Сканеры уязвимостей устарели

Почему будущее — за AI-пентестом



TRIADIX
PLATFORM

1

У кого в компании есть сканер уязвимостей?

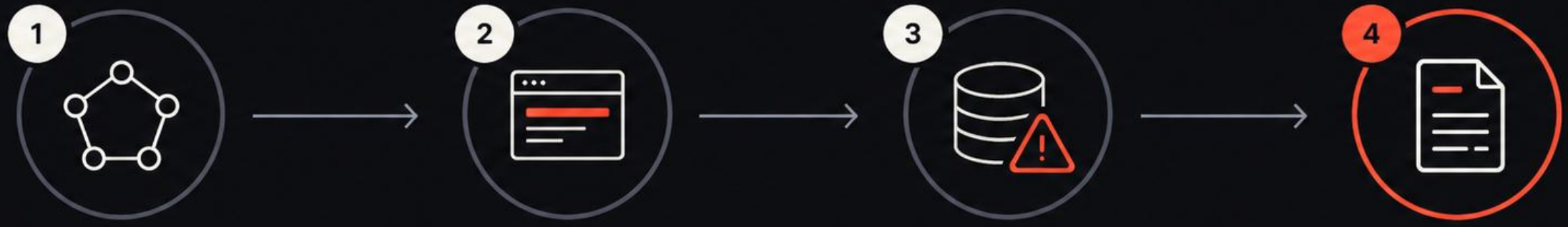


2

У кого был «зелёный» отчёт и всё равно случился инцидент?



Сканер сверяет вас с чужими поломками



Периметр

Баннеры и версии

База сигнатур и CVE

Отчёт

версия → CVE → CVSS

Сканер ищет то, что уже известно

Что сканер видит — и что нет

Видит



Известные CVE



Устаревшие версии



Типовые паттерны атак

Не видит



Неизвестные уязвимости



Ошибки логики в вашем API



Цепочки мелких находок

Обычный запрос регистрации. Что тут не так?

```
POST /register/

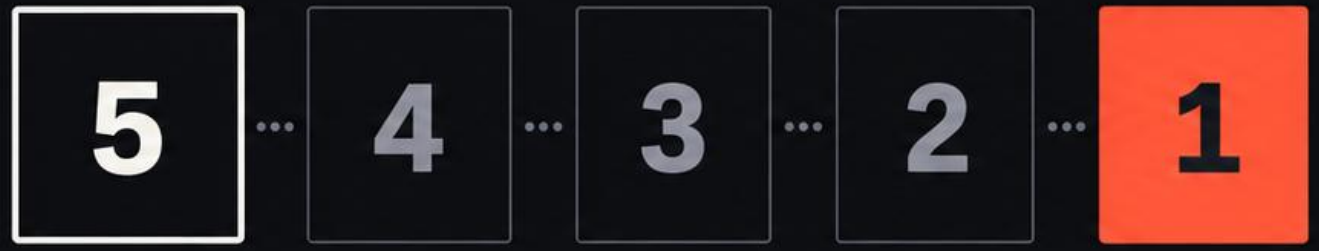
name=Ivan
email=ivan@example.com
password=********
group_id=5   ⟵ группа «обычный пользователь»

200 OK
```

Сканер: нарушений нет

Ни одной сигнатуры атаки, запрос легитимный.

Человек и агент смотрят на тот же запрос иначе



group_id: перебор соседних значений

Для каждого значения регистрирует отдельный аккаунт и сравнит видимую разницу.

	=5	=1
Меню	обычное	**админское**
API	403	**200**
Админка	нет	**полный доступ**

Одна цифра — и вы администратор. Без паролей и CVE.

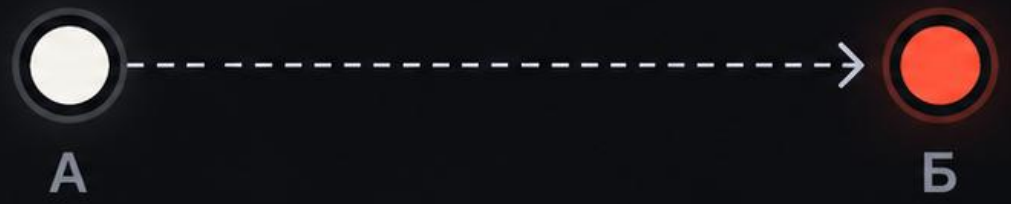
Сканер

Есть ли совпадение с базой?

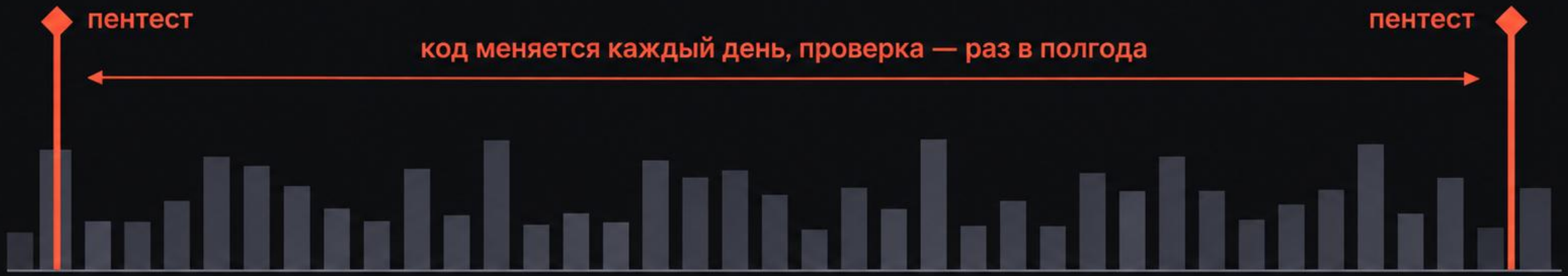


Атакующий

Как попасть из А в Б?



