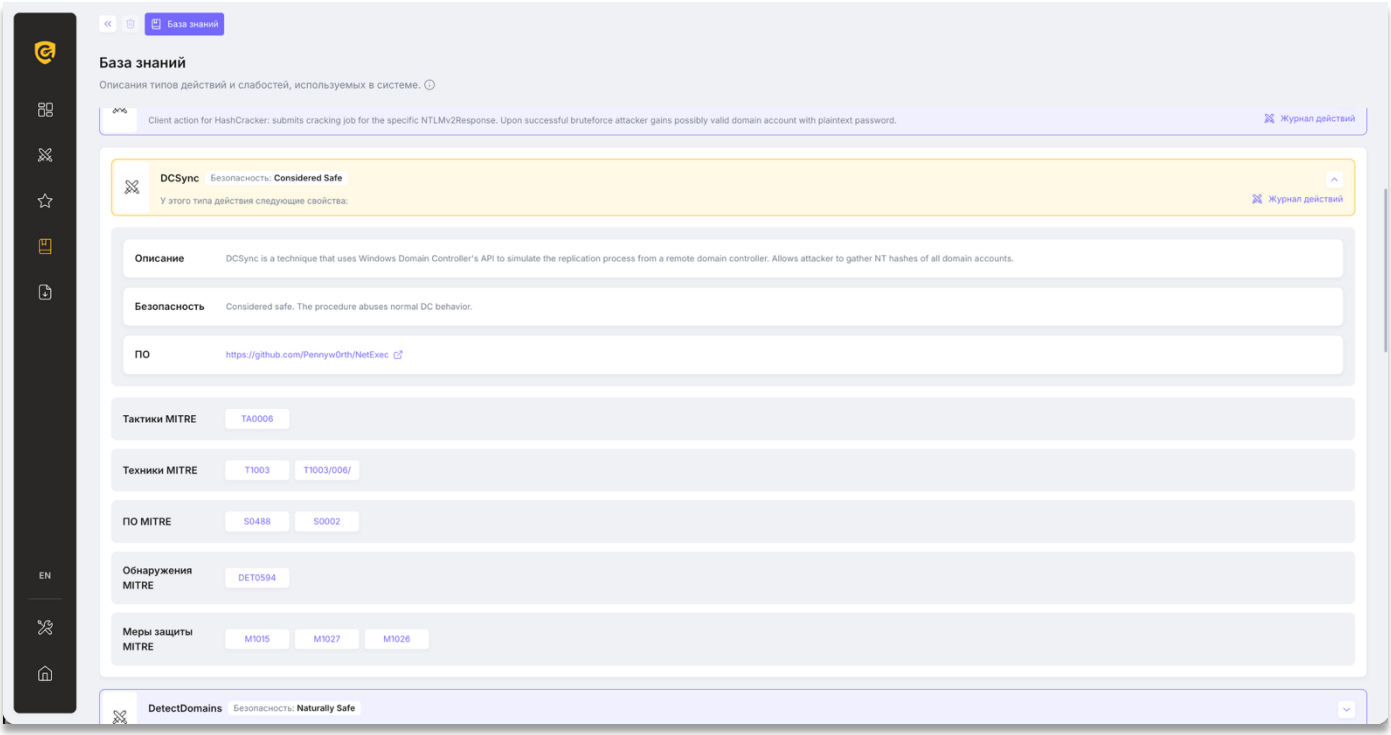


Рисунок 37: База знаний (Knowledge Base)

Для открытия Базы знаний перейдите по ссылке в боковом меню навигации или по ссылке в карточке любого действия — .

Интерактив

- При переходе из бокового меню навигации окно открывается в виде списка карточек действий, которые можно пролистывать и раскрывать для изучения;
- При переходе из карточки действия окно открывается сразу с раскрытой карточкой того типа действия, из которого был инициирован переход;
- Из любой карточки в Базе знаний можно перейти в окно «Журнал действий» (Action Log) — оно откроется с фильтром по тому типу действий, из которого был инициирован переход.

6.5.2 Конфигуратор отчёта (Report Builder)

«Конфигуратор отчёта» генерирует PDF-отчёт в ходе или по итогам проекта. Отчёт разбит на подразделы, которые можно включать или выключать из итоговой версии PDF-документа:

- **Обзор (Overview)** — общая информация о проекте;
- **Слабости (Weaknesses)** — выявленные слабости с разбивкой по критичности;
- **Трофеи (Trophies)** — наиболее ценные находки системы;
- **Действия (Actions)** — общая статистика по действиям проекта во всех статусах: Предложенные (Suggested), Выполняются (Running), Завершённые (Completed), Результативные (Fruitful).

