Платформа имитации ИТ-инфраструктуры R-Vision Threat Deception Platform.

Руководство по эксплуатации

Версия 1.0

ОГЛАВЛЕНИЕ

Руководство по эксплуатации по системе Платформа имитации ИТ-инфраструктуры R-Vision Threat Deception Platform (далее по тексту - TDP) содержит пошаговые инструкции и рекомендации по работе с системой.

1. О ПРОДУКТЕ

Платформа имитации ИТ-инфраструктуры R-Vision Threat Deception Platform (R-Vision Threat Deception Platform, TDP) представляет собой комплекс технологий цифровой имитации объектов ИТ-инфраструктуры для раннего обнаружения злоумышленников, проникших в корпоративную сеть, и предотвращения атак на ранних этапах.

С помощью набора программных ловушек и приманок R-Vision TDP обнаруживает присутствие киберпреступника, замедляет его продвижение внутри сети, запутывая среди ложных объектов, и дает возможность ИБ-специалистам остановить развитие атаки до того, как она приведет к значимому ущербу.

Платформа R-Vision TDP решает следующие задачи:

- Выявляет постоянные серьезные угрозы (APT) и уязвимости нулевого дня (zero-day) на ранних стадиях.
- Собирает данные о злоумышленнике.
- Затрудняет и замедляет продвижение атакующего внутри сети.

Преимущества от использования платформы R-Vision TDP:

- Обнаружение злоумышленников, сумевших обойти классические средства защиты и мониторинга.
- Снижение скорости продвижения атакующего внутри сети, искажение периметра ложными элементами инфраструктуры.
- Возможность предотвращения атак на ранних стадиях.
- Понимание инструментов и действий злоумышленника в отношении конкретной инфраструктуры организации, выявление слабых мест в защите.
- Низкий процент ложных срабатываний.

Платформа поставляется как локальное (on-premise) приложение, поставляемое в виде настроенного образа виртуальной машины.

Платформа состоит из управляющего сервера (Control Center) и сервера управления ловушками (Trap Manager). Возможности платформы по генерации ловушек можно расширять за счет добавления новых серверов управления ловушками.

Через веб-интерфейс управляющего сервера (Control Center) происходит настройка и управление системой.

К центру управления подключается один или несколько серверов управления ловушками (Trap Manager). Эти серверы можно развернуть на отдельном физическом или виртуальном сервере. Серверов-ловушек может быть несколько. На каждом из таких серверов могут быть развернуты одна или несколько ловушек.

Все происходящие в системе события платформа сохраняет в централизованный журнал. Записи можно просмтореть с помощью web-интерфейса как в виде отдельных событий, так и в виде дашборда, на который выводится сводная информация.

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

2.1. Управляющий сервер

Характеристика	Минимальные значения	Рекомендуемые значения
Процессор	4 ядра 2.4 ГГц	6 ядер 2,4 Ггц
Оперативная память	8 ГБ	32 и более ГБ
Дисковое пространство (SSD-накопитель)	150 ГБ	500 ГБ
Сетевые интерфейсы	1 - интерфейс управления	1 - интерфейс управления
Операционная система	CentOS 7 x64	CentOS 7 x64

2.2. Сервер управления ловушками

Характеристика	Рекомендуемое значение
Процессор	4 ядра 2.4 ГГц
Оперативная память	16 ГБ
Дисковое пространство	100 ГБ
Сетевые интерфейсы	1 - интерфейс управления 1 и более - порт доступа/магистральный порт
Операционная система	CentOS 7 x64

2.3. Сетевое взаимодействие между компонентами платформы

Источник	Назначение	Протокол	Порт
Управляющий сервер	Сервер управления ловушками	SSH	22 TCP

Источник	Назначение	Протокол	Порт
Управляющий сервер	Сервер управления ловушками	HTTP(S)	80/443 TCP
Сервер управления ловушками	Управляющий сервер	lumberjack	5044 TCP
FullOS Traps (Windows, Linux)	Управляющий сервер	lumberjack	5044 TCP
АРМ Пользователя (Консоль управления R- Vision Deception)	Управляющий сервер	HTTP(S)	80/443 TCP

3. НАСТРОЙКА

В этом разделе приведено описание параметров платформы и даны рекомендации по настройке.