Ручной пентест: сильный, но редкий



Редко

Релиз во вторник, пентест в декабре

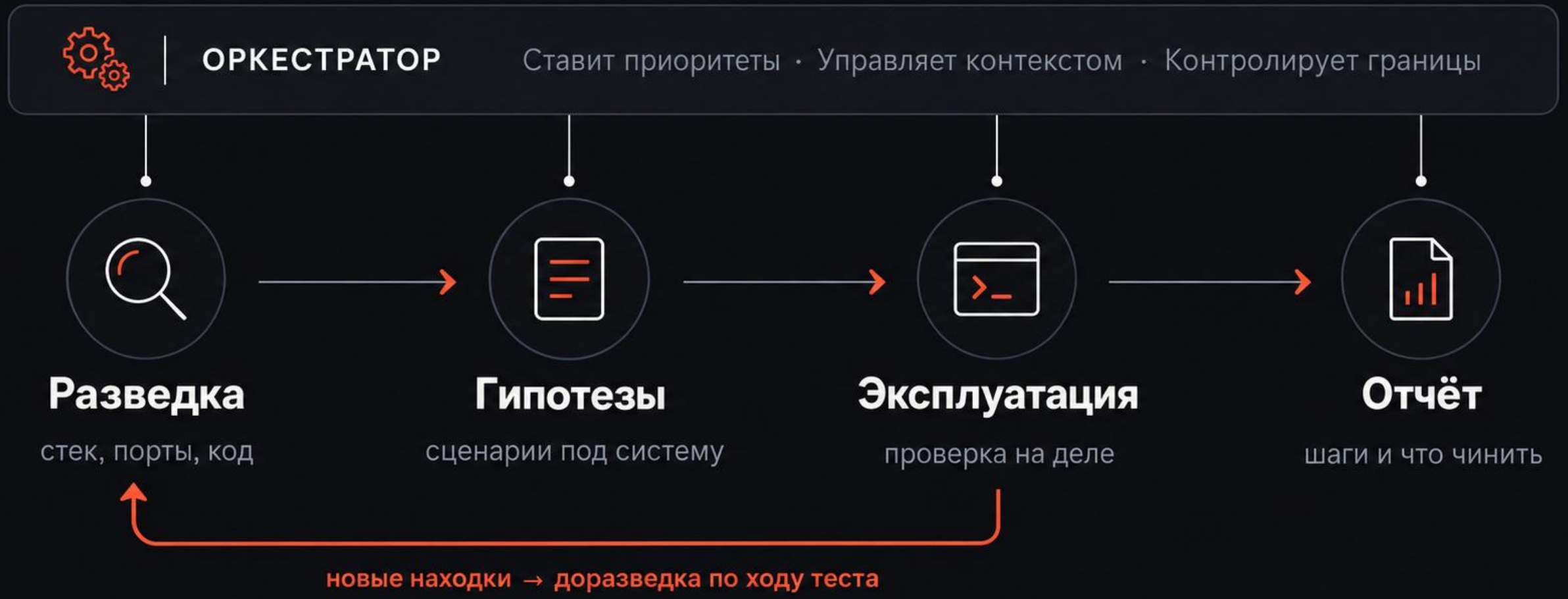
Дорого

Хороших пентестеров не так много

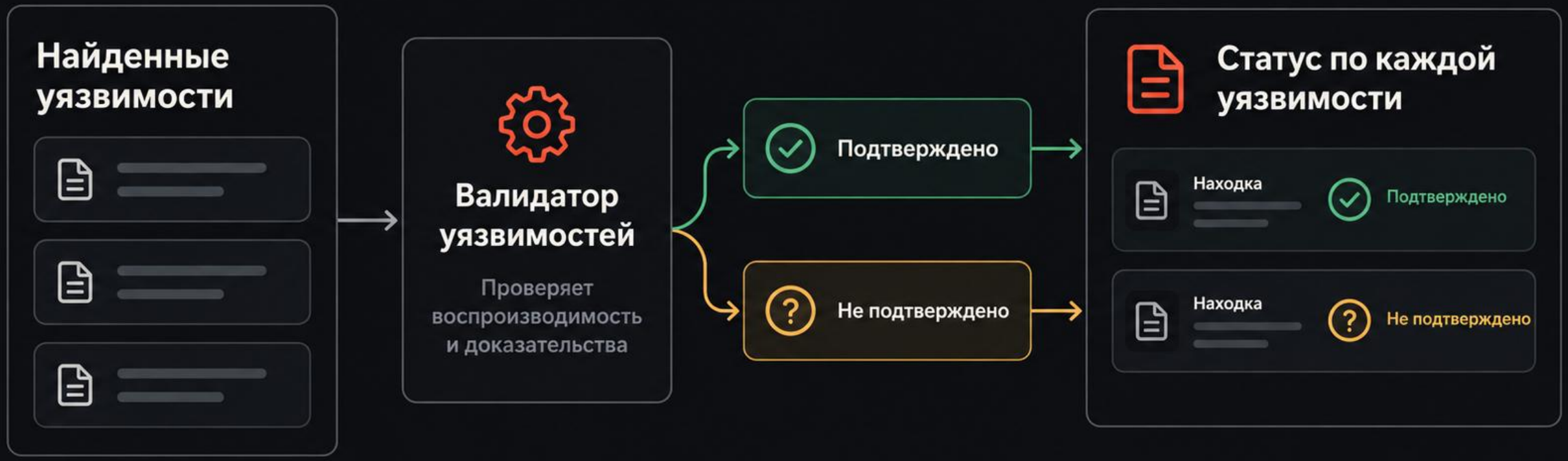
Выборочно

В пентест вложен опыт конкретного человека/команды

Команда агентов, как у живых пентестеров



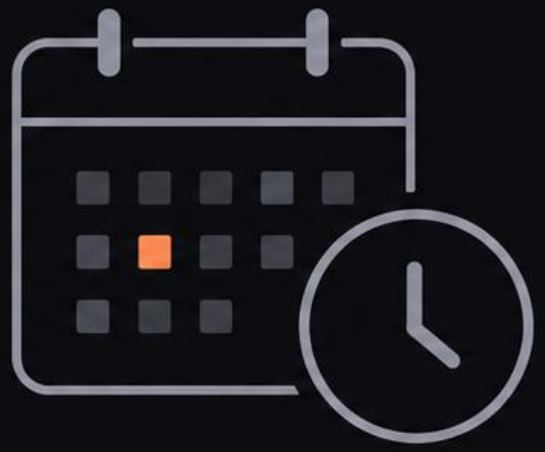
Каждая находка проходит верификацию



Все находки сохраняются с результатом проверки

Где место AI-пентеста

	Сканер	Ручной	AI-пентест
Мыслит сценариями	✗	✓	✓
Находит неизвестное	✗	✓	✓
Работает постоянно	✓	✗	✓
Масштабируется	✓	✗	✓
Для регулятора	✓	✓	🕒



