

Документация, содержащая описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения, в том числе устранение неисправностей и совершенствование, а также информацию о персонале, необходимом для обеспечения такой поддержки

Программное обеспечение

«Мираж — Система раннего обнаружения внутренних угроз»

ООО «Ти Хантер»

2026

Содержание

Общая информация	3
Наименование системы	3
Назначение системы	3
Рекомендуемые технические характеристики	4
Серверная часть (Control Plane).....	4
Серверная часть (Data Plane).....	5
Рабочее место администратора.....	5
Поддержание жизненного цикла программного обеспечения	6
Описание технической инфраструктуры.....	6
Языки программирования и фреймворки	6
Архитектура системы	7
Устранение неисправностей	7
Техническая поддержка.....	7
Информация о персонале	8
Фактический адрес размещения разработчиков	9
Фактический адрес размещения службы поддержки.....	9
Процесс разработки ПО.....	9
Дорожная карта развития	10

Общая информация

Программное обеспечение «Мираж» представляет собой платформу раннего обнаружения внутренних угроз информационной безопасности, размещённую на виртуальных машинах в корпоративной сети. Система работает на основе технологии обмана (Deception Technology) и предназначена для выявления несанкционированной активности внутри периметра.

Платформа разворачивает в инфраструктуре заказчика специализированные ловушки и приманки, имитирующие реальные сетевые сервисы и данные. Любое взаимодействие с ловушками гарантированно является инцидентом безопасности (принцип Zero False Positives), что позволяет выявлять боковое перемещение, инсайдерские угрозы и действия АPT-группировок на ранних этапах атаки.

Наименование системы

Система раннего обнаружения внутренних угроз «Мираж».

Правообладатель: **ООО «Ти Хантер»**.

Назначение системы

Программное обеспечение «Мираж» обеспечивает выполнение следующих функций:

1. Авторизация и аутентификация пользователей (JWT, 2FA TOTP), управление пользователями и ролями.
2. Управление ловушками — создание, развёртывание, запуск, остановка, перезапуск, удаление LXD-контейнеров с эмуляцией 9 сетевых протоколов (SSH, HTTP, SMB, RDP, FTP, MySQL, PostgreSQL, MSSQL, WinRM).
3. Управление приманками — создание файловых приманок и URL canary-токенов, скачивание для ручного размещения, автоматическое размещение с использованием интеграции с Active Directory.
4. Управление сетями — создание и настройка сетевых профилей (VLAN/bridge) для размещения ловушек в различных сегментах инфраструктуры.
5. Сбор и обработка событий безопасности по принципу Zero False Positives с классификацией по степени критичности (severity).

6. Автоматический маппинг событий на тактики и техники MITRE ATT&CK.
7. Мониторинг в реальном времени — дашборд с карточками статистики, временной шкалой, тепловой картой, рейтингом источников атак, визуализацией MITRE ATT&CK.
8. Фильтрация, поиск, подтверждение (acknowledge) и экспорт событий безопасности (CSV, JSON, PDF).
9. Анализ покрытия — контроль охвата сетевых сегментов ловушками (реестр подсетей с классификацией по категории и важности, анализ достижимости, рекомендации по развёртыванию) и охвата пользователей AD приманками (профилирование по ролям, выявление высокоценных целей, статистика и рекомендации по размещению).
10. Интеграции — настройка каналов оповещения (Email, Telegram, Webhook, SIEM Syslog) и обогащение событий через Active Directory.
11. Белый список — управление IP-адресами и подсетями, исключёнными из мониторинга, с типизацией и сроком действия.
12. Диагностические отчёты — автоматическая отправка ежедневных и еженедельных отчётов о состоянии системы.
13. Аудит действий пользователей — полный журнал операций с экспортом в CSV.
14. Лицензирование — привязка к аппаратному отпечатку (hardware fingerprint), поддержка офлайн-активации, ограниченный режим работы.

Рекомендуемые технические характеристики

Серверная часть (Control Plane)

Управляющий компонент, обеспечивающий работу веб-интерфейса, API, базы данных и обработку событий.