3.1. О серверах управления ловушками

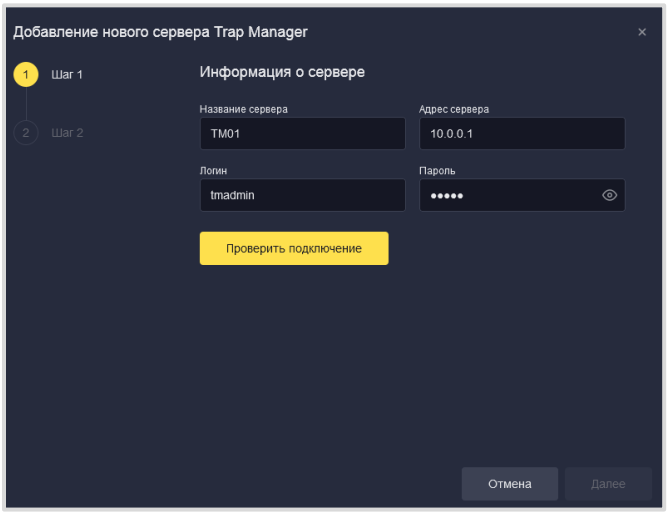
Сервер управления ловушками (Сервер Trap Manager) - это выделенный сервер на котором размещаются ловушки. Система может работать с несколькими серверами.

На сервере может размещаться несколько ловушек разных типов. После добавления сервера для дальнейшей работы на него нужно добавить ловушки.

3.2. Добавление сервера управления ловушками

Чтобы добавить сервер управления ловушками (Trap Manager):

1. Перейдите в раздел Настройки → Серверы Trap Manager.
2. Нажмите на кнопку Добавить. На экране отобразится окно добавления сервера Trap Manager.



3. На первом шаге укажите данные для подключения к серверу:
   a. Название сервера.
   b. Адрес сервера.
   c. Логин.
   d. Пароль.

4. Проверить корректность введенных данных можно по кнопке **Проверить подключение**. Система попытается подключиться к указанному серверу и отобразит сообщение о доступности сервера или об ошибке подключения.
5. Нажмите на кнопку **Далее**, чтобы завершить настройку сервера и перейти к шагу 2.
6. На втором шаге в окне отобразится список сетевых интерфейсов, обнаруженных на сервере Trap Manager. Для используемых сетевых интерфейсов укажите метки VLAN ID.
7. Нажмите на кнопку **Добавить**. Сервер Trap manager отобразится в списке. Если сервер работает корректно, то слева в строке сервера отображается статус **Активно**.

3.3. Просмотр информации о сервере управления ловушками

Информация о серверах управления ловушками отображается в разделе **Серверы Trap Manger**.

Просмотреть подробную информацию о сервере можно по нажатию на строку. На экране отобразится карточка сервера.

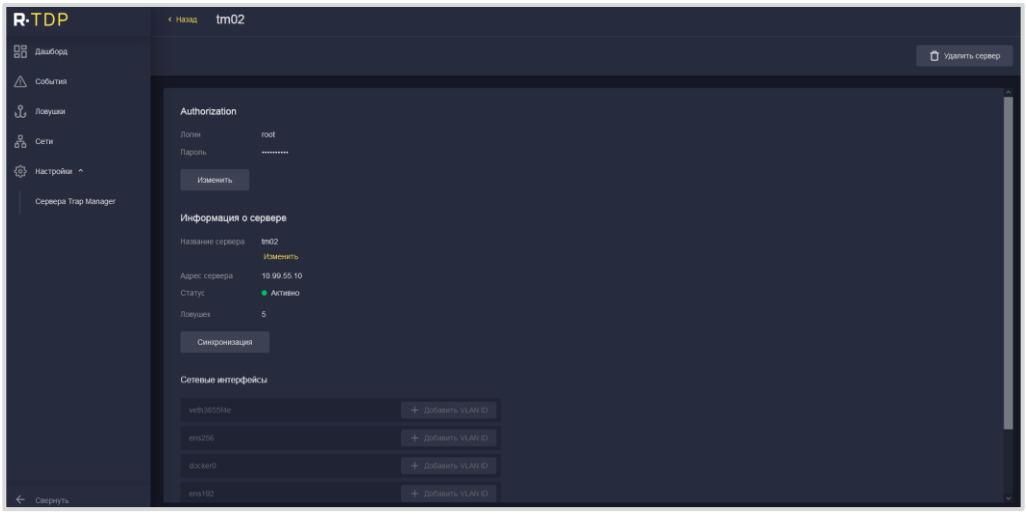
В карточке представлена информация о сервере:

- Данные для авторизации. Данные можно редактировать по кнопке **Изменить**.
- Информация о сервере. Кнопка **Синхронизация** запускает синхронизацию данных с сервером: обновляет данные о сетевых интерфейсах и ловушках.
- Сетевые интерфейсы и метки VLAN ID.