Для открытия Конфигуратора отчёта перейдите по ссылке в боковом меню навигации — .

Интерактив

- При открытии окна сразу же начинается создание отчёта: загружаются данные и статистика проекта;
- В боковой панели справа находится конфигуратор, позволяющий настроить итоговый документ:
  - включать или выключать отдельные подразделы (Report Sections);
  - настраивать пороги критичности для отображения слабостей (Weakness Thresholds);
  - настраивать пороги ценности для отображения трофеев (Trophy Thresholds);

- ограничивать количество отображаемых трофеев;
- для подраздела «Действия» (Actions) — оставлять в отчёте только те типы действий, которые были результативными в рамках проекта;

- В ходе настройки в рабочей области окна отображается прокручиваемый макет отчёта с учётом всех внесённых изменений;
- Для печати или сохранения в PDF нажмите кнопку с иконкой принтера в левом нижнем углу.

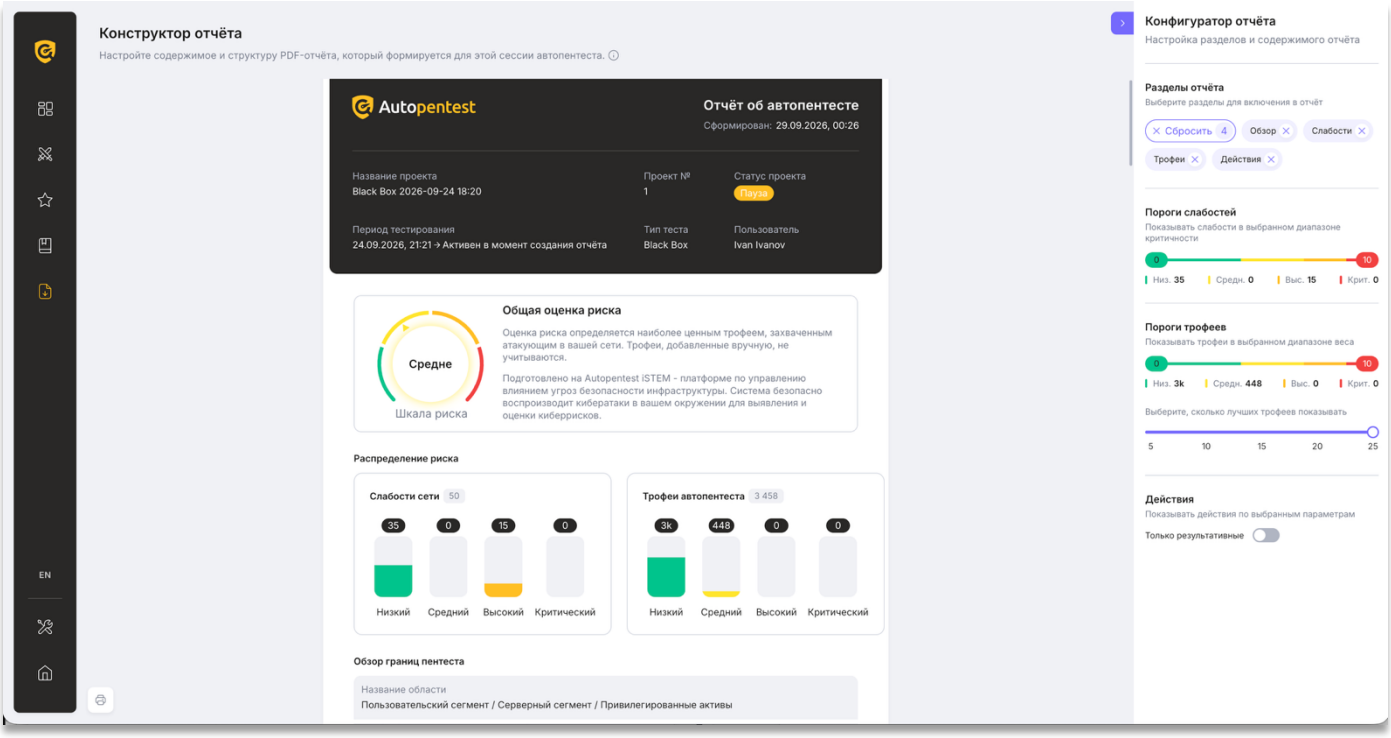


Рисунок 38: Конфигуратор отчёта (Report Builder)

6.6 Ручное управление данными

6.6.1 Пользовательские факты (User Input)

Окно «Пользовательские факты» (User Input) используется для добавления в проект любых фактов.

