

МИРАЖ

Система раннего обнаружения внутренних угроз

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Содержание

Содержание	2
1. Введение	4
1.1. О системе	4
1.2. Концепция Zero False Positives	4
1.3. Обнаруживаемые угрозы	4
1.4. Роли пользователей	4
2. Начало работы	5
2.1. Вход в систему	5
2.2. Восстановление пароля	5
2.3. Интерфейс системы	6
2.3.1. Навигация	7
2.3.2. Уведомления	7
2.3.3. Переключение темы	7
3. Мониторинг (Dashboard)	8
3.1. Карточки статистики	8
3.2. Timeline событий	8
3.3. Тепловая карта активности (Heatmap)	8
3.4. Распределение по Severity	8
3.5. «MITRE ATT&CK»	8
3.6. Тор источников	8
3.7. Последние критические события	8
4. Ловушки	9
4.1. Список ловушек	9
4.2. Создание ловушки	9
4.2.1. Параметры ловушки	11
4.2.2. Поддерживаемые сервисы	11
4.2.3. Детекторы	11
4.3. Управление ловушкой	11
4.4. Статусы ловушки	12
4.5. Просмотр событий ловушки	12
5. Приманки	13
5.1. Типы приманок	13
5.1.1. Файловые приманки	13
5.1.2. URL Canary-токены	13
5.2. Создание файловой приманки	14
5.3. Создание URL Canary	14
5.4. Скачивание и размещение	15
5.5. Отслеживание срабатываний	15
6. События	16

6.1. Фильтрация событий.....	16
6.2. Категории событий.....	16
6.3. Детали события.....	17
6.4. Подтверждение событий	17
6.5. Экспорт	17
7. Сети.....	18
7.1. Создание сети	18
7.2. Управление сетями.....	18
8. Настройки.....	19
8.1. Интеграции	19
8.1.1. Email (SMTP).....	19
8.1.2. Telegram	19
8.1.3. Webhook	19
8.1.4. SIEM (Syslog)	19
8.2. Диагностика	19
8.3. Active Directory.....	20
8.4. Белый список.....	21
8.5. Профиль	22
9. MITRE ATT&CK.....	24
Приложение А. Матрица прав доступа.....	25
Приложение Б. Горячие клавиши и подсказки	25

1. Введение

1.1. О системе

Мираж (*Mirage*) — платформа раннего обнаружения внутренних угроз, работающая по принципу предположения, что злоумышленник уже находится внутри сети, и создаёт условия для его обнаружения.

Система развёртывает в корпоративной сети два типа активов:

- **Ловушки** — поддельные серверы (SSH, HTTP, SMB, RDP, FTP, MySQL, PostgreSQL, MSSQL, WinRM), фиксирующие любое обращение к ним.
- **Приманки** — поддельные артефакты (файлы с паролями, сапай-токены), ведущие атакующего к ловушкам.

1.2. Концепция Zero False Positives

В корпоративной сети легитимные пользователи знают, куда им нужно ходить: бухгалтер — в 1С, разработчик — в Git, менеджер — в CRM. Никто из них не будет сканировать подсети, пробовать случайные учётные данные или открывать файлы с паролями на чужих компьютерах.

Любое взаимодействие с системой Мираж — это либо атакующий, либо скомпрометированный хост, либо инсайдер. В любом случае — инцидент, требующий реакции. Ноль ложных срабатываний.

1.3. Обнаруживаемые угрозы

Угроза	Как обнаруживается
Инсайдер	Сотрудник сканирует сеть или использует найденные приманки
Скомпрометированный хост	Вредоносное ПО выполняет lateral movement, сканирует подсети
APT внутри периметра	Атакующий исследует сеть после проникновения
Red Team / Pentest	Пентестеры попадают на ловушки (валидация защиты)
Responder/LLMNR Poisoning	Детектор обнаруживает poisoning атаки в сети

1.4. Роли пользователей

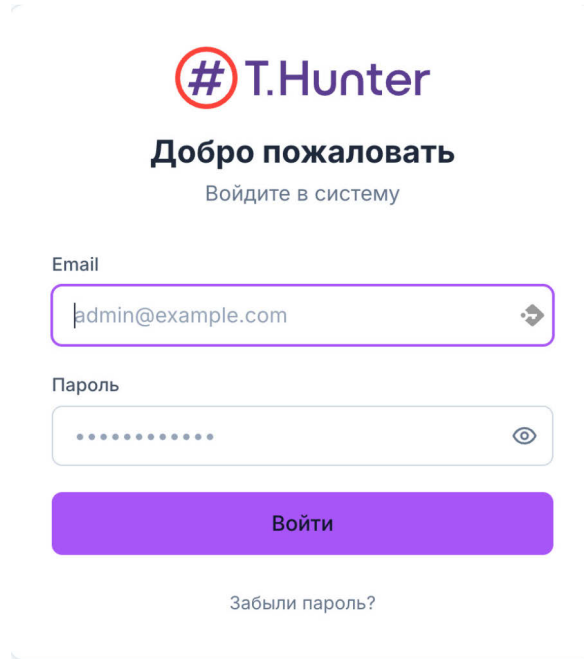
В системе предусмотрены три роли с различными уровнями доступа:

Роль	Описание	Ключевые права
Аналитик	Только просмотр	Просмотр дашбордов, ловушек, приманок, событий, сетей
Оператор	Управление инфраструктурой	Создание/управление ловушками, приманками, сетями, интеграциями
Администратор	Полный контроль	Все операции + управление пользователями, аудит, настройки, лицензия

2. Начало работы

2.1. Вход в систему

Откройте веб-браузер и перейдите по адресу системы (например, <https://mirage.local>). Вы увидите страницу входа.



СКРИНШОТ: Страница входа — форма с полями Email и Пароль

1. Введите ваш email-адрес.
2. Введите пароль.
3. Если у вас включена двухфакторная аутентификация (2FA), введите код из приложения-аутентификатора.
4. Нажмите "Войти".

⚠ После 5 неудачных попыток входа учётная запись блокируется на 15 минут. Если ваш аккаунт заблокирован, обратитесь к администратору.

2.2. Восстановление пароля

На странице входа нажмите ссылку "Забыли пароль?". Система предлагает два способа восстановления:

- **По email** — на указанный email будет отправлена ссылка для сброса пароля (требуется настроенная интеграция Email).
- **По коду восстановления** — используйте один из одноразовых кодов, полученных при первоначальной настройке системы.