В карточке и в списке отображается статус сервера Trap Manager:

- Активно: сервер работает.
- Подключение: система подключается к серверу.
- Ошибка: сервер не работает.

Удалить сервер можно по кнопке **Удалить сервер** в верхнем правом углу экрана.



3.4. Удаление сервера управления ловушками

Чтобы удалить сервер управления ловушками:

1. Перейдите в раздел Серверы Trap Manager.
2. Выберите в списке сервер. На экране отобразится карточка сервера.
3. В правом верхнем углу экрана нажмите на кнопку **Удалить сервер**.
4. Подтверите удаление. Сервер будет удален из системы.

4. РАБОТА С СЕТЯМИ

В этом разделе приведены инструкции по работе с сетями, в которых размещаются ловушки.

4.1. О сетях

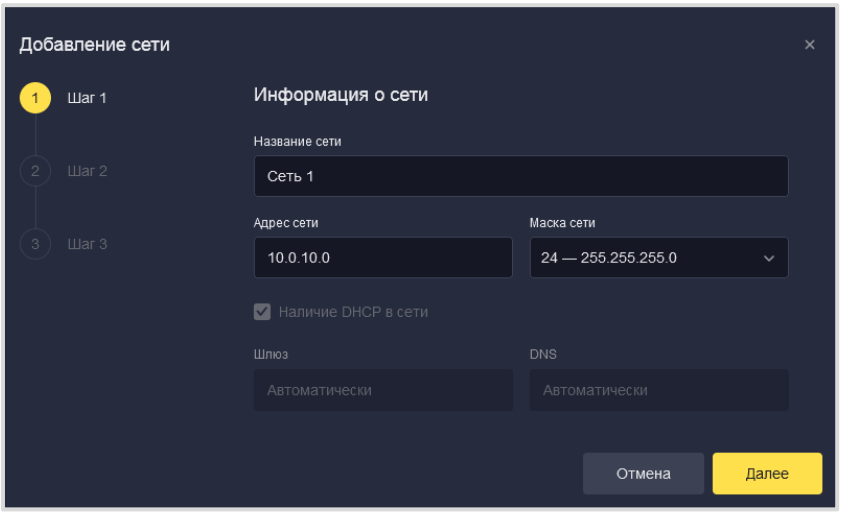
Сеть (Network) - это сущность, отражающая конфигурацию сети для размещения в ней ловушек. В системе каждая сеть уникальна (по IP адресу и маске сети). Сеть может быть привязана к нескольким сетевым интерфейсам разных серверов Trap Manager. Доступ к сети осуществляется через предоставленные интерфейсы на Control Center или сервере Trap Manager.

> В рамках одного сервера сеть может быть привязана только к одному интерфейсу.

4.2. Добавление сетей

Чтобы добавить сеть:

1. Перейдите в раздел **Сети**.
2. Нажмите на кнопку **Добавить сеть**. На экране отобразится окно **Добавление сети**.



3. На первом шаге настройте информацию о сети:

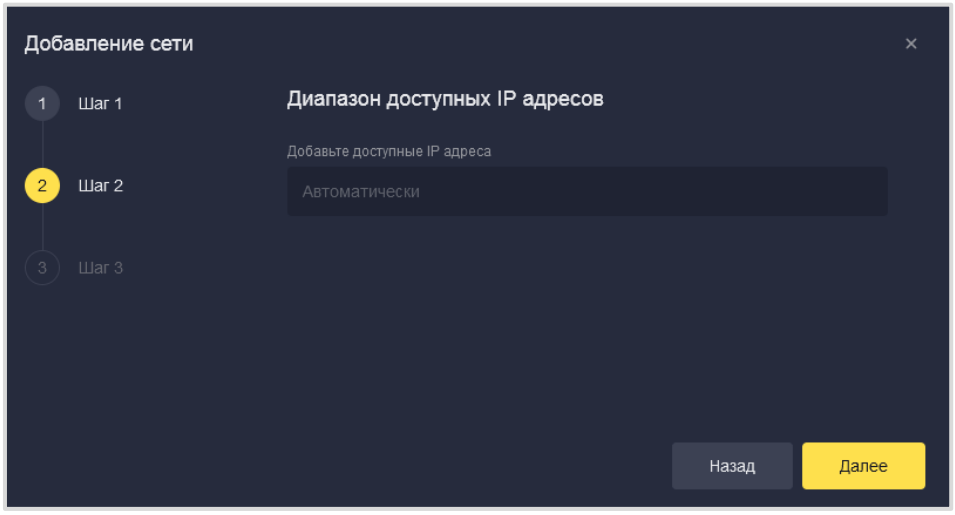
   a. Название.

b. Адрес.

c. Маска.

4. Для перехода на следующий шаг нажмите на кнопку **Далее**.

5. На втором шаге настройте диапазон доступных IP-адресов сети. Диапазон формируется автоматически.



6. Для перехода на следующий шаг нажмите на кнопку **Далее**.

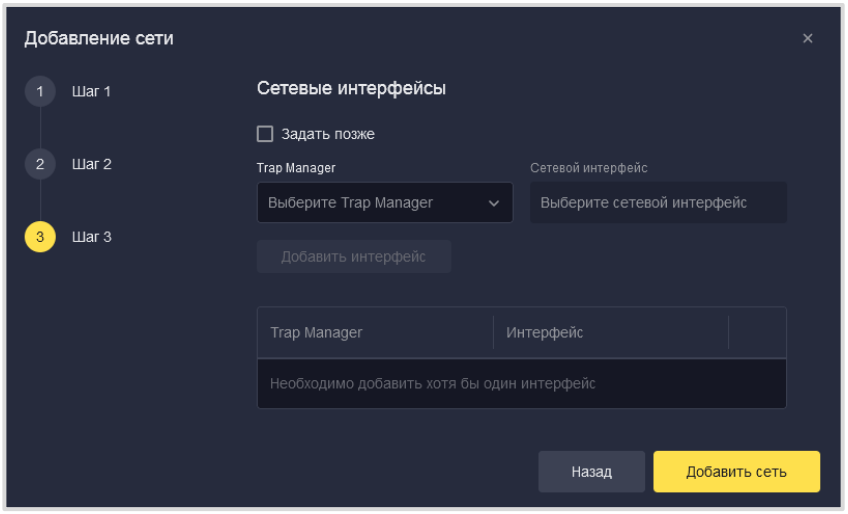
7. На третьем шаге сформируйте список сетевых интерфейсов серверов Trap Manager для работы с сетью. Для добавления интерфейса:

a. Выберите сервер Trap Manager.

b. Укажите сетевой интерфейс для работы с сетью.

c. Нажмите на кнопку **Добавить интерфейс**. Интерфейс отобразится в таблице в нижней части окна. Повторите шаги a - c для каждого интерфейса, которые нужно добавить.

d. Вы можете установить флажок **Задать позже**, чтобы завершить настройку сети без добавления интерфейсов. Добавить интерфейсы можно при редактировании свойств сети.



8. Нажмите на кнопку **Добавить сеть**. Сеть отобразится в списке в разделе **Сети**.