Параметр	Требование
Операционная система	Ubuntu Server 22.04/24.04 LTS, Debian 11/12, Astra Linux SE 1.7/1.8, РЕД ОС 7.3/8, Альт СП 10, Альт Сервер 10, Альт Виртуализация 10, РОСА ХРОМ Сервер
Процессор	4 vCPU (x86_64)
Оперативная память	8 ГБ (рекомендуется 16 ГБ)

Дисковое пространство	100 ГБ SSD
Сетевые интерфейсы	1 Ethernet (управляющая сеть)
Программное обеспечение	Docker 24+, Docker Compose 2.20+

Серверная часть (Data Plane)

Компонент, обеспечивающий работу LXD-контейнеров с ловушками и сетевой доступ к целевым сегментам.

Параметр	Требование
Операционная система	Ubuntu Server 22.04/24.04 LTS, Debian 11/12, Astra Linux SE 1.7/1.8, РЕД ОС 7.3/8, АЛЬТ СП 10, АЛЬТ Сервер 10, АЛЬТ Виртуализация 10, РОСА ХРОМ Сервер
Процессор	4 vCPU (x86_64), рекомендуется 8 vCPU
Оперативная память	8 ГБ (рекомендуется 16 ГБ)
Дисковое пространство	200 ГБ SSD
Сетевые интерфейсы	2+ Ethernet (управляющая сеть + целевые сегменты VLAN)
Программное обеспечение	LXD 5.0+, Python 3.11+
Виртуализация	Поддержка вложенной виртуализации (nested virtualization)

Рабочее место администратора

Для работы с веб-интерфейсом управления Системой необходимо:

Параметр	Требование
Веб-браузер	Яндекс.Браузер 23+, Google Chrome 104+, Chromium-Gost 104+, Mozilla Firefox 115+, Microsoft Edge 104+
Разрешение экрана	1920×1080 и выше
Сетевое подключение	Доступ к Control Plane по HTTPS (порт 443)

Поддержание жизненного цикла программного обеспечения

Поддержание жизненного цикла программного обеспечения «Мираж» обеспечивается ООО «Ти Хантер» за счёт непрерывного сопровождения и проведения обновлений в соответствии с внутренним планом разработки, а также по заявкам заказчиков. В рамках поддержания жизненного цикла осуществляются следующие работы:

- выпуск обновлений, устраняющих выявленные неисправности и уязвимости;
- разработка и внедрение нового функционала в соответствии с дорожной картой развития продукта;
- адаптация и тестирование совместимости с новыми версиями операционных систем и зависимостей;
- обновление документации при изменении функциональности;
- консультирование заказчиков по вопросам установки, настройки и эксплуатации;
- помощь в поиске и устранении проблем в случае некорректной работы Системы.

Обновления доставляются заказчикам в виде пакетов обновлений (release-архивов) для установки в изолированных средах без доступа к сети Интернет.

Описание технической инфраструктуры

Языки программирования и фреймворки

Компонент	Технологии
Серверная часть (backend)	Python 3.11+, FastAPI, SQLAlchemy 2.0, Celery, asyncio
Клиентская часть (frontend)	TypeScript, React 18, Vite
База данных	PostgreSQL 15+
Кэширование и очереди	Redis 7+
Контейнеризация	Docker, Docker Compose, LXD 5.0+

Архитектура системы

Система построена по двухуровневой архитектуре:

Control Plane — управляющий компонент, включающий веб-интерфейс, REST API, базу данных PostgreSQL, систему очередей Redis и Celery. Развёртывается в Docker-контейнерах.

Data Plane — компонент исполнения, обеспечивающий работу LXD-контейнеров с ловушками. Каждая ловушка — изолированный LXD-контейнер с набором эмулируемых сетевых сервисов. Контейнеры подключаются к целевым сегментам сети через настраиваемые сетевые мосты (bridges) и VLAN-интерфейсы.

Взаимодействие между Control Plane и Data Plane осуществляется по защищённому каналу с использованием mTLS-аутентификации.

Устранение неисправностей

Неисправности, выявленные в ходе эксплуатации программного обеспечения, устраняются следующими способами:

- выпуск обновлений (patch-релизов), содержащих исправления. Обновления доставляются в виде архивов для офлайн-установки;
- оперативное исправление конфигурации по запросу заказчика с участием специалиста технической поддержки через защищённый удалённый доступ;
- предоставление обходных решений (workaround) до выпуска исправления в следующей версии.