Восстановление доступа

Выберите способ восстановления пароля

Восстановление по Email

Получите ссылку для сброса пароля на почту

Код восстановления

Используйте одноразовый код, полученный при настройке

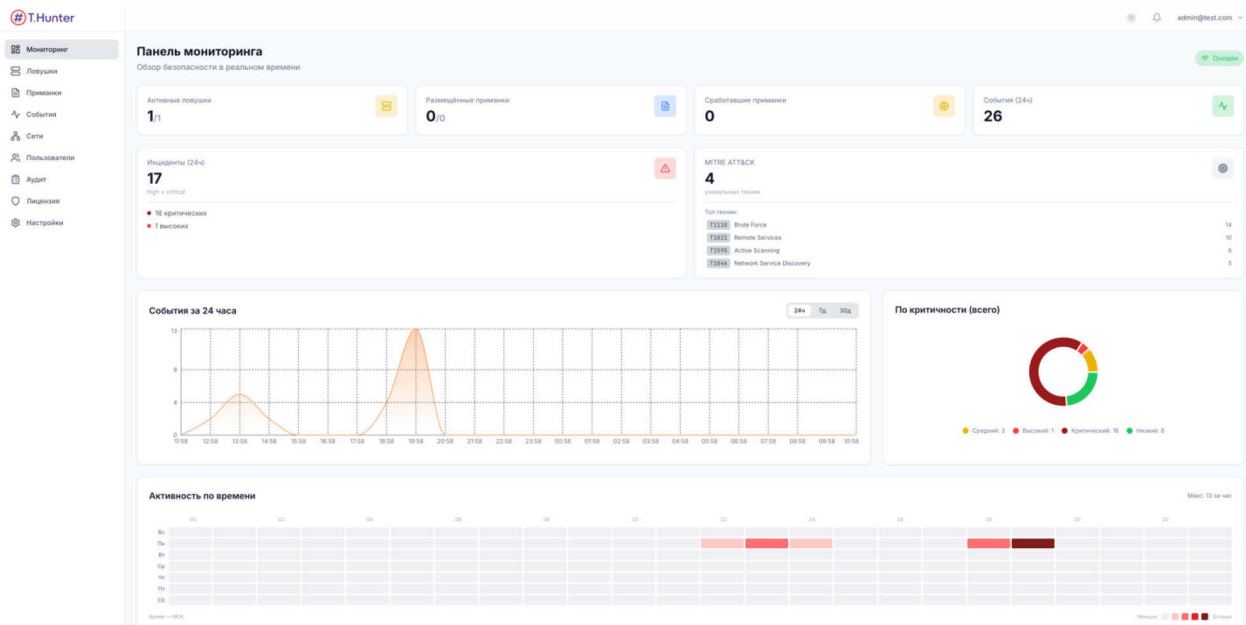
[← Вернуться к входу](#)

СКРИНШОТ: Страница восстановления пароля — переключатель между восстановлением по email и по коду

2.3. Интерфейс системы

После входа вы попадаете в главный интерфейс. Он состоит из:

- **Боковая панель (слева)** — навигация между разделами системы. Набор доступных пунктов зависит от вашей роли.
- **Верхняя панель** — переключатель темы (светлая/тёмная/системная), колокольчик уведомлений, меню пользователя.
- **Рабочая область** — содержимое текущего раздела.



СКРИНШОТ: Главный интерфейс — боковая панель навигации

2.3.1. Навигация

Пункты меню боковой панели:

Раздел	Описание
Мониторинг	Сводная панель со статистикой и графиками событий
Ловушки	Управление honeypot-серверами
Приманки	Управление файловыми приманками и сапату-токенами
События	Журнал всех обнаруженных событий безопасности
Сети	Управление сетевыми профилями для размещения ловушек
Пользователи	Управление учётными записями (только для администраторов)
Аудит	Журнал действий пользователей (только для администраторов)
Лицензия	Управление лицензией (только для администраторов)
Настройки	Интеграции, диагностика, AD, белый список, профиль

2.3.2. Уведомления

Иконка колокольчика в верхней панели показывает количество непрочитанных уведомлений. При нажатии открывается панель с последними событиями высокого и критического уровней. Уведомления поступают в реальном времени через WebSocket-соединение.

2.3.3. Переключение темы

Мираж поддерживает три темы оформления: Светлая, Тёмная и Системная (автоматически подстраивается под настройки ОС). Переключатель доступен в верхней панели.

3. Мониторинг (Dashboard)

Раздел Мониторинг — главная страница системы, предоставляющая обзор текущего состояния безопасности.

3.1. Карточки статистики

В верхней части дашборда расположены 4 карточки:

- **Ловушки** — общее количество, сколько работает/остановлено/с ошибками.
- **Приманки** — общее количество, сколько развёрнуто, сколько сработало.
- **События за 24ч** — общее число событий за последние сутки
- **Инциденты за 24ч** — общее число инцидентов за последние сутки, количество критических и высоких событий.

3.2. Timeline событий

Интерактивный график (Area Chart), показывающий количество событий во времени. Позволяет быстро оценить динамику активности и выявить аномальные всплески.

3.3. Тепловая карта активности (Heatmap)

Матрица «дни недели × часы суток», визуализирующая распределение событий. Каждая ячейка окрашена в зависимости от интенсивности: от бледного (мало событий) до насыщенного (много событий). При наведении курсора отображается точное количество событий.

3.4. Распределение по Severity

Круговая диаграмма (Pie Chart) показывает соотношение событий по уровням критичности: Низкий (зелёный), Средний (жёлтый), Высокий (красный), Критический (бордовый).