4.3. Просмотр информации о сети

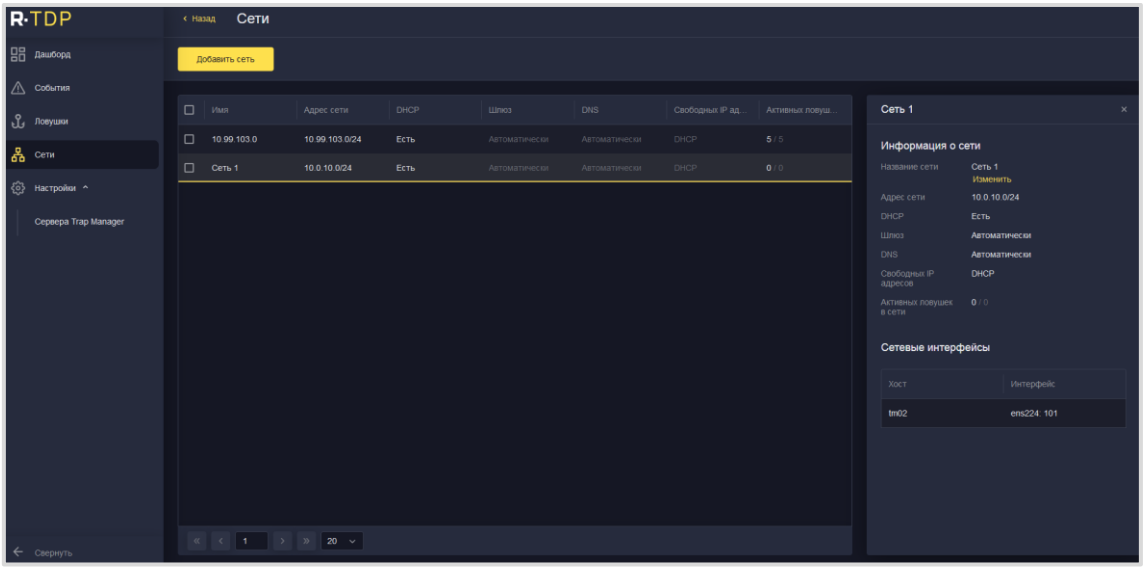
Информация о сетях отображается в разделе **Сети**.

Просмотреть подробную информацию о сети можно по нажатию на строку в списке сетей. В правой части экрана отобразится карточка сети.

В карточке представлена информация о сети:

- Название. Название можно редактировать по ссылке **Изменить**.
- Адрес сети.
- Наличие DHCP.
- Информация о шлюзе и DNS-сервере.
- Количество свободных IP-адресов.
- Количество ловушек в сети: активных и общее.
- Сетевые интерфейсы и серверы Trap Manager.

Вы можете выбрать несколько сетей в списке с помощью флажка в левой части списка.



4.4. Удаление сети

Чтобы удалить сеть:

1. Перейдите в раздел **Сети**.
2. Выберите одну или несколько сетей с помощью флажка в левой части списка.

> После удаления сети связанные с ней ловушки будут недоступны.

3. Нажмите на кнопку **Удалить**.
4. Подтвердите удаление. Сети будут удалены из системы.

5. РАБОТА С ЛОВУШКАМИ

В этом разделе описаны действия по управлению ловушками.

5.1. О ловушках

Ловушка (Trap) - это любой сервер/docker контейнер, с помощью которого можно собрать информацию о злоумышленнике и его действиях. Ловушки размещаются на серверах управления ловушками (Trap Manager).

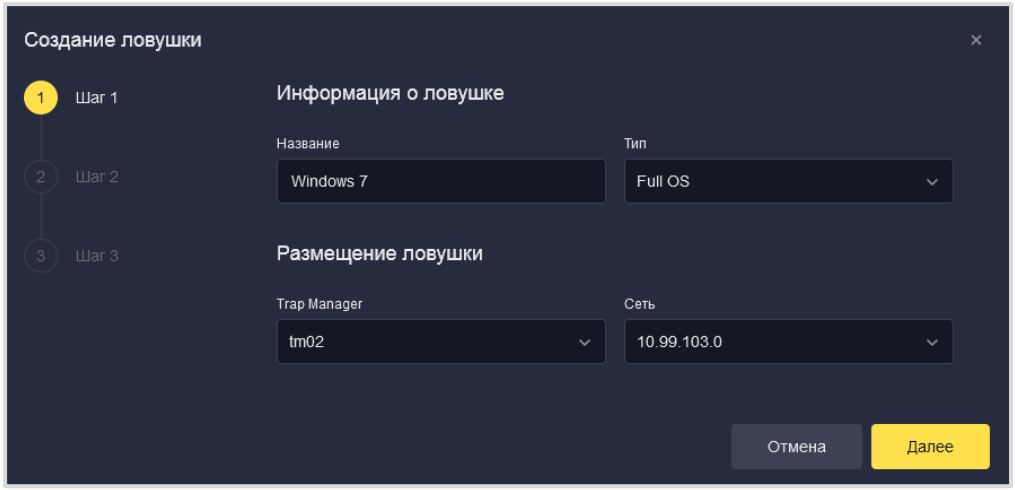
Существует три категории ловушек:

- **High-Interaction** - виртуальная машина, которая может быть Windows/Linux сервером, сетевым оборудованием или виртуальным appliance.
- **Medium-Interaction** - Docker контейнер, который может быть любым сервисом или его эмуляцией. Предполагает взаимодействие злоумышленника с ловушкой.
- **Low-Interaction** - Docker контейнер, который не предполагает прямое взаимодействие злоумышленника с ловушкой.

