МИРАЖ

Система раннего обнаружения внутренних угроз

Руководство пользователя

Версия документа: 2.0.1
Дата редакции: 13 ноября 2026 г.
Разработчик: ООО «Ти Хантер»

Санкт-Петербург
2026

Содержание

1 Назначение 3

2 Вход в систему 3

3 Разделы интерфейса 3

4 Мониторинг 3

5 Список ловушек 4

6 Создание LXC-ловушки 4

7 Создание RealOS-ловушки 5

8 Состояния и действия с ловушками 6

9 Работа с приманками 7

9.1 Файловая приманка 7

9.2 URL Canary 8

10 Поиск и разбор событий 9

11 Сети и Data Plane 9

12 Пользователи и роли 10

13 Настройки и лицензия 11

14 Типовой разбор события 11

15 Если что-то не работает 11

16 Термины 12

17 Обращение в поддержку 12

1 Назначение

Руководство описывает ежедневную работу с Mirage 2.0.1: просмотр состояния ловушек, создание приманок и разбор событий. Состав разделов зависит от роли пользователя и лицензии.

2 Вход в систему

Откройте в браузере адрес Control Plane, начинающийся с HTTPS. Введите выданные администратором логин и пароль. Если для учётной записи включена двухфакторная аутентификация, введите код из второго фактора.

Если вход отклонён, запишите текст сообщения и время попытки. Передайте эти сведения администратору, который управляет учётными записями Mirage.

3 Разделы интерфейса

Боковое меню открывает основные страницы системы: «Мониторинг», «Ловушки», «Автогенерация», «Приманки», «Деплой», «Покрытие», «События», «Сети», «Пользователи», «Аудит», «Лицензия» и «Настройки». Некоторые пункты видны только пользователям с соответствующими правами.

4 Мониторинг

На панели «Мониторинг» собраны счётчики ловушек и приманок, число событий и инцидентов, сведения об активных RealOS-сессиях и графики событий. Кнопки «24ч», «7д» и «30д» меняют период графика. Нажмите на последнюю запись, чтобы перейти к её карточке в журнале событий.

Если на панели нули или нет графика, сначала проверьте выбранный период. Затем откройте «События» и убедитесь, что фильтры не скрывают записи.

5 Список ловушек

Откройте «Ловушки». Строка поиска находит ловушку по имени. Списки рядом фильтруют данные по статусу, операционной системе и типу окружения. В меню сортировки можно выбрать дату создания, имя, число событий или статус. Переключатель справа меняет карточный вид на таблицу.

Фильтр «Удалённые» показывает удалённые записи, если роль пользователя разрешает их просмотр. Чтобы вернуться к полному списку, очистите строку поиска и установите фильтры «Все».

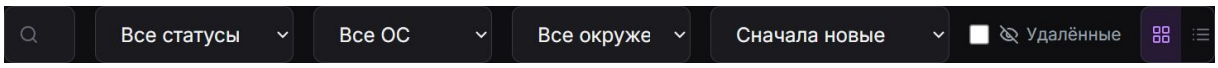

Рисунок 1 - Поиск, фильтры и переключение вида списка ловушек.

6 Создание LXC-ловушки

Нажмите «Создать ловушку» и оставьте выбранным тип «Обычная ловушка». Быстрый старт задаёт профиль и набор сервисов; после выбора их можно изменить. Выберите операционную систему и нужные сервисы, затем укажите имя ловушки и сеть Data Plane.

Имя вводится латинскими буквами. Допускаются цифры и дефис; имя должно начинаться с буквы. Сеть обязательна: если нужного сегмента нет в списке, попросите администратора добавить его.

Перед нажатием «Создать» проверьте сервисы и их порты. Выбирайте сеть, из которой тестовые рабочие станции смогут обратиться к ловушке. После отправки следите за статусом задачи на странице «Ловушки».