3.5. «MITRE ATT&CK»

Количество уникальных обнаруженных техник. Список «Топ техник» с ID техники (например, T1110.001), названием и счётчиком. Клик по технике открывает страницу MITRE ATT&CK

3.6. Топ источников

Таблица IP-адресов с наибольшим количеством зарегистрированных событий. Для каждого IP отображается:

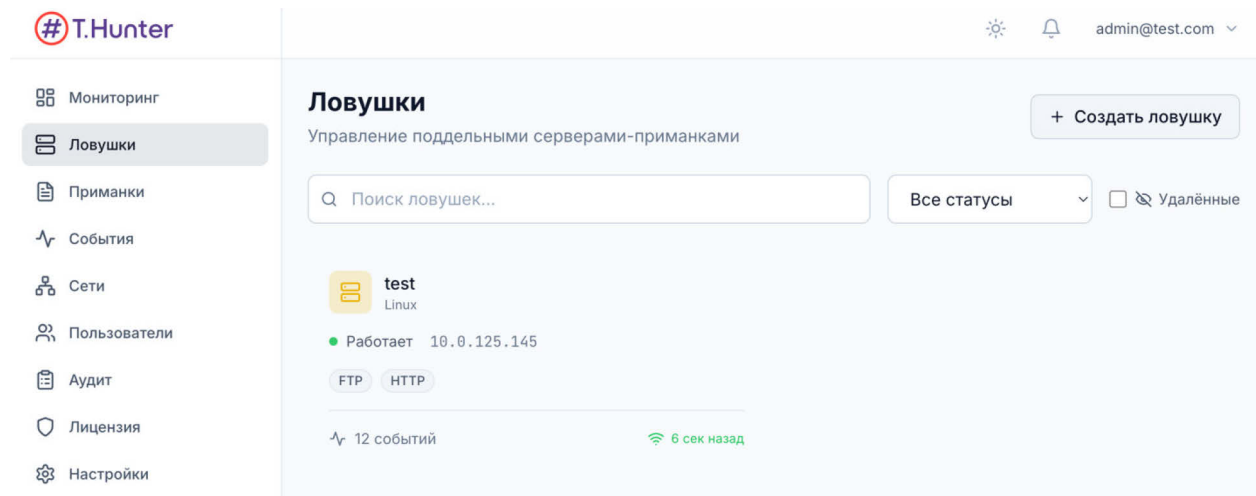
- IP-адрес источника
- Hostname (при наличии reverse DNS)
- Количество событий
- Время последнего события
- Статус белого списка (если добавлен)

3.7. Последние критические события

Список недавних событий с критическим и высоким уровнем severity. Каждое событие содержит временную метку, тип действия, IP-источник, имя актива и маппинг MITRE ATT&CK (при наличии).

4. Ловушки

Ловушки — поддельные серверы, развёрнутые в сети в виде контейнеров. Их задача — зафиксировать факт обращения. Если кто-то пытается подключиться к SSH на сервере, о котором не знает — это инцидент.



СКРИНШОТ: Страница Ловушки

4.1. Список ловушек

Страница отображает таблицу всех ловушек с полями:

- **Имя** — уникальное имя ловушки (например, SRV-BACKUP-01)
- **Статус** — текущее состояние: Ожидание, Развёртывание, Работает, Остановлена, Неисправна, Ошибка
- **ОС** — тип эмулируемой ОС: Linux или Windows
- **Сервисы** — список активных сервисов (SSH, HTTP, SMB и т.д.)
- **IP-адрес** — выделенный IP в корпоративной сети
- **Событий** — количество зарегистрированных событий
- **Heartbeat** — время последнего сигнала от ловушки

Доступна фильтрация по статусу, поиск по имени, а также переключатель отображения удалённых ловушек.

4.2. Создание ловушки

Для создания ловушки (требуется роль Оператор или Администратор):

1. Нажмите кнопку "+ Создать ловушку".
2. В открывшемся модальном окне заполните параметры.

Создание ловушки
✕

Название *

Только буквы (a-z), цифры и дефисы. Должно начинаться с буквы.

Описание

Операционная система

Linux Windows

Сервисы *

Показаны сервисы, доступные для Linux

SSH (22)

HTTP (80)

FTP (21)

MySQL (3306)

PostgreSQL (5432)

Детекторы угроз опционально

Активные механизмы обнаружения сетевых атак

Responder Detector

Обнаружение LLMNR/NBT-NS/mDNS poisoning атак (Responder, Inveigh)

Сеть

Выберите сеть...
▾

Отмена

Создать

СКРИНШОТ: Модальное окно создания ловушки

Создание ловушки
✕

Название *

Только буквы (a-z), цифры и дефисы. Должно начинаться с буквы.

Описание

Операционная система

Linux Windows

Сервисы *

Показаны сервисы, доступные для Windows

FTP (21)

SMB (445)

RDP (3389)

MSSQL (1433)

WinRM (5985)

Идентификация Windows

Имена, видимые атакующим при сканировании (SMB, RDP, WinRM)

Hostname (NetBIOS)	Домен
<input type="text" value="FILESERVER"/>	<input type="text" value="corp.local или CORP"/>
<small>A-Z, 0-9, дефис (макс. 15)</small>	<small>NetBIOS (CORP) или DNS (corp.local)</small>

Примеры

SMB: WIN-SERVER01 \ corp

WinRM: WIN-SERVER01 \ corp.local

Детекторы угроз опционально

Активные механизмы обнаружения сетевых атак

Responder Detector

Обнаружение LLMNR/NBT-NS/mDNS poisoning атак (Responder, Inveigh)

Сеть

Выберите сеть...
▾

Отмена

Создать

СКРИНШОТ: Модальное окно создания ловушки

4.2.1. Параметры ловушки

Параметр	Обязательный	Описание
Имя	Да	Уникальное имя (латиница, цифры, дефис). Примеры: SRV-BACKUP, SQL-TEST
Описание	Нет	Текстовое описание назначения ловушки
Тип ОС	Да	Linux или Windows — определяет набор доступных сервисов
Сервисы	Да	Один или несколько сервисов для эмуляции
Детекторы	Нет	Дополнительные детекторы угроз (например, Responder Detector)
Сеть	Да	Сетевой профиль (bridge), определяющий VLAN размещения
Hostname (Windows)	Нет*	NetBIOS-имя хоста для SMB/RDP/WinRM сервисов
Домен (Windows)	Нет*	Домен (CORP или corp.local) для Windows-идентификации
HTTP-пресет	Нет	Шаблон веб-страницы: Basic Auth, Zabbix 7.0, Grafana 11

 * *Hostname и Домен рекомендуются для Windows-ловушек с сервисами SMB, RDP, WinRM для реалистичной эмуляции.*