Ручной пентест

Раз в год



AI-пентест

В любое время

На наших глазах формируется новый принцип CART:
Continuous Automated Red Teaming

TRIADIX: оркестратор ИИ-агентов



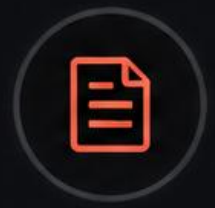
Цель: домен, приложение, API

→



Команда агентов-специалистов

→



Отчёт с доказательствами

Границы скоупа задаются при запуске



≈50

Пилотных пентестов



0

Сломанных продов

Чем отличается от DAST и BAS



DAST

Заранее заложенные шаблоны атак

BAS

Известные тактики MITRE ATT&CK

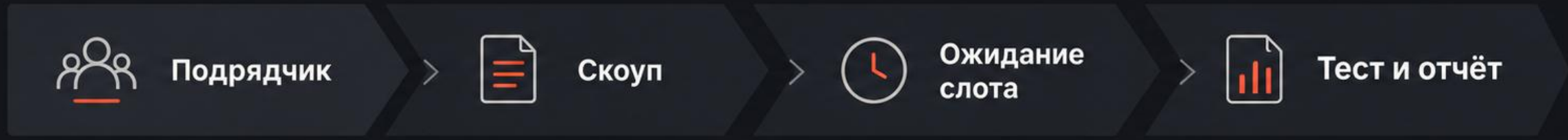
TRIADIX

Сценарий строится на лету

0day в российских продуктах с лицензиями ФСТЭК

От месяцев к часам

Классический пентест



1–2 месяца

Оркестратор ИИ-агентов

Первые находки в течение нескольких часов



Параллельно

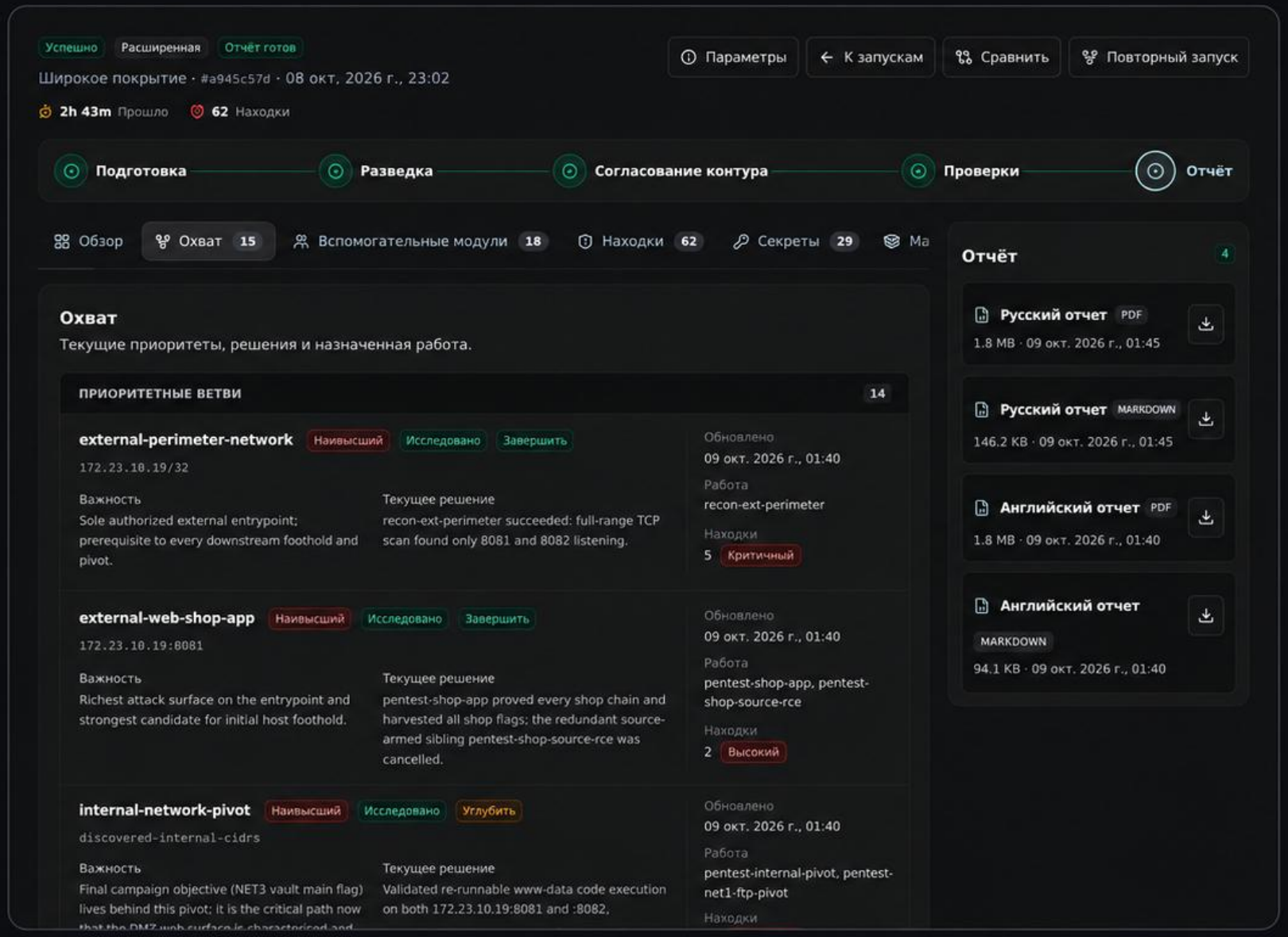
На нескольких целях сразу



По запросу

Платите за вычислительные мощности, не за человеко-часы

Какие направления уже проверены



ОХВАТ

Приоритеты

Текущие приоритеты,
решения и назначенная работа.