5.2. Добавление ловушек

Чтобы добавить ловушку:

1. Перейдите в раздел **Ловушки**.
2. Нажмите на кнопку **Создать ловушку**. На экране отобразится окно **Создание ловушки**.



3. На первом шаге заполните информацию о ловушке:

a. Название.

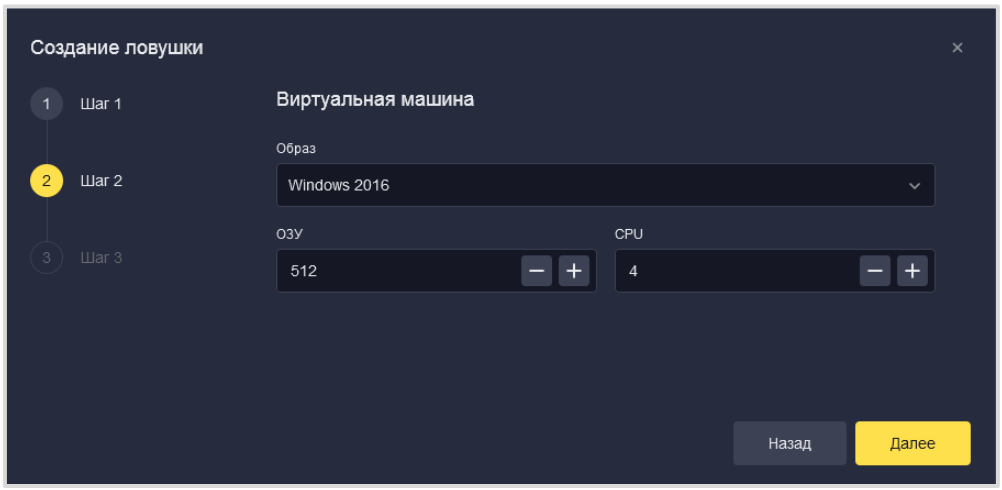
b. Тип.

c. Trap Manager, к которому привязана ловушка.

d. Сеть, с которой связана ловушка.

4. Для перехода на следующий шаг нажмите на кнопку **Далее**.
5. Набор параметров, настраиваемый на втором шаге, зависит от выбранного типа ловушки:

a. FullOS: выберите образ, укажите объем ОЗУ и количество процессоров на виртуальной машине.



b. SMB: Параметры протокола SMB, параметры ресурсов. Список ресурсов отобразится в таблице в нижней части окна.

c. SSH: Параметры протокола SSH, тип аутентификации (учетная запись пользователя или случайная),

6. Для перехода на следующий шаг нажмите на кнопку **Далее**.
7. На третьем шаге в окне отобразятся настроенные параметры. Убедитесь, что параметры заданы верно и нажмите на кнопку **Сохранить**. Если при настройке допущена ошибка, вернитесь на предыдущий шаг по кнопке **Назад**.

5.3. Просмотр ловушек

Информация о сетях отображается в разделе **Ловушки**.

Просмотреть подробную информацию о ловушке можно по нажатию на строку в списке ловушек. В правой части экрана отобразится карточка ловушки. Кнопка **Подробнее** отображает карточку в расширенном режиме.