4.2.2. Поддерживаемые сервисы

Сервис	Порт	ОС	Описание
SSH	22	Linux	Логирование попыток входа: username, password, client banner
HTTP	80	Linux	Веб-сервер с пресетами (Basic Auth, Zabbix, Grafana)
FTP	21	Linux, Windows	Логирование попыток входа по FTP, действия с папками и файлами
MySQL	3306	Linux	Эмуляция MySQL-сервера, перехват учётных данных
PostgreSQL	5432	Linux	Эмуляция PostgreSQL-сервера
SMB	445	Windows	Эмуляция файлового сервера, захват NTLMv2-хэшей
RDP	3389	Windows	Эмуляция Remote Desktop, логирование подключений
MSSQL	1433	Windows	Эмуляция Microsoft SQL Server
WinRM	5985	Windows	Эмуляция Windows Remote Management

4.2.3. Детекторы

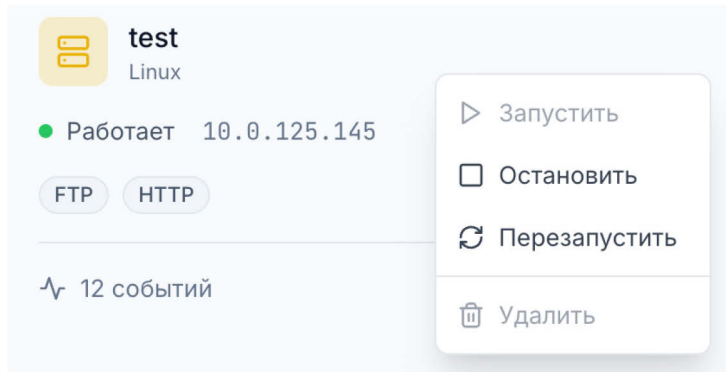
Responder Detector — обнаруживает LLMNR/NBT-NS/mDNS poisoning атаки (инструменты Responder, Inveigh). Доступен для ловушек обоих типов ОС.

4.3. Управление ловушкой

Для каждой ловушки доступны действия через контекстное меню (...):

- **Запустить** — запускает остановленную ловушку
- **Остановить** — останавливает работающую ловушку (контейнер сохраняется)

- **Перезапустить** — перезапускает ловушку
- **Удалить** — мягкое удаление (события сохраняются, контейнер удаляется)



СКРИНШОТ: Контекстное меню ловушки с действиями: Запустить, Остановить, Перезапустить, Удалить

4.4. Статусы ловушки

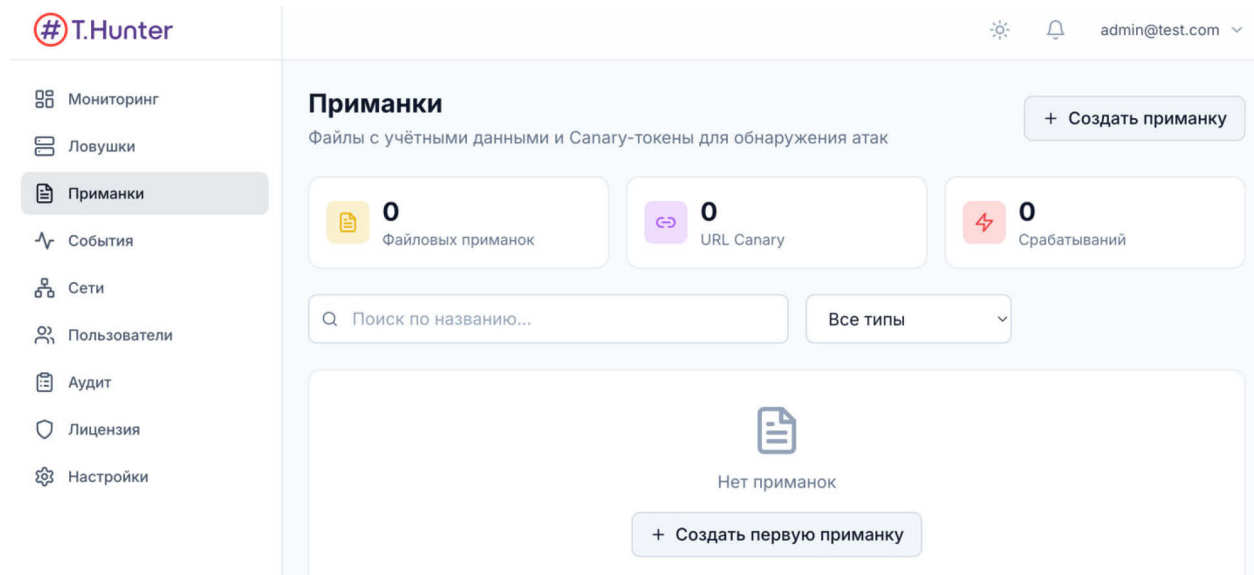
Статус	Индикатор	Описание
Ожидание	Серый	Создана, ожидает развёртывания в LXD
Развёртывание	Жёлтый (мигает)	Идёт создание контейнера и запуск сервисов
Работает	Зелёный (пульсирует)	Активна, собирает события, отправляет heartbeat
Остановлена	Серый	Остановлена администратором, контейнер существует
Неисправна	Жёлтый	Нет heartbeat более 3 минут
Ошибка	Красный	Ошибка развёртывания или работы

4.5. Просмотр событий ловушки

В детальной карточке ловушки отображается количество событий. Нажатие переводит в раздел События с предустановленным фильтром по данной ловушке.

5. Приманки

Приманки — поддельные артефакты, ведущие атакующего к ловушкам. Атакующий ищет ценное: пароли, конфиги, документы. Мираж подкидывает ему «ценности», использование которых создаёт событие безопасности.