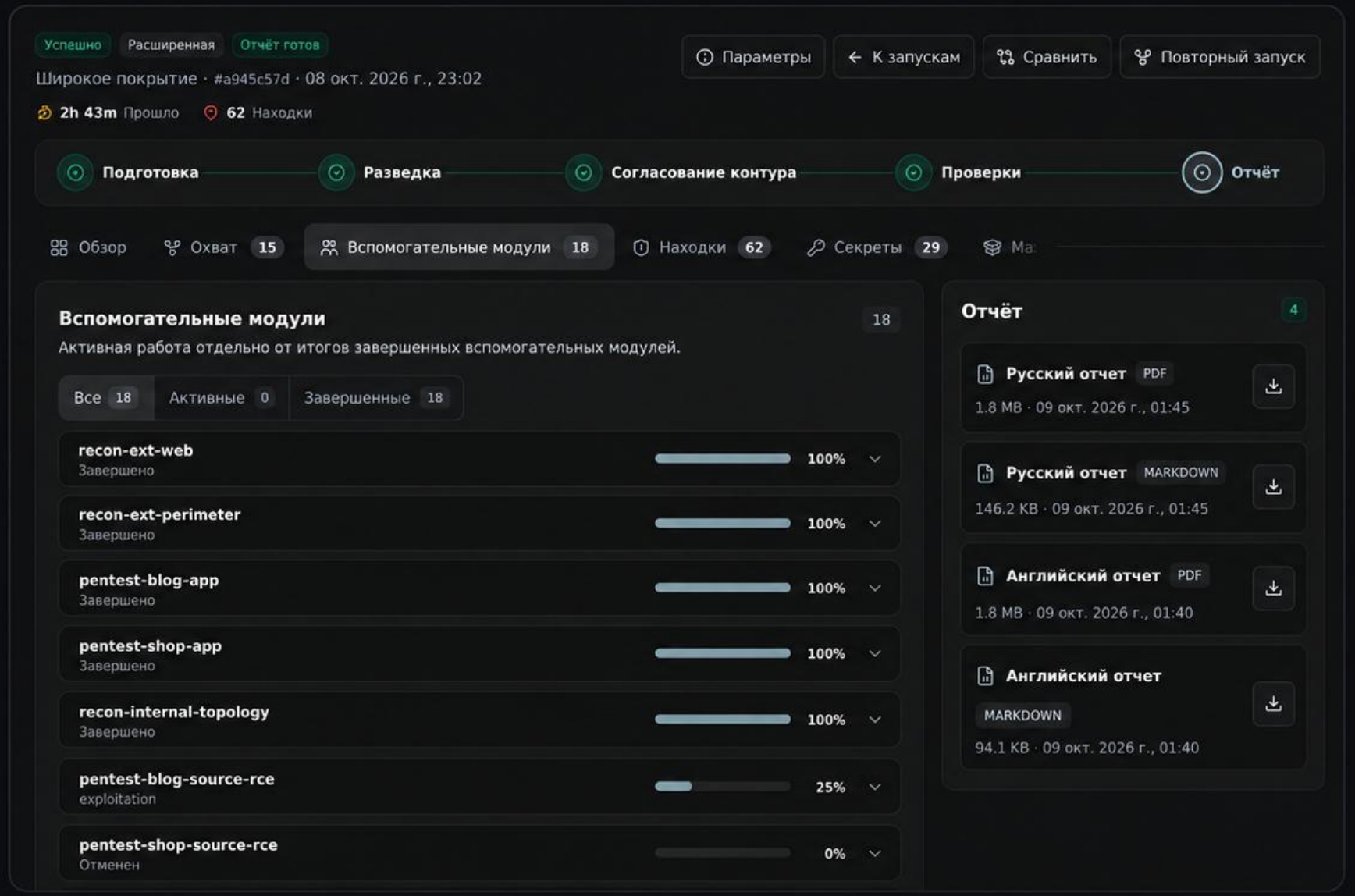
Назначенная работа

Кто и что проверяет
по каждому направлению.

Результат проверки

Статус решений
и найденные результаты.

Что сделали агенты



МОДУЛИ

Задачи и статусы

Какие модули запускались и в каком состоянии: активные, завершенные или отмененные.

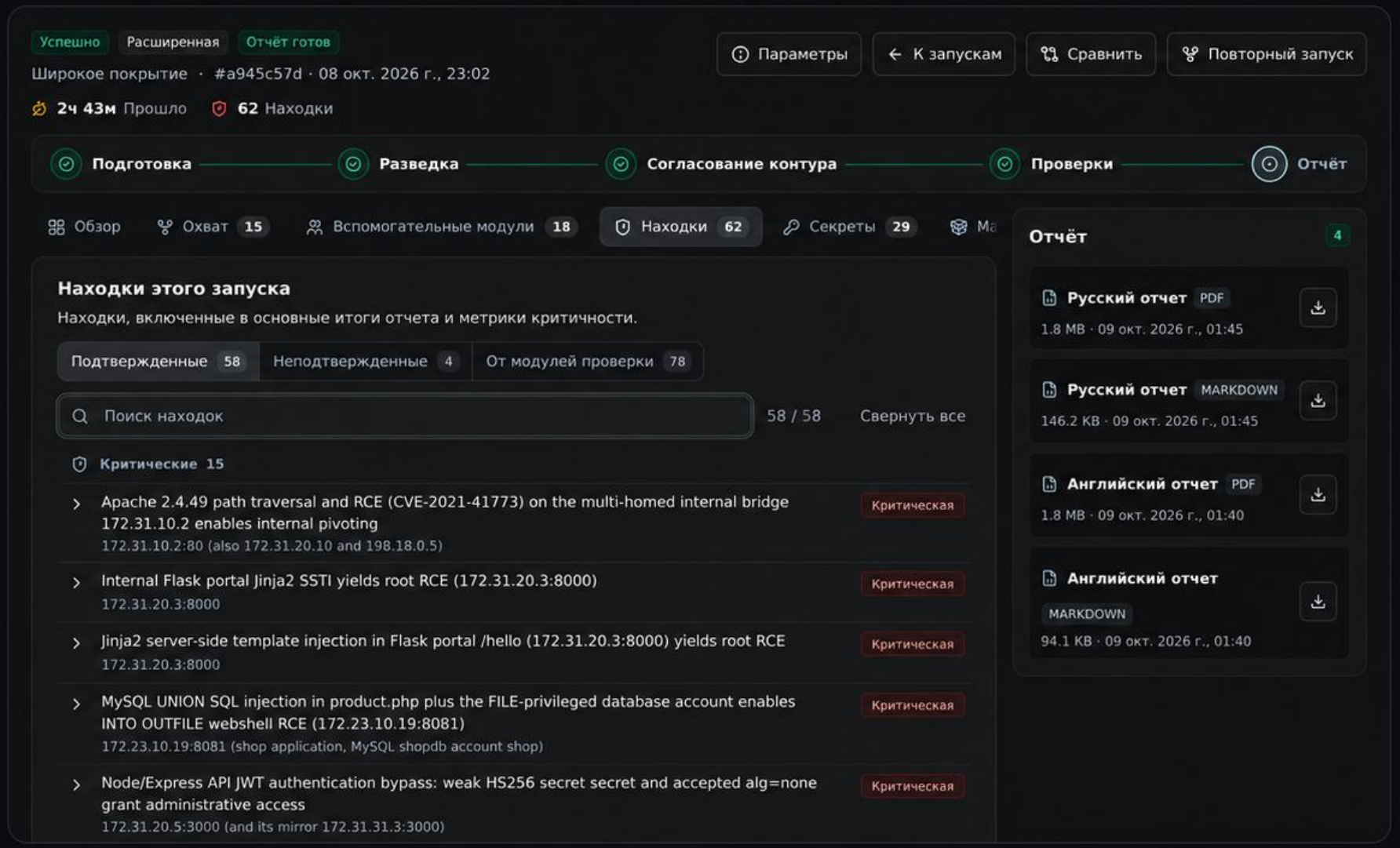
Ход работы

Как агенты выполняли запланированные этапы и с каким прогрессом.