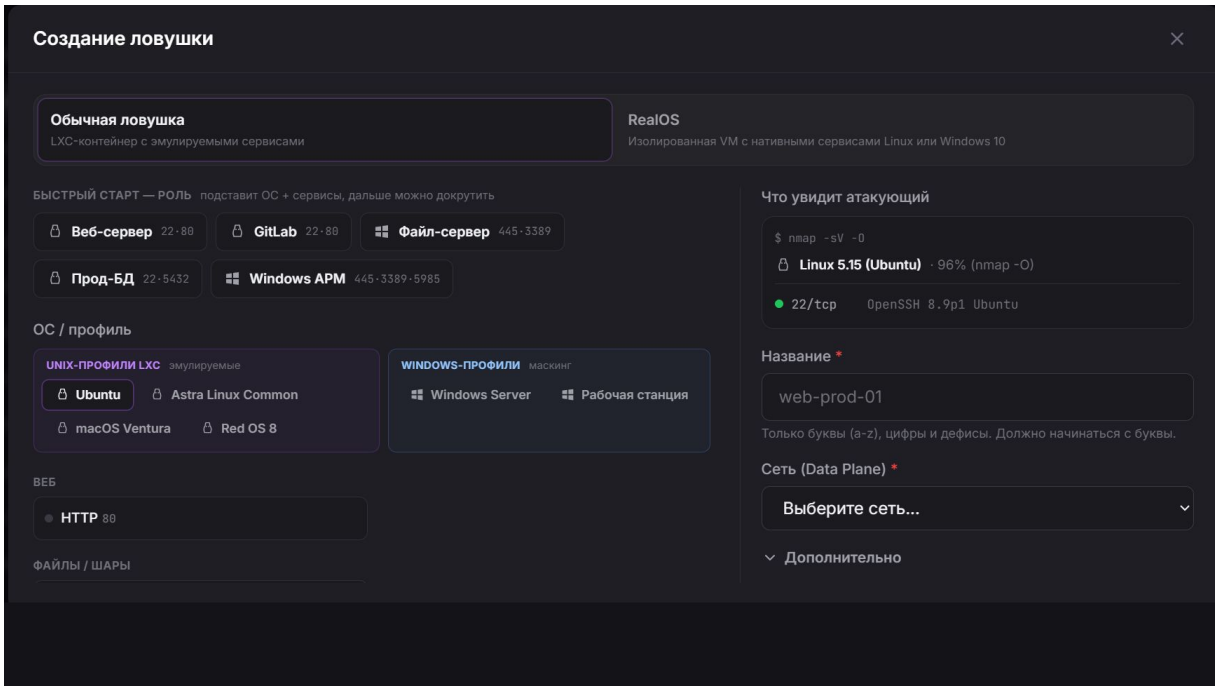

Рисунок 2 - Форма создания обычной LXC-ловушки. Показана верхняя часть формы.

7 Создание RealOS-ловушки

В форме создания переключитесь на вкладку «RealOS». Выберите доступный образ Ubuntu или Windows 10 и отметьте необходимые службы. Укажите сеть Data Plane и задайте имя, как для LXC-ловушки.

Для RealOS форма также содержит профиль рабочей роли, учётное имя, политику исходящих соединений и параметры очистки виртуальной машины. Значения TTL и Idle timeout задают ограничения времени сессии. Согласуйте их с ответственным за стенд до создания ловушки.

Перед отправкой проверьте, что выбранная сеть предназначена для тестовых машин, а политика исходящих соединений соответствует плану испытаний. После создания дождитесь завершения развёртывания; повторный запуск задачи не ускоряет уже выполняющуюся операцию.