СКРИНШОТ: Страница Приманки

5.1. Типы приманок

5.1.1. Файловые приманки

Файлы с «интересным» содержимым — поддельными учётными данными от ловушек. Поддерживаемые форматы:

Формат	Расширение	Описание
Текстовый	.txt	Файл с паролями (passwords.txt, credentials.txt)
Environment	.env	Файл переменных окружения с адресами и паролями
Config	.config	Конфигурационный файл INI-формата
JSON	.json	Конфигурация в формате JSON

При создании файловой приманки доступны стили генерации учётных данных:

- **Корпоративный** — пароли вида Admin2024!, Backup@Corp
- **Разработчик** — пароли вида password123, dev_pass
- **Устаревший** — простые пароли вида admin24
- **Безопасный** — сложные, длинные пароли

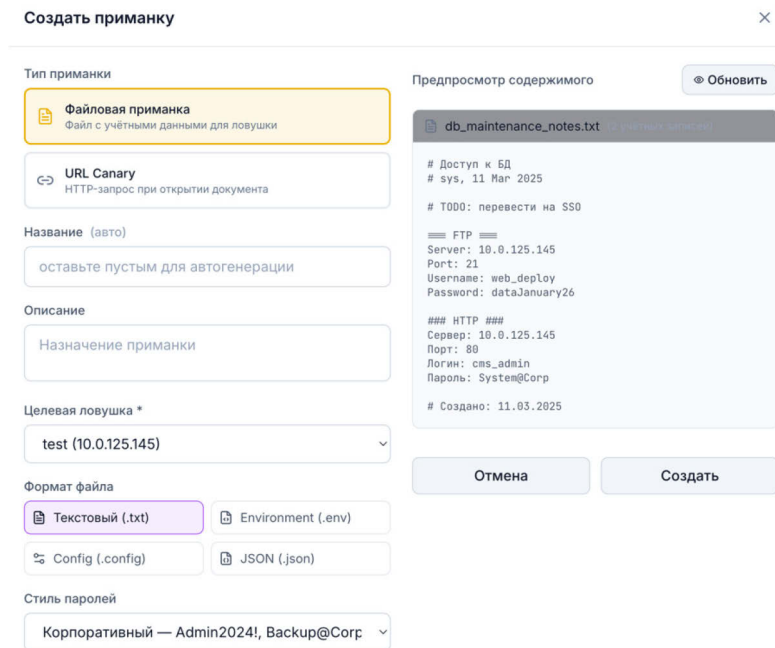
5.1.2. URL Canary-токены

Уникальные URL, генерирующие событие безопасности при обращении. Токен можно встроить в документы, конфигурации, закладки браузера. Доступны форматы встраивания:

- HTML-ссылка, HTML-изображение (трекинг-пиксель)
- Bash/Python/PowerShell-скрипт
- Markdown, JSON/YAML конфигурация
- Word-документ (невидимый пиксель), Excel-макрос, PDF-ссылка

5.2. Создание файловой приманки

1. Перейдите на вкладку "Файлы" и нажмите "+ Создать".
2. Выберите целевую ловушку — ту, на которую будут указывать поддельные учётные данные.
3. Выберите формат файла (txt, env, config, json).
4. Выберите стиль генерации паролей.
5. При необходимости отредактируйте имя файла и предварительно просмотрите содержимое.
6. Нажмите "Создать".

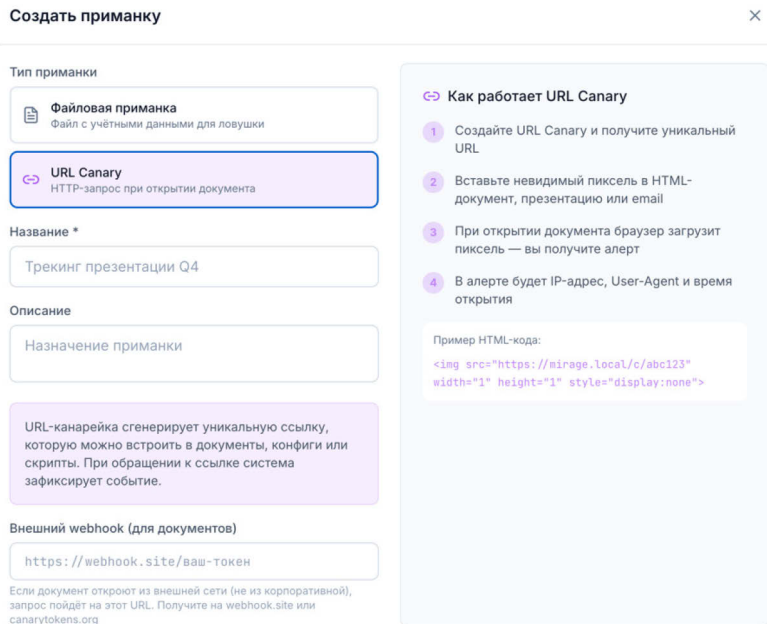


СКРИНШОТ: Модальное окно создания файловой приманки — выбор ловушки, формата файла, стиля, предпросмотр содержимого

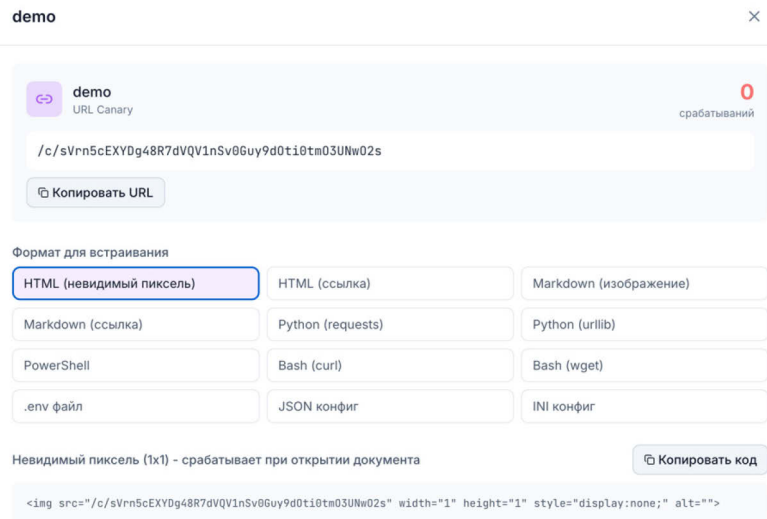
5.3. Создание URL Canary

1. Перейдите на вкладку "URL Canary" и нажмите "+ Создать".
2. Укажите имя и описание.
3. Опционально задайте пользовательский путь URL.
4. Нажмите "Создать".

После создания система сгенерирует уникальный URL и предоставит варианты встраивания в различные форматы.



СКРИНШОТ: Детали URL Canary



СКРИНШОТ: Детали URL Canary

5.4. Скачивание и размещение

Файловые приманки можно скачать и разместить вручную в целевых директориях. Для автоматического размещения (при наличии интеграции с AD) доступна функция Deploy:

- Укажите путь размещения (UNC-путь, например \\filesrver\IT\Documentation)
- Укажите учётные данные для доступа к целевому хосту или используйте AD-интеграцию

5.5. Отслеживание срабатываний

Для каждой приманки отображается:

- Количество срабатываний
- Время первого и последнего срабатывания
- Детали каждого срабатывания (IP-источник, User-Agent, время)

6. События

Раздел События — центральный журнал всех обнаруженных инцидентов. Каждое событие — это зафиксированное взаимодействие с ловушкой или приманкой.