Источники находок

Где зафиксированы результаты работы: отчеты и артефакты в разных форматах.

Все находки в одном пространстве



Находки

62

находки

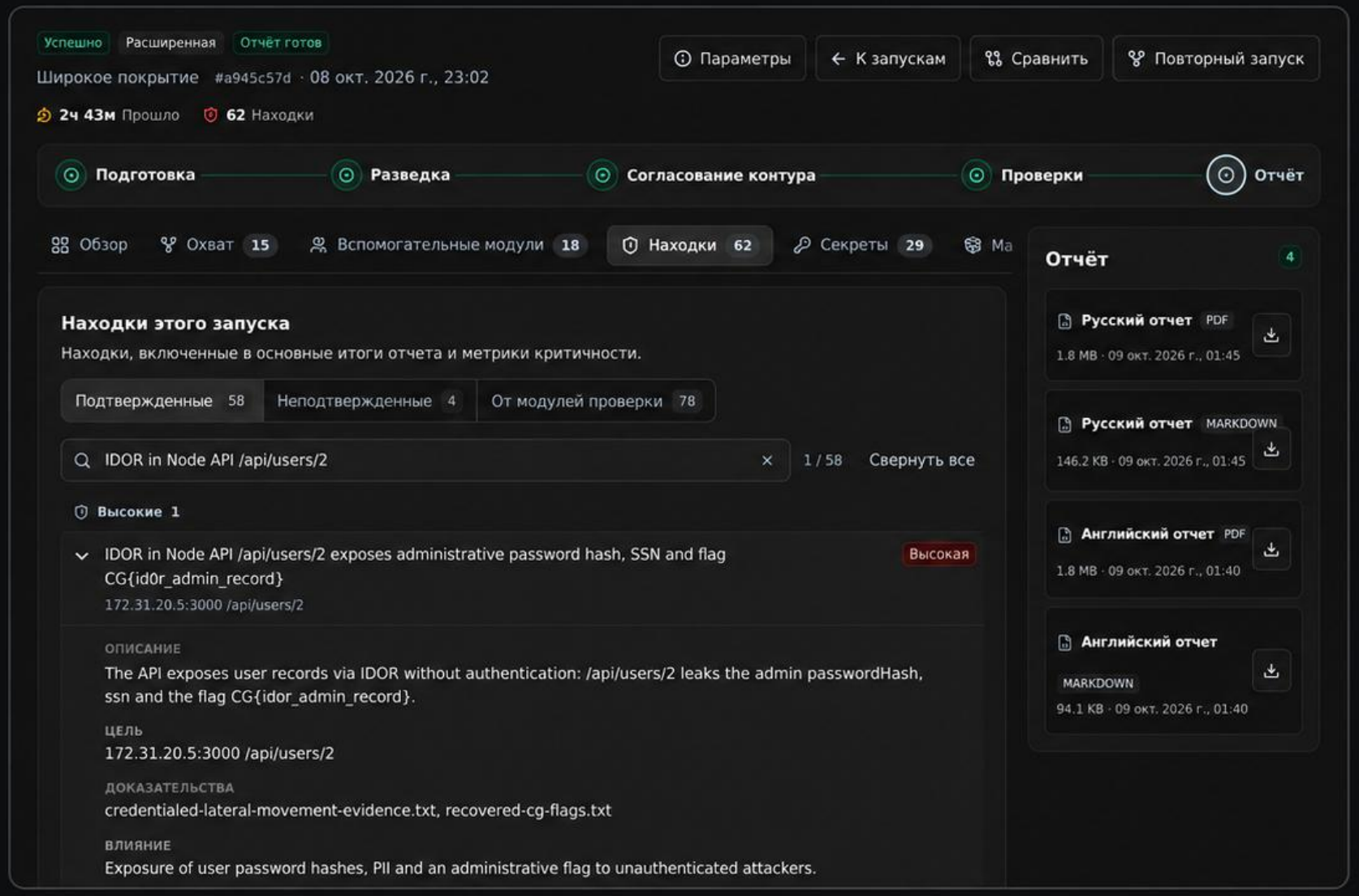
58

подтверждено

4

требуют проверки

IDOR: чужая запись без авторизации



GET /api/users/2

Запись администратора без аутентификации

Сохранены доказательства

IDOR: из карточки — в отчёт

Та же находка: /api/users/2

НАХОДКА F-38

ВЫСОКАЯ

ПОДТВЕРЖДЕНО

IDOR в Node API /api/users/2 раскрывает хеш административного пароля, SSN и флаг CG{idor_admin_record}

ЦЕЛЬ	АГЕНТЫ-ИСТОЧНИКИ
172.31.20.5:3000 /api/users/2	pentest-net1-ftp-pivot

Описание

API раскрывает записи пользователей через IDOR без аутентификации: /api/users/2 утекает административные passwordHash, ssn и флаг CG{idor_admin_record}.

Влияние

Раскрытие хешей паролей пользователей, PII и административного флага неаутентифицированным атакующим.

Воспроизведение

1. GET /api/users/2 -> запись администратора, включая passwordHash, ssn и CG{idor_admin_record}

Рекомендации

Добавьте проверки авторизации для /api/users/:id и никогда не возвращайте хеши паролей, SSN или флаги в ответах.

Влияние

Раскрытие хешей паролей пользователей, PII и административного флага неаутентифицированным атакующим.