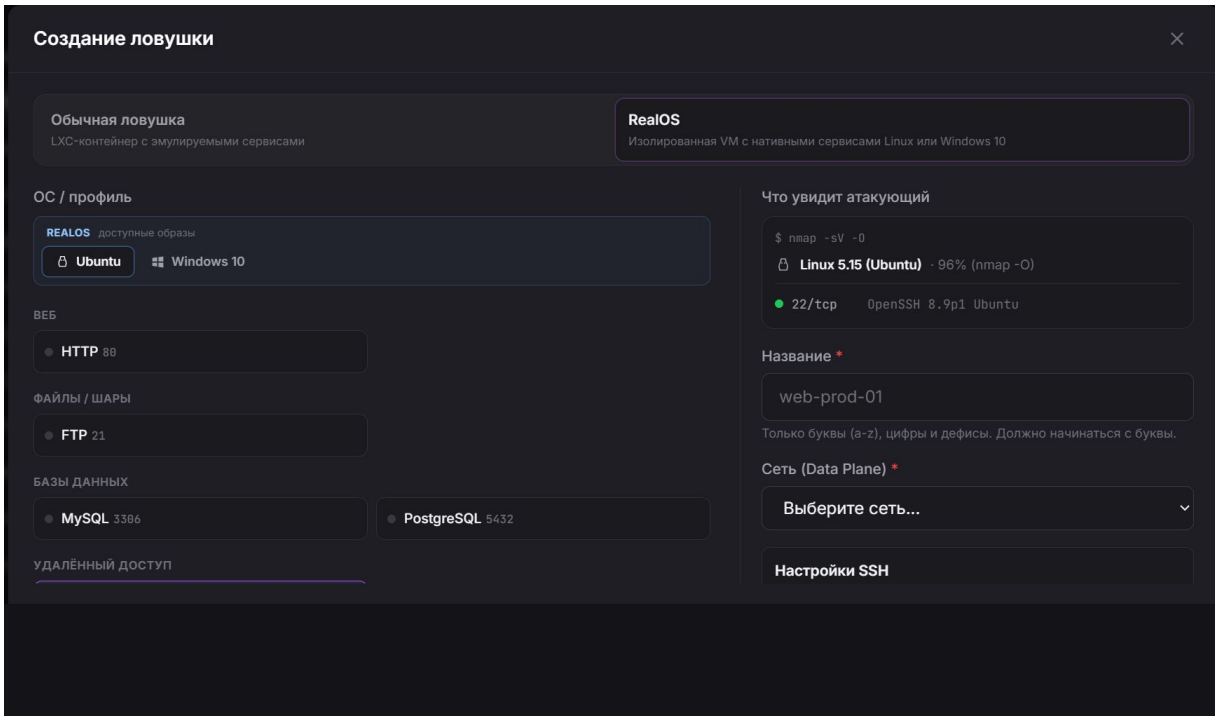

Рисунок 3 - Форма RealOS: образ, службы, сеть и параметры сессии. Нижняя часть формы находится ниже области снимка.

8 Состояния и действия с ловушками

В списке отображаются состояния «Развёртывание», «Работает», «Пауза», «Остановлена», «Ошибка», «Неисправна» и «Изолирована». Для ошибки откройте значок причины рядом со статусом и сохраните текст сообщения вместе с именем ловушки и временем.

Карточка ловушки содержит команды запуска, остановки, перезапуска и удаления. Доступные кнопки зависят от состояния и роли. Удалить работающую ловушку нельзя: сначала остановите её, затем подтвердите удаление.

Для RealOS доступны просмотр сессий, показ реквизитов доступа, изоляция сети и восстановление сети. Кнопка «Очистить» заменяет текущую виртуальную машину чистой копией. Перед подтверждением проверьте, что данные текущей сессии больше не нужны. Изоляция отключает сетевой доступ виртуальной машины; восстановите сеть после проверки инцидента.

Кнопка «Порты» открывает сведения о внешнем и внутреннем портах. Перед изменением внешнего порта проверьте, что он не занят другой службой и изменение согласовано с сетевым администратором.

9 Работа с приманками

На странице «Приманки» можно искать записи по имени и отбирать их по типу: файловые приманки или URL Canary. В верхней части страницы показаны счётчики созданных приманок и срабатываний.