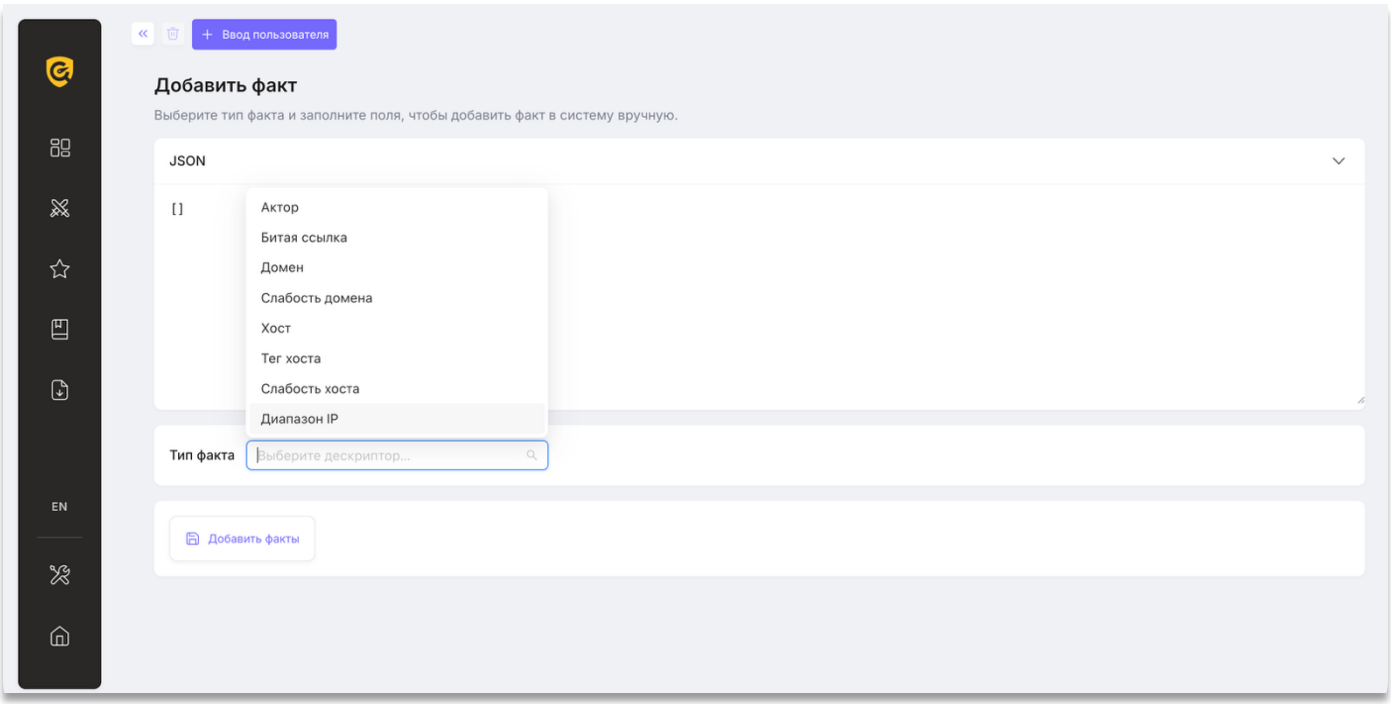


Рисунок 39: Пользовательские факты (User Input)

Для открытия окна нажмите кнопку + в панели «Факты» на Панели управления или кнопку + Добавить факт в конфигураторе проекта.

Интерактив

Добавлять пользовательские факты можно в проекты в любом статусе: «Создан» (Created), «Активен» (Running), «Пауза» (Paused) или «Окончен» (Stopped).

Инструмент позволяет вводить факты двумя способами:

- через заполнение полей формы — каждый факт добавляется отдельно;
- используя JSON — можно единовременно добавить любое количество фактов.

6.6.2 Создать действие (Create Action)

Окно «Создать действие» позволяет запускать любые действия вручную, не дожидаясь предложения от системы.