События
Всего 26 событий

Экспорт

Поиск: [] [] Последние 24 ч [] Все уровни [] Все категории [] Инциденты []

Время	Уровень	Категория	Действие	MITRE	Источник	Цель
02 фев. 19:46:18	Высокий	Аутентификация	Попытка входа	T1118 T1118.001	10.0.115.212	test:80
02 фев. 19:46:14	Низкий	Сканирование	Сканирование портов	T1595 T1595.001 +1	10.0.115.212	test:80
02 фев. 19:46:09	Низкий	Сканирование	http_request	T1595	10.0.115.212	test:80
02 фев. 19:43:28	Критич.	Доступ	file_download	—	10.0.115.212	test:21
02 фев. 19:43:22	Средний	Доступ	file_list	—	10.0.115.212	test:21
02 фев. 19:43:21	Критич.	Аутентификация	Успешный вход	T1110 T1110.001	10.0.115.212	test:21
02 фев. 19:38:47	Критич.	Доступ	file_download	—	10.0.115.212	test:21
02 фев. 19:38:40	Средний	Доступ	file_list	—	10.0.115.212	test:21
02 фев. 19:38:39	Критич.	Аутентификация	Успешный вход	T1110 T1110.001	10.0.115.212	test:21

СКРИНШОТ: Страница Событий

6.1. Фильтрация событий

Доступные фильтры:

- **Временной диапазон** — последний час, 6 часов, 24 часа, 7 дней, 30 дней, всё время, пользовательский период
- **Severity** — Низкий, Средний, Высокий, Критический
- **Категория** — Сканирование, Аутентификация, Эксплойт, Доступ, Приманка, Безопасность
- **Поиск** — полнотекстовый поиск по IP, имени актива, действию

6.2. Категории событий

Категория	Severity	Примеры действий	Описание
scan	Низкий	port_scan, service_probe	Сканирование и разведка
auth	Средний	login_attempt, login_failed	Попытки аутентификации
auth	Критический	login_success	Успешный вход (учётные данные сработали)
exploit	Высокий	sql_injection, xss_attempt	Попытки эксплуатации уязвимостей
access	Высокий	file_access, command_exec	Доступ к ресурсам ловушки

canary	Критический	breadcrumb_triggered	Сработал canary-токен или файловая приманка
security	Варьируется	brute_force_detected, rate_limit_exceeded	Атаки на саму систему Мираж

6.3. Детали события

При нажатии на событие открывается модальное окно с полной информацией:

- **Основные данные** — время, категория, действие, severity, IP-источник/назначение, порт, протокол
- **Данные актива** — имя ловушки/приманки, тип
- **MITRE ATT&CK** — автоматический маппинг на тактики и техники MITRE ATT&CK Framework (со ссылками)
- **Raw Data** — специфичные данные: username, password hash, client banner, user-agent и т.д.

Детали события
×

Время
02.02.2026 19:43:21

Категория
Аутентификация

Источник
10.0.115.212:64498

Уровень
Критич.

Действие
login_success

Назначение
10.0.125.145:21

MITRE ATT&CK

T1110 Перебор паролей
Brute Force - Credential Access

Подтехники

T1110.001 Угадывание паролей

Логин: anonymous Пароль: anonymous

Результат: Успешно

Сырые данные

```
{
  "service": "ftp",
  "success": true,
  "password": "anonymous",
  "username": "anonymous"
}
```

СКРИНШОТ: Модальное окно деталей события — все поля, секция MITRE ATT&CK с тактиками и техниками, секция Raw Data

6.4. Подтверждение событий

События можно подтвердить (acknowledge), чтобы отметить, что они были рассмотрены аналитиком. На дашборде отображается счётчик неподтверждённых критических и высоких событий.

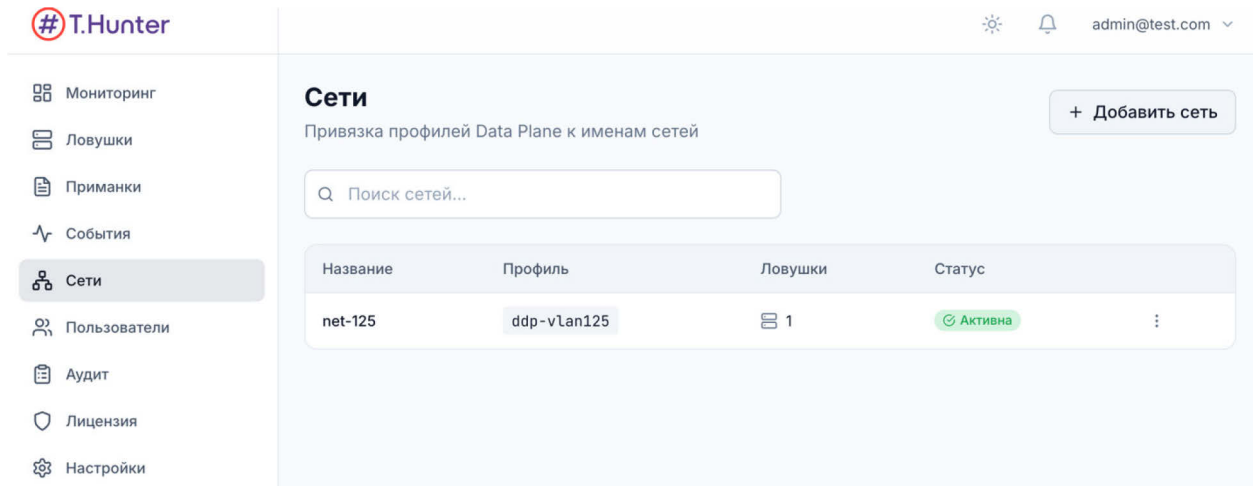
6.5. Экспорт

Доступен экспорт событий в форматах:

- **CSV** — таблица для загрузки в Excel или SIEM
- **JSON** — структурированные данные для автоматизации
- **PDF** — отчёт для руководства и аудиторов

7. Сети

Раздел Сети управляет сетевыми профилями, определяющими, в каких VLAN и подсетях размещаются ловушки.