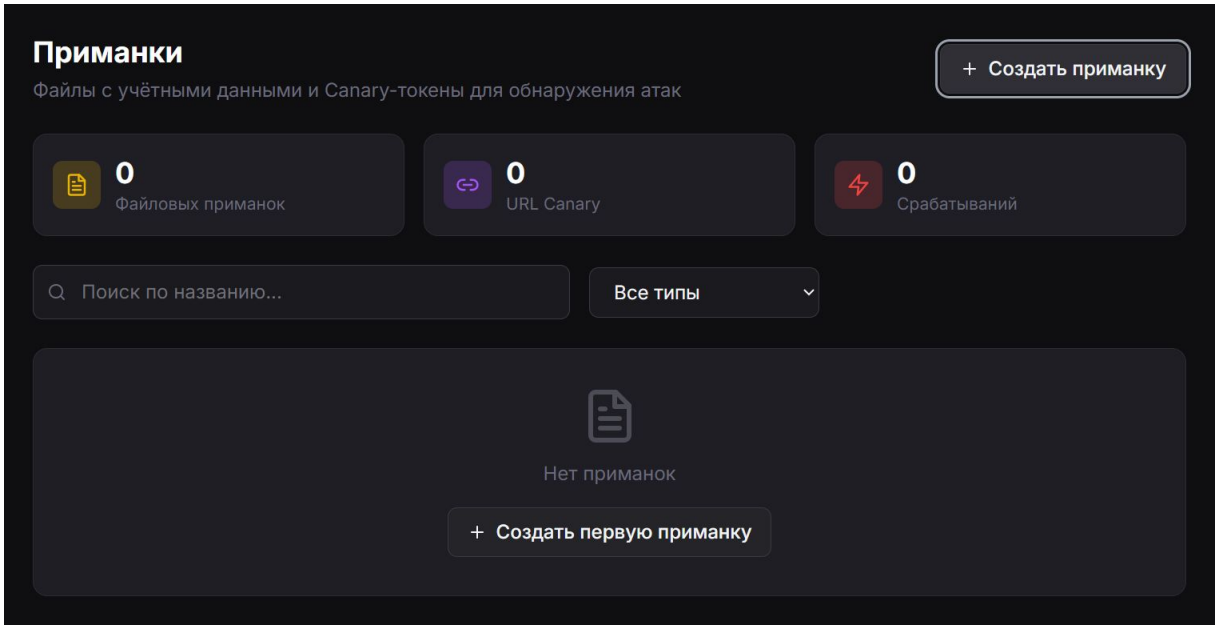

Рисунок 4 - Список приманок, поиск и фильтр по типу. На момент снимка список пуст.

9.1 Файловая приманка

Нажмите «Создать приманку» и выберите формат файла в каталоге. Доступны обычный текст, ENV, конфигурационные и JSON-файлы, а также форматы для SSH, RDP, Git, Docker, AWS, Kubernetes, PostgreSQL и MySQL. Для обычной файловой приманки укажите целевую ловушку, если форма этого требует.

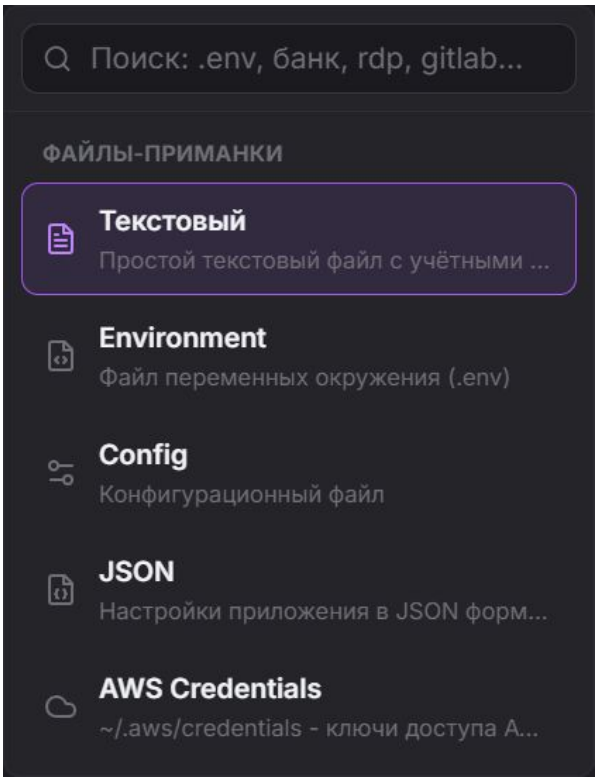

Рисунок 5 - Каталог форматов файловых приманок.

В карточке создания проверьте предполагаемое место размещения и предварительный просмотр содержимого. Используйте только тестовые учётные данные, созданные Mirage. Не подставляйте рабочие пароли, ключи или файлы из производственной среды. После создания скачайте файл и разместите его в тестовой папке или на выбранной рабочей станции.