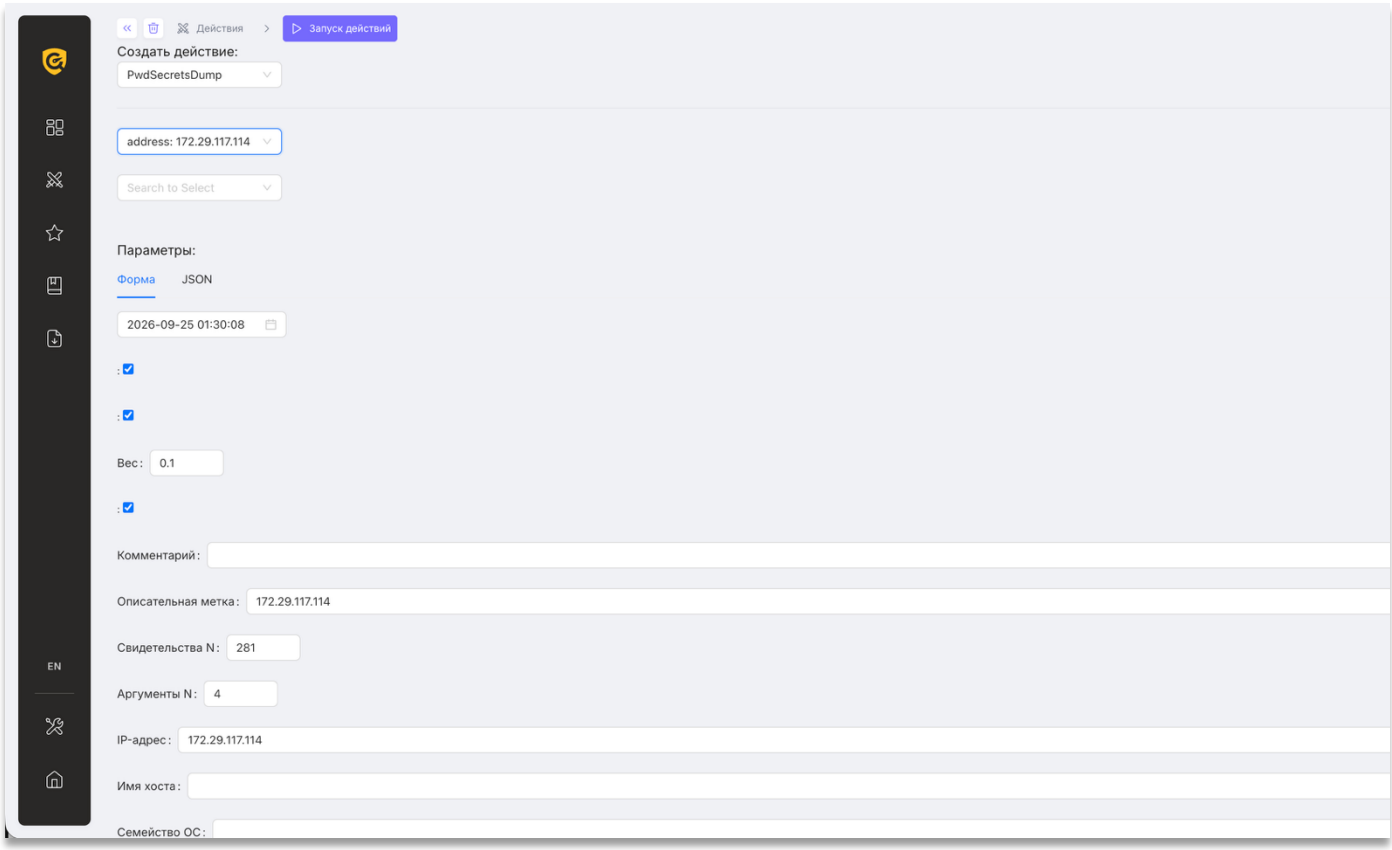


Рисунок 40: Создать действие (Create Action)

Для открытия окна нажмите кнопку + Запустить действия (+ Run actions) в верхней части окна «Журнал действий» (Action Log).

Интерактив

- При открытии окна выберите тип запускаемого действия — откроется форма с набором полей для заполнения (это факты-аргументы, необходимые в качестве параметра для выполнения действия);
- Для действий, не требующих параметров, форма не отображается, а запуск возможен сразу после выбора типа;
- Заполните обязательные поля формы — кнопка Запустить (Run) станет активной;
- Нажмите Запустить (Run) для запуска действия;
- Результат выполнения действия отображается в окне «Журнал действий» (Action Log).