Техническая поддержка

Пользователи программного обеспечения «Мираж» могут обращаться в службу технической поддержки по следующим каналам:

- электронная почта: support@tomhunter.ru;
- Telegram-канал технической поддержки;
- телефон: +7 (812) 677-17-05.

Регламент обработки обращений:

- устранение критических неисправностей (полная неработоспособность Системы, потеря данных, нарушение безопасности) — в срок не более 24 часов;
- устранение существенных неисправностей (отказ отдельных модулей, некорректная обработка событий) — в срок не более 3 рабочих дней;
- устранение незначительных неисправностей (косметические ошибки интерфейса, неточности документации) — в срок не более 10 рабочих дней.

Классификация критичности неисправности определяется специалистами технической поддержки.

Служба технической поддержки работает в рабочие дни (понедельник — пятница) с 10:00 до 19:00 (МСК). По критическим инцидентам предусмотрено экстренное реагирование вне рабочего времени.

Информация о персонале

Обеспечение поддержки продукта осуществляется силами штатных сотрудников ООО «Ти Хантер».

Гарантийное обслуживание и развитие программного обеспечения:

Должность	ФИО
Разработчик	Художил Александр Анатольевич

Техническая поддержка программного обеспечения:

Должность	ФИО
Разработчик	Художил Александр Анатольевич

Фактический адрес размещения разработчиков

Отдел разработки находится по месту регистрации организации: 196191, г. Санкт-Петербург, вн.тер.г. муниципальный округ Новоизмайловское, пл. Конституции, д. 7, литера А, помещ. 171-Н, офис 639.

Фактический адрес размещения службы поддержки

Служба технической поддержки находится по месту регистрации организации: 196191, г. Санкт-Петербург, вн.тер.г. муниципальный округ Новоизмайловское, пл. Конституции, д. 7, литера А, помещ. 171-Н, офис 639.

Процесс разработки ПО

Разработка программного обеспечения «Мираж» ведётся в соответствии с итеративной методологией. Каждая итерация включает полный цикл работ от постановки задачи до выпуска обновления.

Каждая итерация включает следующие этапы:

1. Планирование. Формулирование требований на основании дорожной карты развития, результатов анализа угроз и запросов заказчиков. Декомпозиция требований в технические задания.
2. Разработка. Реализация функционала в соответствии с техническим заданием. Код проходит обязательное ревью, статический анализ безопасности и проверку на соответствие стандартам оформления.
3. Тестирование. Модульное тестирование (unit-тесты), интеграционное тестирование, тестирование безопасности (проверка ловушек инструментами nmap, netexec, impacket и другими инструментами тестирования на проникновение). Тестирование проводится в изолированной среде, воспроизводящей условия заказчика.
4. Исправление дефектов. В случае обнаружения дефектов разработчик вносит исправления, после чего функционал повторно подвергается тестированию до полного устранения выявленных проблем.
5. Выпуск. Формирование релиз-пакета, обновление документации, подготовка инструкций по обновлению. Пакет подписывается цифровой подписью для подтверждения целостности.
6. Внедрение. Доставка обновления заказчикам и оказание поддержки при установке.

Система контроля версий обеспечивает полную трассируемость изменений. Каждый релиз имеет уникальный номер версии в формате MAJOR.MINOR.PATCH (семантическое версионирование).

Дорожная карта развития

План развития продукта предусматривает реализацию следующих функциональных возможностей:

Направление развития	Плановый срок
Расширение библиотеки HTTP-пресетов: шаблоны 1С-Битрикс, Roundcube, vSphere, Proxmox, GitLab для повышения реалистичности ловушек	Q2 2026
Модуль Desertion Mesh — автоматическая генерация ландшафта ловушек на основе анализа реальной инфраструктуры (сканирование сети, интеграция с AD, профилирование именования и сервисов)	Q3 2026
Получение сертификата ФСТЭК России	2027

Конкретные сроки реализации могут корректироваться с учётом приоритетов заказчиков, результатов пилотных проектов и требований регуляторов.