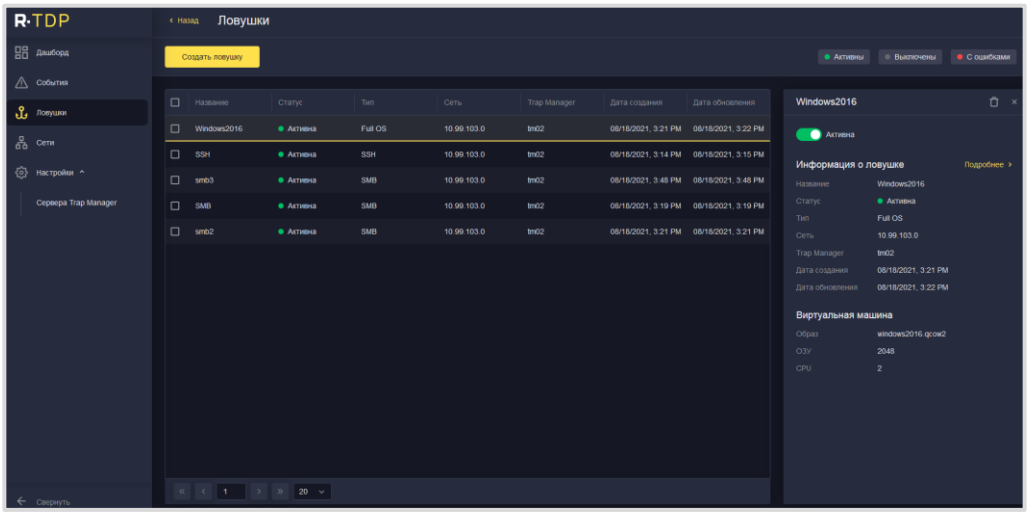
В карточке представлена информация о ловушке (набор данных зависит от типа ловушки):

- Статус. Ловушку можно отключить с помощью переключателя в верхней части карточки.
- Название.
- Статус.
- Тип.
- Сетевые параметры.
- Сервер Trap Manager.
- Дата создания и обновления.
- Параметры протокола или виртуальной машины (в зависимости от типа ловушки).

Вы можете выбрать несколько ловушек в списке с помощью флажка в левой части списка.

В карточке и в списке отображается статус ловушки:

- Активна: ловушка работает.
- Выключена: ловушка отключена. Вы можете включить ловушку с помощью переключателя в карточке ловушки.
- С ошибкой: ловушка не работает. Возможна ошибка в настройках ловушки.



5.4. Удаление ловушек

Чтобы удалить ловушку:

1. Перейдите в раздел **Ловушки**.
2. Выберите одну или несколько ловушек с помощью флажка в левой части списка.
3. Нажмите на кнопку **Удалить**.
4. Подтвердите удаление. Ловушки будут удалены из системы.

6. МОНИТОРИНГ СОБЫТИЙ

В этом разделе приведены инструкции по работе с журналом событий.

6.1. О событиях

Событие (Event) - это зарегистрированное действие на ловушке. Ловушка предоставляет сообщение с подробной информацией о событии.

События различаются по уровню критичности:

- Критичный. Событие требует немедленной реакции.
- Высокий. Событие реакции.
- Средний. Событие может угрожать безопасности, но не требует срочного реагирования.
- Низкий. Событие требует обработки в плановом порядке.

6.2. Просмотр событий

Раздел **События** содержит список событий, связанных с регистрацией действий на ловушке.

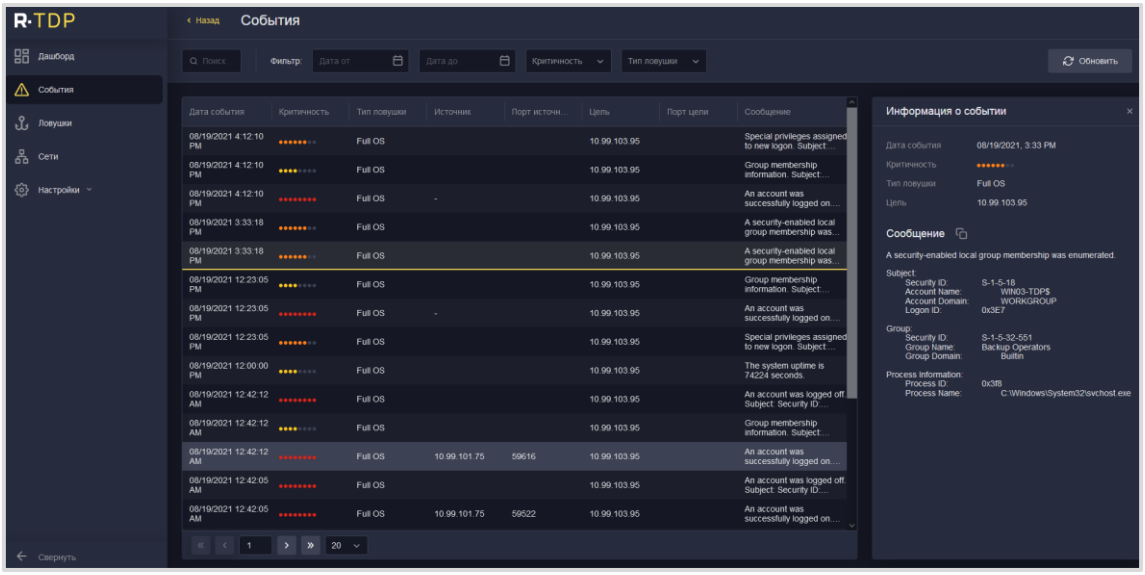
В списке событий отображается следующая информация:

- дата;
- критичность;
- тип ловушки, на которой произошло событие;
- источник (атакующий);
- порт источника (атакующего);
- цель;
- порт цели;
- сообщение.

По щелчку на событии в списке можно просмотреть карточку события. В карточке приводятся данные о событии и текст сообщения. Скопировать сообщение в буфер обмена можно по кнопке  .

Вы можете использовать поле поиска для поиска события в списке. Список можно фильтровать по значениям параметров в группе **Фильтр** над списком событий.

Кнопка **Обновить** в правом верхнем углу экрана обновляет список событий.


R·TDP
Назад
События
Дашборд
События
Ловушки
Сети
Настройки
Свернуть
Поиск
Фильтр:
Дата от
Дата до
Критичность
Тип ловушки
Обновить
Дата события
Критичность
Тип ловушки
Источник
Порт источн...
Цель
Порт цели
Сообщение
08/19/2021 4:12:10 PM
Full OS
10.99.103.95
Special privileges assigned to new logon. Subject:...
08/19/2021 4:12:10 PM
Full OS
10.99.103.95
Group membership information. Subject:...
08/19/2021 4:12:10 PM
Full OS
10.99.103.95
An account was successfully logged on...
08/19/2021 3:33:18 PM
Full OS
10.99.103.95
A security-enabled local group membership was...
08/19/2021 3:33:18 PM
Full OS
10.99.103.95
A security-enabled local group membership was...
08/19/2021 12:23:05 PM
Full OS
10.99.103.95
Group membership information. Subject:...
08/19/2021 12:23:05 PM
Full OS
10.99.103.95
An account was successfully logged on...
08/19/2021 12:23:05 PM
Full OS
10.99.103.95
Special privileges assigned to new logon. Subject:...
08/19/2021 12:00:00 PM
Full OS
10.99.103.95
The system uptime is 74224 seconds.
08/19/2021 12:42:12 AM
Full OS
10.99.103.95
An account was logged off. Subject: Security ID:...
08/19/2021 12:42:12 AM
Full OS
10.99.103.95
Group membership information. Subject:...
08/19/2021 12:42:12 AM
Full OS
10.99.101.75
59616
10.99.103.95
An account was successfully logged on...
08/19/2021 12:42:05 AM
Full OS
10.99.103.95
An account was logged off. Subject: Security ID:...
08/19/2021 12:42:05 AM
Full OS
10.99.101.75
59522
10.99.103.95
An account was successfully logged on...
1
20
Информация о событии
Дата события
08/19/2021, 3:33 PM
Критичность
Тип ловушки
Full OS
Цель
10.99.103.95
Сообщение
A security-enabled local group membership was enumerated.
Subject:
Security ID: S-1-5-18
Account Name: WIN03-TDP$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Group:
Security ID: S-1-5-32-551
Group Name: Backup Operators
Group Domain: Builtin
Process Information:
Process ID: 0x3f8
Process Name: C:\Windows\System32\svchost.exe

7. РАБОТА С ГРАФИКАМИ

В этом разделе приведено описание работы с графиками в системе.

7.1. Об отображении данных

Дашборд отображает сводные данные о работе системы. Нна дашборде отображаются показатели работы системы, например, статистака ловушек и событий.

Данные обновляются автоматически.

7.2. Просмотр данных на дашборде

Чтобы просмотреть данные, перейдите в раздел **Дашборд**.

Для просмотра подробной информации наведите курсор мыши на сегмент графика.

Изменить размер виджета можно, потянув за нижний правый угол.

Переместить виджет на дашборде можно перетаскиванием мышью за заголовок виджета.