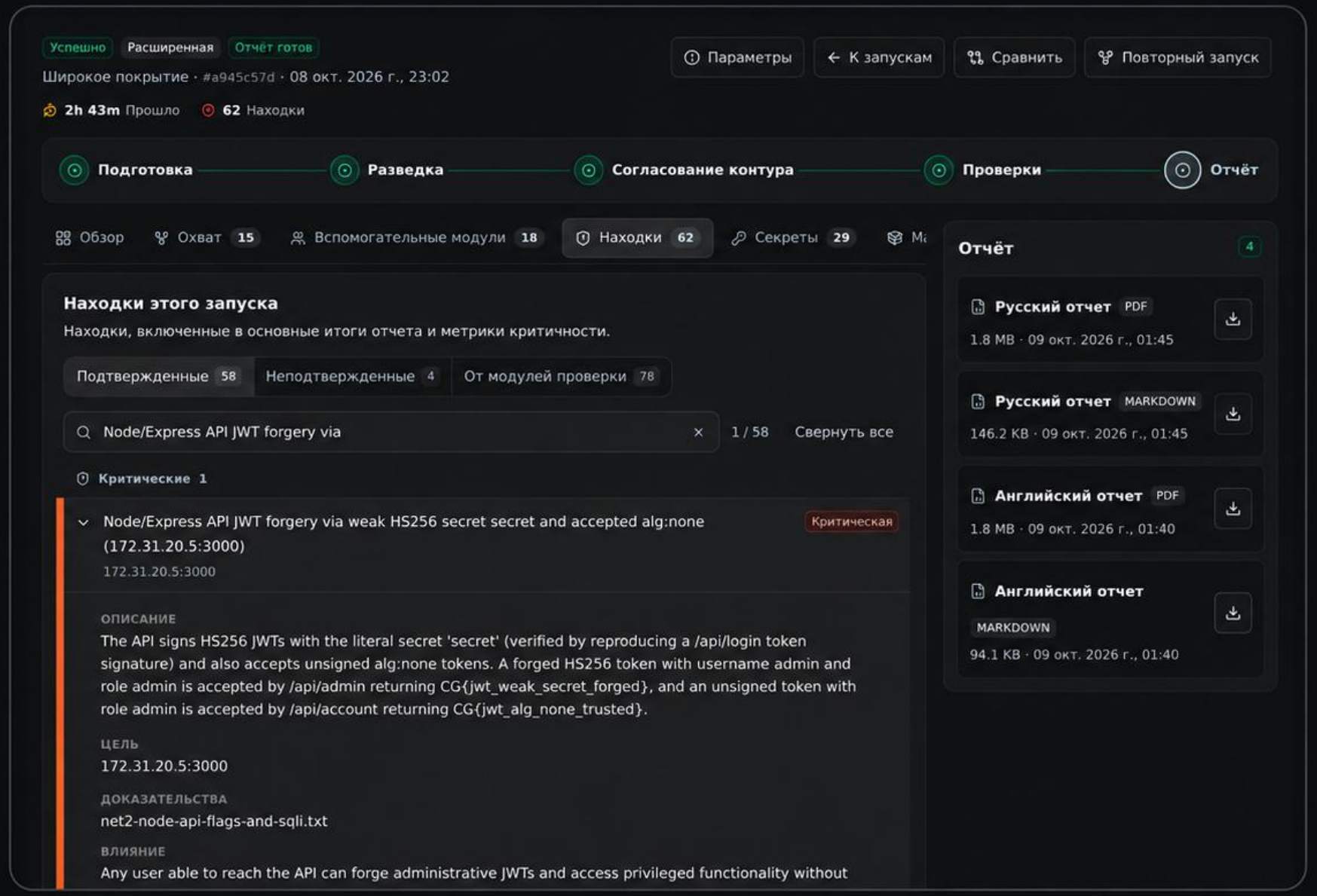
Воспроизведение

GET /api/users/2 -> запись администратора, включая passwordHash, ssn и CG{idor_admin_record}.

Рекомендация

Добавьте проверки авторизации для /api/users/:id и никогда не возвращайте хеши паролей, SSN или флаги в ответах.

JWT: доступ с поддельной ролью



01 —

Слабый ключ HS256

02 —

Принимается alg:none

03 —

Два контрольных флага

JWT: тот же обход в русском отчёте

Карточка JWT → находка F-10 в отчёте

НАХОДКА F-10

Подделка JWT API Node/Express через слабый секрет HS256 secret и принимаемый alg:none (172.31.20.5:3000)

КРИТИЧЕСКАЯ

ПОДТВЕРЖДЕНО

ЦЕЛЬ	АГЕНТЫ-ИСТОЧНИКИ
172.31.20.5:3000	pentest-net2-estate

Описание

API подписывает JWT алгоритмом HS256 с буквальным секретом 'secret' (проверено воспроизведением подписи токена /api/login) и также принимает неподписанные токены alg:none. Поддельный токен HS256 с username admin и role admin принимается /api/admin, возвращая CG{jwt_weak_secret_forged}, а неподписанный токен с role admin принимается /api/account, возвращая CG{jwt_alg_none_trusted}.

Влияние

Любой пользователь, способный достичь API, может подделывать административные JWT и получать доступ к привилегированному функционалу без учётных данных.

- Права администратора
- Слабый ключ HS256
- Принятие alg:none
- Подтверждённое влияние

От результата — к повторной проверке

Находка F-10: воспроизведение, исправление, доказательства

Воспроизведение

1. Подделайте JWT HS256 с payload username=admin, role=admin, подписанный ключом 'secret'
2. GET /api/admin с Authorization: Bearer -> {"ok":true,"flag":"CG{jwt_weak_secret_forged}"}
3. GET /api/account с неподписанным токеном header {"alg":"none"} payload {"role":"admin"} -> {"ok":true,"flag":"CG{jwt_alg_none_trusted}"}

Рекомендации

Используйте высокоэнтропийный секрет из окружения, фиксируйте принимаемый алгоритм, никогда не принимайте alg:none и определяйте роли на стороне сервера, а не из утверждений токена.

Доказательства

НАЗВАНИЕ	ТИП	ИСТОЧНИК	РАЗМЕР	SHA-256
net2-node-api-flags-and-sqli.txt	Evidence	pentest-net2-estate	1.8 KB	eb3896b91ac12b7f01585d5b75a880db806436cabf16dab7af131371d93b678f

1 **Запрос и ответ**

Показываем, как воспроизвести находку: последовательность запросов и полученные ответы с флагами.