9.2 URL Canary

Выберите тип «URL Canary» и задайте имя. В поле назначения можно выбрать Control Plane, подходящую ловушку или настроенный Data Plane relay. Если целевой компьютер находится в закрытом сегменте, используйте relay только при наличии соответствующего адреса в списке.

Создайте ресурс и скопируйте выданную ссылку. Поместите её в тестовый документ или другой согласованный объект. Открытие ссылки должно появиться в событиях как срабатывание приманки. Для DNS Canary используйте имя, выданное формой, и проверьте, что рабочая станция может разрешить его через настроенный DNS.

10 Поиск и разбор событий

Откройте страницу «События». По умолчанию выбран период «Последние 24 часа». Его можно заменить на час, 6 часов, 7 или 30 дней либо задать даты вручную. Фильтры позволяют отобрать уровень, категорию, статус и отображение инцидентов или записей белого списка. Поле поиска принимает IP-адрес источника.

Выберите строку события, чтобы открыть подробности. Сверьте время, источник, связанную ловушку, действие и категорию. Если событие связано с приманкой, проверьте её имя и метод срабатывания. В статусе укажите результат разбора: «Новое», «В работе», «Ложное» или «Закрыто».

Экспорт доступен в CSV и PDF. Для PDF можно выбрать краткий отчёт или отчёт с техническими деталями; период задаётся перед выгрузкой. Перед передачей отчёта проверьте, что в нём нет паролей, токенов и данных, которые нельзя передавать получателю.

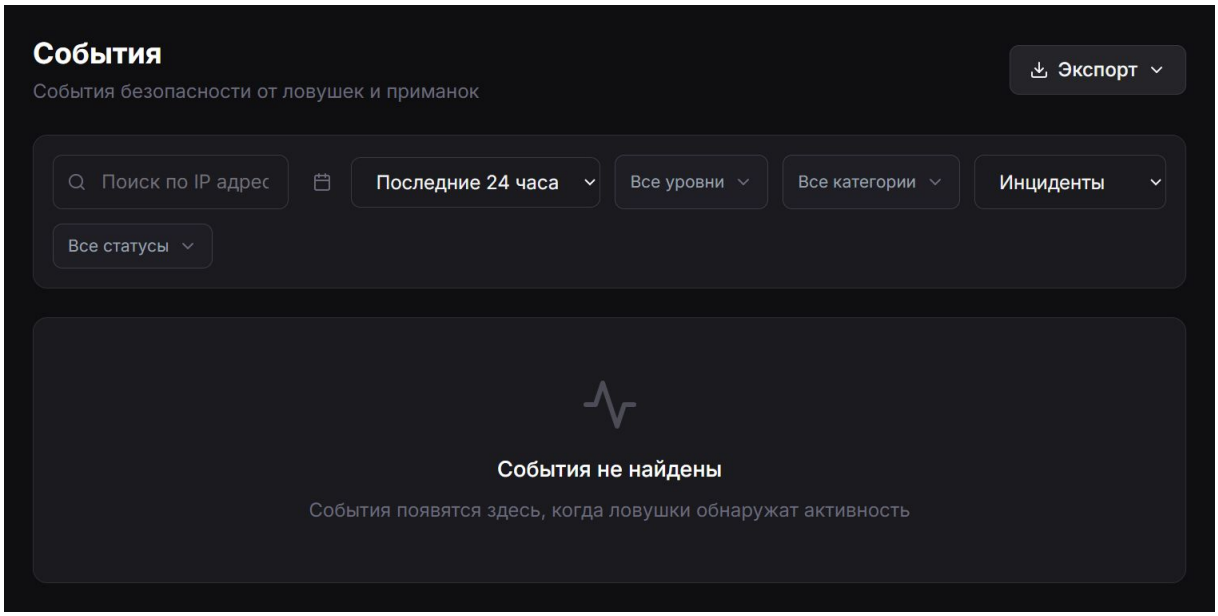

Рисунок 6 - Период и фильтры журнала событий. Снимок показывает пустое состояние списка.