СКРИНШОТ: Страница Сети — список сетевых профилей с указанием профиля, статуса и количества ловушек в каждой сети

7.1. Создание сети

1. Нажмите "+ Создать сеть".
2. Введите имя (например, Corporate VLAN 100) и описание.
3. Выберите профиль из списка доступных на Data Plane.
4. Нажмите "Создать".

⚠ Профили предварительно настраиваются администратором на VM2 (Data Plane). Каждый профиль определяет bridge-интерфейс, подключённый к соответствующему VLAN.

7.2. Управление сетями

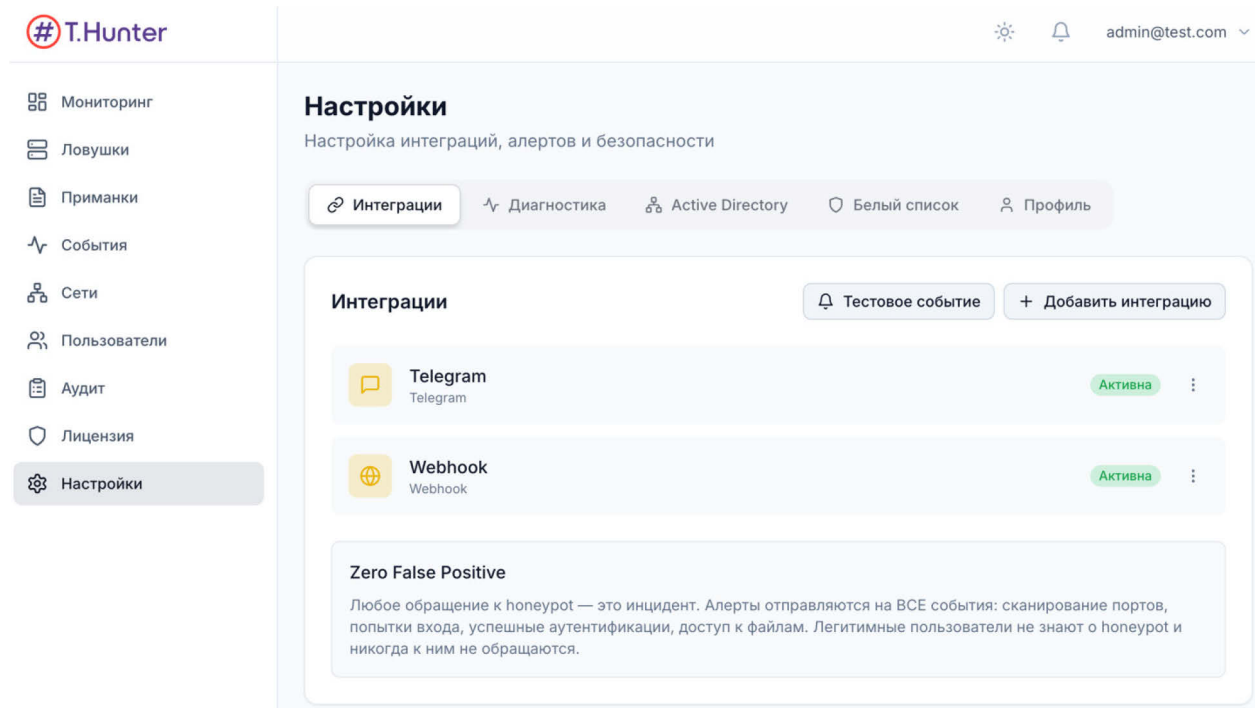
Для каждой сети доступны: редактирование имени и описания, удаление (только если в сети нет ловушек). Столбец «Ловушек» показывает количество ловушек, развёрнутых в данной сети.

8. Настройки

Раздел Настройки содержит пять вкладок: Интеграции, Диагностика, Active Directory, Белый список и Профиль.

8.1. Интеграции

Настройка каналов отправки уведомлений и экспорта событий.



СКРИНШОТ: Вкладка Интеграции — список настроенных интеграций (Email, Telegram, Webhook, SIEM Syslog) с индикаторами статуса

8.1.1. Email (SMTP)

Отправка алертов на email. Параметры: SMTP-сервер, порт, пользователь, пароль, адрес отправителя, адреса получателей, TLS.

8.1.2. Telegram

Отправка алертов в Telegram. Параметры: Bot Token (получается у @BotFather), Chat ID (ID чата или группы).

8.1.3. Webhook

Отправка событий POST-запросом на произвольный URL в формате JSON. Параметры: URL, опционально заголовки авторизации.

8.1.4. SIEM (Syslog)

Экспорт событий в SIEM через Syslog (RFC 5424). Параметры: хост, порт, протокол (UDP/TCP), формат (RFC 5424/CEF).

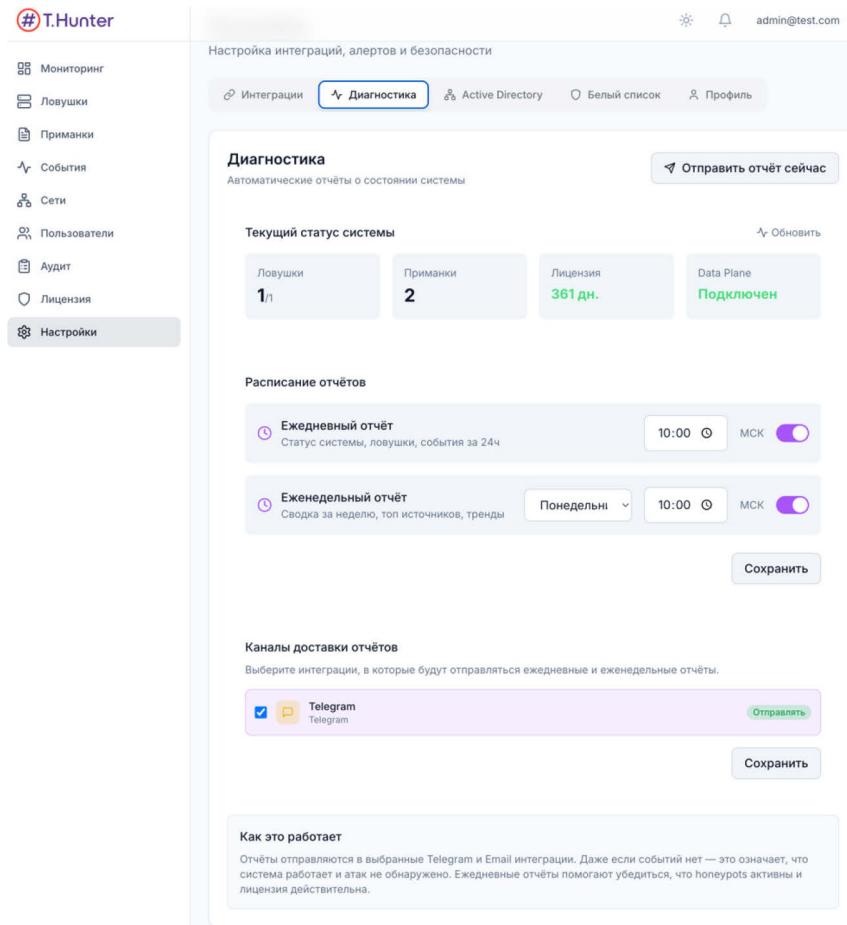
Для каждой интеграции доступны: тестирование связи, включение/отключение, удаление.

