МИРАЖ

Система раннего обнаружения внутренних угроз

Документация, содержащая описание функциональных характеристик экземпляра программного обеспечения

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

Санкт-Петербург
2026

Содержание

1 Назначение 3

2 Область применения 3

3 Состав системы 3

4 Основные функции 3

4.1 Управление ресурсами 3

4.2 Регистрация и анализ событий 4

4.3 Администрирование 4

5 Архитектура и обмен данными 4

6 Условия применения 5

7 Ограничения 5

8 Сведения о правообладателе 5

1 Назначение

«Мираж» управляет ловушками и приманками в сети организации и регистрирует обращения к ним. Администратор настраивает систему через веб-интерфейс.

В документе описаны функции Mirage 2.0.1. Доступ к отдельным функциям определяется лицензией и настройками установленного экземпляра.

2 Область применения

Система регистрирует обращения к сервисам ловушек, файлам-приманкам и URL/DNS canary-ресурсам. Состав наблюдаемых событий зависит от включённых источников телеметрии.

3 Состав системы

Таблица 1 - Состав системы.

Компонент	Описание
Control Plane (CP)	Веб-интерфейс, API и управление системой.
Data Plane (DP)	Размещение ловушек и передача событий на CP.
Ловушка	Узел с выбранными сервисами.
Приманка	Файл или сетевой адрес, обращение к которому регистрируется.

4 Основные функции

4.1 Управление ресурсами

- создание, изменение, запуск, остановка и удаление ловушек в пределах разрешений пользователя;
- выбор Data Plane, сетевого профиля и поддерживаемых сервисов при создании ловушки;
- создание файловых приманок и URL/DNS canary-ресурсов; доступные типы зависят от версии и конфигурации.

4.2 Регистрация и анализ событий

- приём событий от включённых источников телеметрии и отображение их в журнале;
- поиск, фильтрация, просмотр карточки события и доступные действия подтверждения;
- классификация и сопоставление с MITRE ATT&CK для поддерживаемых типов событий;
- передача данных во внешние системы через настроенные интеграции.

Событие содержит данные, полученные от источника. Само по себе оно не устанавливает причину обращения.

4.3 Администрирование

- управление учётными записями и ролями;
- настройка интеграций, сетей и параметров системы в пределах роли;
- просмотр журнала аудита и состояния компонентов, если соответствующие разделы доступны пользователю.

5 Архитектура и обмен данными

Control Plane и Data Plane работают как отдельные компоненты. CP управляет объектами через LXD API на DP. События и heartbeat поступают на CP напрямую или через настроенный relay. Для защищённых соединений используются TLS и сертификаты.

Состав портов и направлений сетевого обмена определяется конкретной схемой установки. Перед вводом в эксплуатацию следует сверить правила межсетевого экрана с руководством по установке и фактическими параметрами релиза.

6 Условия применения

Для работы требуются совместимые серверы Linux для CP и DP, сетевой доступ между компонентами, ресурсы хранения для базы данных и образов, а также браузер с поддержкой современного JavaScript. Конкретные поддерживаемые ОС, версии зависимостей и размеры серверов указываются в документации того же релиза, что установлен у заказчика.

Нагрузочные показатели и предельное число ловушек зависят от выбранных сервисов, числа событий, характеристик хранилища и сетевой топологии. Их определяют при проектировании и пилотной эксплуатации.

7 Ограничения

- система регистрирует только те действия, которые наблюдаются включёнными ловушками, приманками и источниками телеметрии;
- доступность функций зависит от роли, лицензии, настройки и состояния CP/DP;
- приманки размещаются в инфраструктуре заказчика только после согласования места, типа и сценария использования.

8 Сведения о правообладателе

Правообладатель программного обеспечения «Мираж» - ООО «Ти Хантер».