11 Сети и Data Plane

Сеть связывает ловушку с нужным сегментом. При подготовке записи указывают её имя, Data Plane и CIDR; при необходимости задают VLAN, шлюз, DNS-серверы и адресный пул. Профиль, полученный с Data Plane, может заполнить часть параметров автоматически.

Перед созданием или изменением сети передайте администратору сегмент, VLAN, наличие DHCP и диапазон адресов, который разрешено выделить ловушкам. Если список профилей пуст или форма сообщает, что Data Plane недоступен, проверьте подключение узла с администратором.

В разделе «Data Plane» смотрите состояние узла. Если ловушка развёртывается, но не получает ожидаемый адрес, приложите к обращению её имя, выбранную сеть и время задачи.

12 Пользователи и роли

В системе предусмотрены роли «Аналитик», «Оператор» и «Администратор». Аналитик просматривает панели, ловушки и события и может выгружать отчёты. Оператор управляет ловушками, событиями и интеграциями. Администратор управляет пользователями и системными настройками. В конкретной установке доступ может быть ограничен дополнительными разрешениями.

Если нужная кнопка или раздел отсутствует, проверьте назначенную роль. Учётные записи добавляет и изменяет администратор.

13 Настройки и лицензия

В «Настройках» находятся разделы интеграций, диагностики, Active Directory, белого списка, Data Plane, RealOS и профиля. В интеграциях доступны Email (SMTP), Telegram, MAX, Webhook и SIEM через Syslog или Webhook. После сохранения конфигурации используйте тестовую отправку, если она доступна для выбранной интеграции.

Для Active Directory нужны адрес сервера каталога, домен и отдельная учётная запись интеграции. Параметры подключения передаёт администратор AD. Вкладка RealOS задаёт ресурсы для новых виртуальных машин; уже созданные ловушки эти настройки не меняют.

Страница «Лицензия» находится в боковом меню отдельно от «Настроек». Там проверяют состояние установленной лицензии. Если срок или состав лицензии не соответствует договору, обратитесь к администратору Mirage.

14 Типовой разбор события

1. Откройте карточку события и запишите время, источник и связанную ловушку.

2. Проверьте, какой сервис или приманка вызвали запись. Сопоставьте адрес с сегментом, где размещена ловушка.

3. Если действие ожидаемое, укажите это в статусе события. Если оно требует проверки, переведите запись в «В работе» и передайте данные ответственному за сеть или рабочую станцию.

4. После проверки внесите результат в карточку и установите итоговый статус. При повторяющихся разрешённых срабатываниях обсудите с администратором правило белого списка.

15 Если что-то не работает

- Ловушка долго остаётся в статусе «Развёртывание». Откройте задачу, сохраните её номер и сообщение. Проверьте выбранные Data Plane и сеть.

- Ловушка получила ошибку или статус «Неисправна». Откройте причину ошибки и приложите её к обращению.
- События не видны. Увеличьте период, сбросьте фильтры уровня, категории и статуса, затем проверьте время последнего heartbeat ловушки.
- URL Canary не срабатывает. Проверьте, что ссылка скопирована полностью и доступна из тестового сегмента. Если используется Data Plane relay, проверьте адрес relay вместе с администратором.
- Интеграция не получила событие. Запишите время и идентификатор события; передайте их администратору интеграции для проверки журнала доставки.

16 Термины

Термин	Значение
Control Plane (CP)	Веб-интерфейс и API для управления системой.
Data Plane (DP)	Узел, на котором размещаются ловушки и сетевые профили.
LXC	Контейнерная ловушка с эмулируемыми сервисами.
RealOS	Ловушка в отдельной виртуальной машине с нативной ОС и сервисами.
URL Canary	Уникальная ссылка, обращение к которой регистрируется как событие.
Heartbeat	Сообщение, по которому интерфейс показывает последнюю связь компонента с системой.

17 Обращение в поддержку

Передайте обращение по каналу, указанному в договоре. Укажите версию Mirage, время ошибки, имя ловушки или приманки, номер задачи или события и текст сообщения. Приложите снимок экрана, если он помогает воспроизвести проблему. Удалите из снимка адреса, пароли и данные пользователей, которые не относятся к обращению.