8.2. Диагностика

Настройка автоматической отправки диагностических отчётов о состоянии системы:

- Включение/отключение ежедневных и еженедельных отчётов

- Время отправки (по московскому времени)
- Каналы отправки (Telegram, Email)



СКРИНШОТ: Вкладка Диагностика — настройки расписания отчётов, переключатели ежедневных и еженедельных отчётов

8.3. Active Directory

Интеграция с Active Directory для обогащения событий данными о пользователях и хостах. Параметры:

- **Сервер** — адрес контроллера домена (ldap://dc.company.local)
- **Bind User** — служебная учётная запись для чтения AD
- **Bind Password** — пароль служебной учётной записи

После настройки система автоматически обогащает события: для каждого IP-источника определяется hostname, имя пользователя, отдел и должность.

Настройки
Настройка интеграций, алертов и безопасности

Интеграции Диагностика **Active Directory** Белый список Профиль

Active Directory
Интеграция с AD для обогащения событий и деплоя приманок

Не настроено • Не настроено

Настройка подключения ×

Сервер
dc.corp.local или 192.168.1.10
IP-адрес или hostname контроллера домена

Логин
admin@corp.local
Укажите домен: user@domain.local или DOMAIN\user

Пароль

Отмена Сохранить

СКРИНШОТ: Вкладка Active Directory — форма подключения к AD

8.4. Белый список

Управление IP-адресами и подсетями, исключёнными из мониторинга. Типы записей:

- **Инфраструктура** — серверы мониторинга, сканеры уязвимостей
- **Администрирование** — IP рабочих станций ИБ-команды
- **Тестирование** — временные исключения для тестов (с датой истечения)
- **Другое** — прочие исключения

Для каждой записи указывается IP или CIDR-диапазон, имя, описание, тип и опционально дата истечения.

Настройки

Настройка интеграций, алертов и безопасности

Интеграции

Диагностика

Active Directory

Белый список

Профиль

Белый список



IP-адреса сканеров и систем мониторинга (события записываются, но не алертятся)

+ Добавить

Поиск по имени или IP...

Все типы

Активные

Имя / IP	Тип	Статус	Срабатываний	Истекает	Действия
Infrastructure 10.0.124.237 <small>Auto-added: Data Plane endpoint</small>	system	Активен	0	—	 

СКРИНШОТ: Вкладка Белый список — таблица записей с типом, IP/CIDR, описанием, статусом, кнопка проверки IP

8.5. Профиль

Управление личной учётной записью:


- **Смена пароля** — требуется текущий пароль; новый должен соответствовать политике (12+ символов, заглавные/строчные буквы, цифры, спецсимволы)
- **Двухфакторная аутентификация (2FA)** — включение/отключение TOTP через приложение-аутентификатор (Google Authenticator, Authy и др.)

A A
admin@test.com
2FA выключена

Двухфакторная аутентификация

Настройка 2FA

Отсканируйте QR-код приложением-аутентификатором (Google Authenticator, Authy)



Или введите код вручную:
K2UDD645H60TA6QBNGF2MVRDX3DV6TT

Введите код из приложения

Смена пароля

Текущий пароль

Новый пароль

Подтверждение пароля

СКРИНШОТ: Вкладка Профиль — секция смены пароля, секция настройки 2FA с QR-кодом

9. MITRE ATT&CK

Система автоматически маппирует каждое событие на тактики и техники MITRE ATT&CK Framework. Это помогает классифицировать обнаруженные действия в контексте стандартизированной модели угроз.

Для каждого события отображается:

- **Тактика** — этап атаки (Reconnaissance, Lateral Movement, Credential Access и т.д.)
- **Техника** — конкретный метод (Remote Services, Brute Force, Network Sniffing и т.д.)
- **Подтехника** — детализация техники при наличии
- **Ссылка** — прямая ссылка на описание в базе MITRE

Маппинг выполняется автоматически на основе категории события, типа действия и контекста (тип сервиса, детали raw_data).

Приложение А. Матрица прав доступа

Право	Аналитик	Оператор	Администратор
Просмотр ловушек/приманок/сетей	✓	✓	✓
Создание ловушек/приманок/сетей	—	✓	✓
Управление ловушек/приманок/сетей	—	✓	✓
Удаление ловушек/приманок/сетей	—	✓	✓
Запуск/остановка ловушек	—	✓	✓
Просмотр событий	✓	✓	✓
Экспорт событий	✓	✓	✓
Удаление событий	—	—	✓
Просмотр настроек	✓	✓	✓
Изменение настроек	—	—	✓
Создание интеграций	—	✓	✓
Управление пользователями	—	—	✓
Просмотр аудит-лога	—	—	✓
Управление лицензией	—	—	✓

Приложение Б. Горячие клавиши и подсказки

- Нажатие на логотип Мираж возвращает на дашборд
- Уведомления помечаются как прочитанные при открытии панели
- Фильтры событий сохраняются в URL (можно делиться ссылкой на отфильтрованный вид)
- Дашборд автоматически обновляется каждые 30 секунд и по WebSocket
- В мобильной версии боковая панель скрывается и открывается по кнопке.