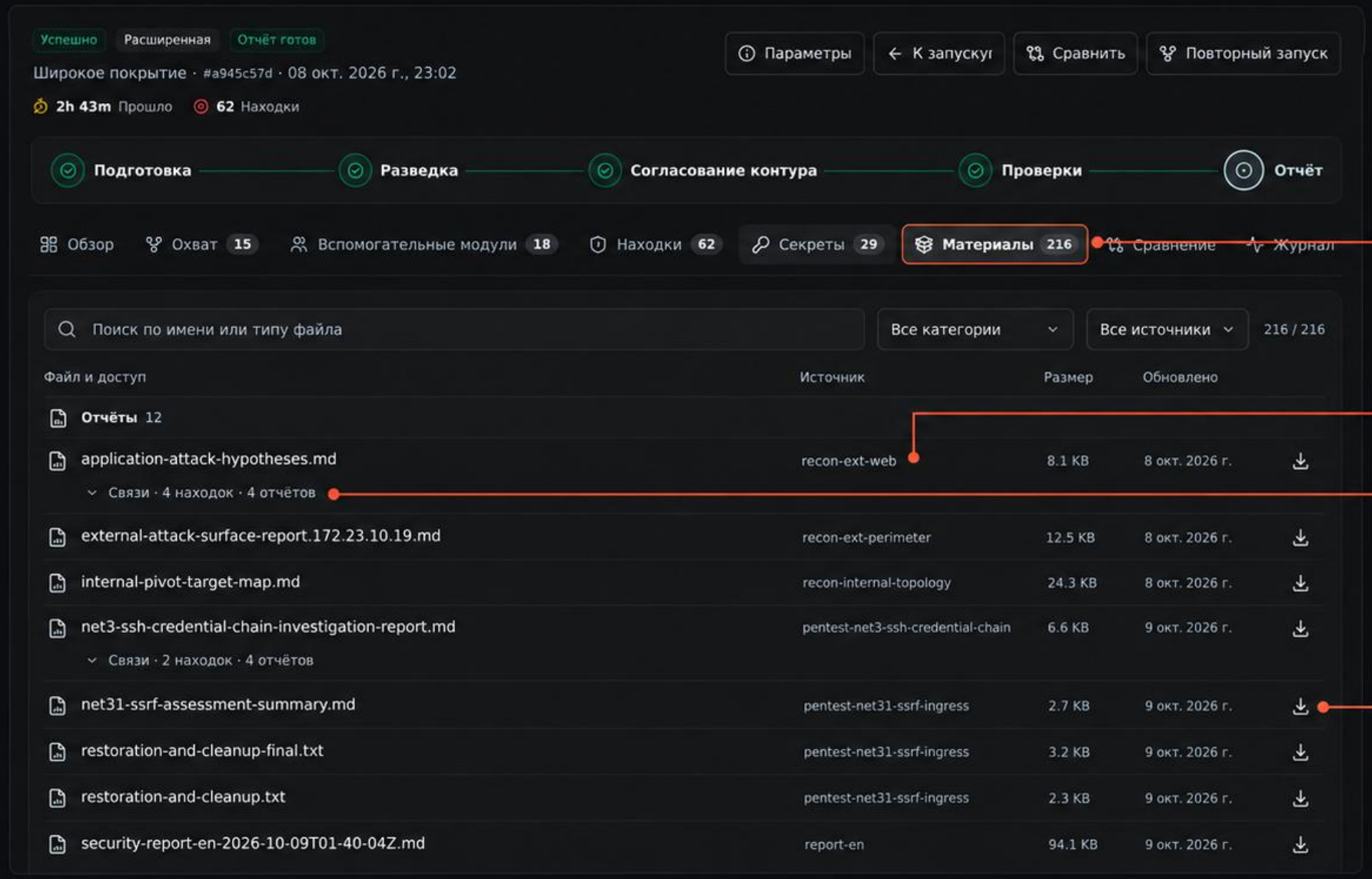
2 **Что исправить**

Краткие рекомендации по устранению: безопасный секрет, фиксация алгоритма, запрет alg:none, определение ролей на сервере.

3 **Где доказательство**

Файл с результатами и флагами: название, тип, источник, размер и SHA-256.

Артефакты связаны с результатами



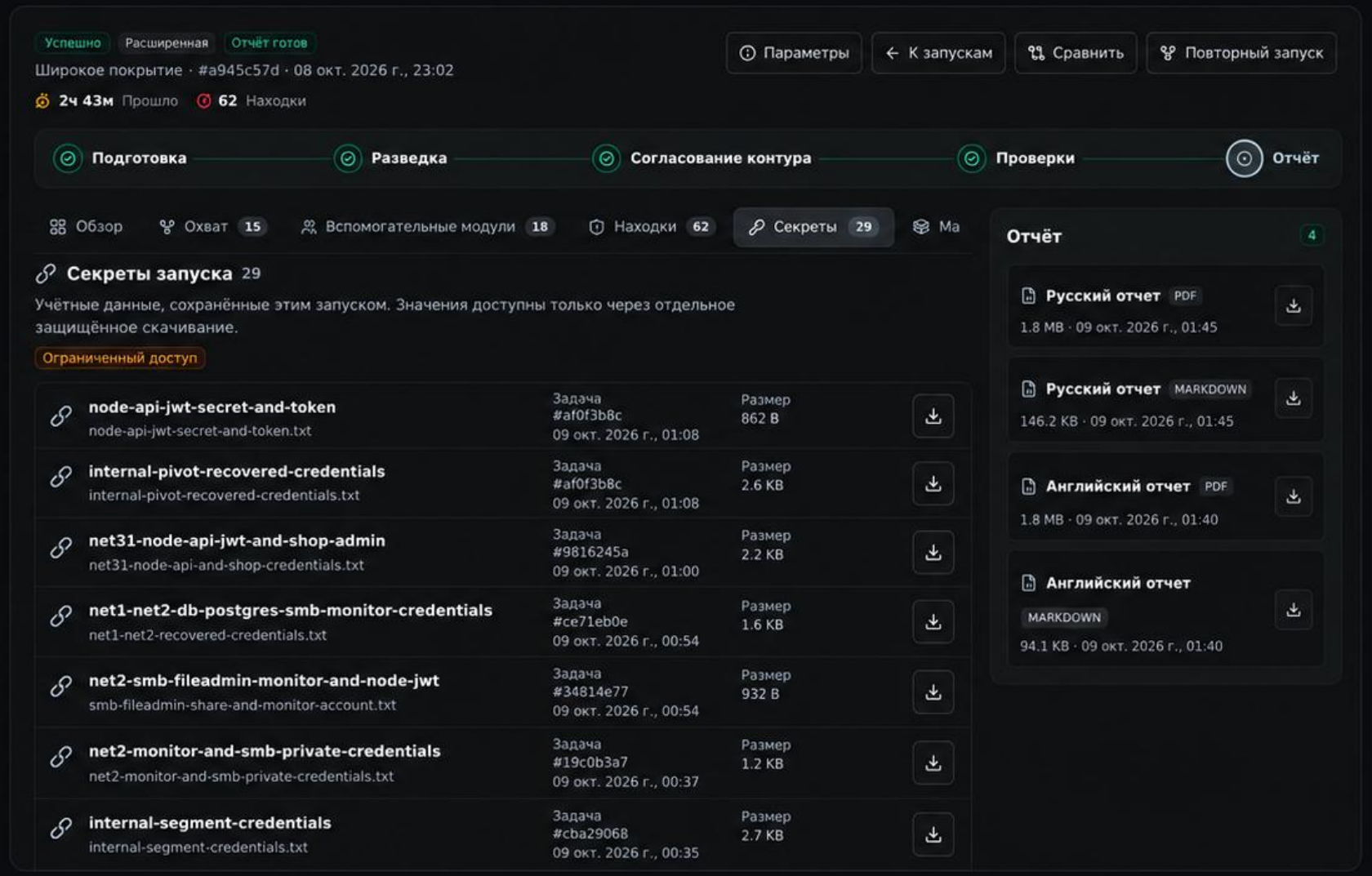
Категории материалов

Источник — агент

Связь с находкой

Просмотр и скачивание

Учётные данные
в отдельном каталоге

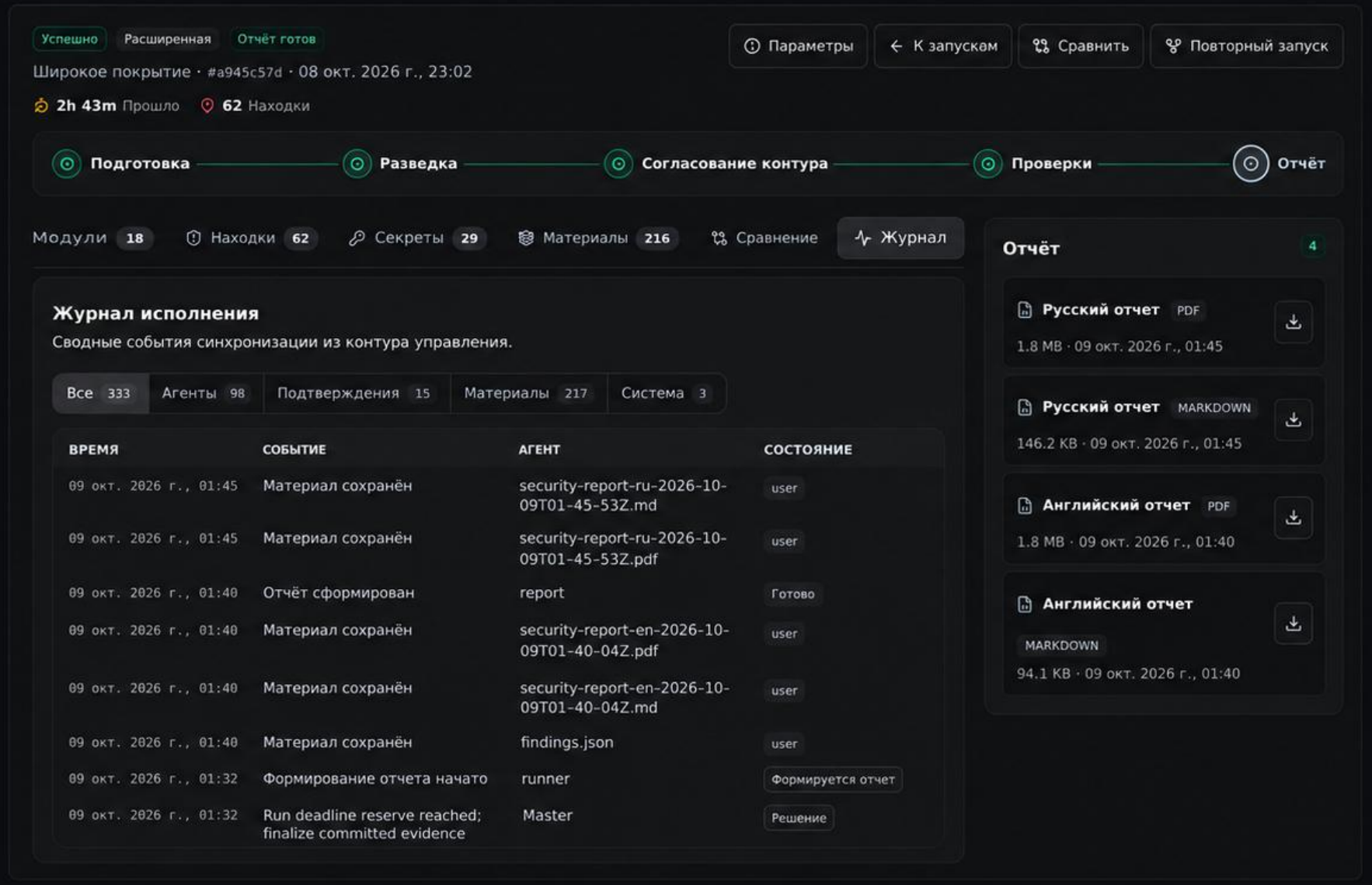


Найденные доступы

Источник и контекст

Связь с проверкой

История действий остаётся доступной



- **События запуска**
- **Последовательность действий**
- **Разбор результата**

Всё исследование — в итоговом отчёте

Находки + материалы + история → сводка результатов

Обзор результатов

В снимок включено находок: 62.
Подтверждено: 58; не подтверждено: 4.

НАИВЫСШАЯ КРИТИЧНОСТЬ

Критическая

62	58	4	211
НАХОДОК	ПОДТВЕРЖДЕНО	НЕ ПОДТВЕРЖДЕНО	МАТЕРИАЛОВ

Распределение по критичности



КРИТИЧЕСКАЯ 15 ВЫСОКАЯ 42 СРЕДНЯЯ 4 НИЗКАЯ 0 ИНФОРМАЦИОННАЯ 1

Итог проверки

62
находки

58
подтверждены

4
требуют проверки

211
материалов

Результаты нашего бенчмарка

Cunning Goose · сравнение запусков

Инструмент	Реализовано критических событий	Время	Использование токенов
Triadix	**22 / 30** 73,3%	**2 ч 40 мин**	**298,75 млн** Измерено: работники + оркестратор
PentAGI	**11 / 30** 36,7%	**11 часов**	**1,246 млрд токенов** (оценка)

В 2 раза больше событий · в 4,1 раза меньше времени

Сканер	Известные CVE
Ручной пентест	Индивидуальный подход, но дорого и редко
AI-пентест	Всегда доступен и готов к работе любому сценарию проверки

Покажем, на что способна наша система



triadix.ru

Пилотный запуск на вашем скоупе