

Общество с ограниченной ответственностью
«Инфрасек»

Infrasec Deception

Руководство пользователя

Версия 1.0

ОГЛАВЛЕНИЕ

Введение 3

1. Создание ловушек 3

1.1. Добавление узла ловушек 3

1.2. Добавление сетевого интерфейса 3

1.3. Добавление ловушек 3

1.4. Управление ловушками 4

2. Создание приманок 4

2.1. Создание скрипта распространения приманок 4

2.2. Распространение приманок 4

3. Создание Canary-токенов 4

4. Работа с инцидентами 5

5. Генерация рекомендаций ловушек 5

6. Управление пользователями 5

7. Управление ключами 6

7.1. Предварительная настройка Узла ловушек 6

7.2. Добавление ключа 6

8. Настройка передачи событий 6

9. Настройка уведомлений 7

10. Добавление исключений 7

.

Введение

Данный документ содержит инструкции по работе с системой Infrasec Deception.

1. Создание ловушек

1.1. Добавление узла ловушек

Для добавления узла ловушек необходимо:

1.1.1. Перейти в раздел Ловушки;

1.1.2. Нажать кнопку «Создать»;

1.1.3. Написать название Узла и выбрать тэг ключа. Необходимо добавить предварительно ключ, инструкция по добавлению которых описана в разделе 7 настоящей Инструкции;

1.1.4. Нажать кнопку «Создать».

1.2. Добавление сетевого интерфейса

Для добавления сетевого интерфейса необходимо:

1.2.1. Перейти в выбранный Узел ловушек;

1.2.2. Нажать кнопку создать;

1.2.3. Заполнить необходимые поля: Имя виртуального интерфейса, имя интерфейса подключения, и IP-адрес;

1.2.4. Нажать кнопку «Создать».

1.3. Добавление ловушек

1.3.1. Перейти в выбранный Узел ловушек и Сетевой интерфейс;

1.3.2. Нажать кнопку «Добавить»;

1.3.3. Из появившегося списка нажатием «+» добавить необходимые ловушки. При желании есть возможность добавить Шаблон сервера – предопределенный набор ловушек;

1.3.4. Нажать «Создать»;

1.3.5. Через некоторое время все выбранные Ловушки будут созданы и подняты на выбранном сетевом интерфейсе выбранного Узла ловушек.

1.4. Управление ловушками

1.4.1. Перейти в выбранный Узел ловушек и Сетевой интерфейс;

1.4.2. Можно останавливать работу, перезапускать, удалять и запускать ловушки с помощью соответствующих кнопок на веб-интерфейсе.

2. Создание приманок

Распространение и создание приманок происходит безагентским способом. Для этого необходимо сконфигурировать скрипт для соответствующей операционной системы и запустить его.

2.1. Создание скрипта распространения приманок

2.1.1. Перейти в раздел «Приманки»;

2.1.2. Нажать кнопку «Создать»;

2.1.3. Выбрать тип операционной системы, для которой будет сгенерировать скрипт распространения приманок (Linux, Windows);

2.1.4. Выбрать типы существующих ловушек, для которых будут сгенерированы приманки;

2.1.5. Выбрать конкретные ловушки, для которых будут сгенерированы приманки и варианты их создания;

2.1.6. Нажать кнопку «Создать»;

2.1.7. В «Загрузки» будет сохранен скрипт распространения приманок.

2.2. Распространение приманок

Для распространения приманок на защищаемые хосты, необходимо запустить полученный скрипт распространения приманок с правами администратора. Для массового распространения рекомендуется использовать средства автоматизации.

3. Создание Canary-токенов

3.1. Перейти в раздел «Canary-токены»;

3.2. Нажать кнопку «Создать»;

3.3. Заполнить «Тег» и выбрать тип файла Canary-токена;

3.4. Нажать кнопку «Создать»;

3.5. Если был выбран файл, то он будет автоматически загружен в «Загрузки». Если выбран URL, то необходимо напротив URL Canary-токена нажать кнопку «скопировать»;

3.6. В зависимости от выбранной модели защиты, разместите Canary-токены по ИТ-инфраструктуре.

4. Работа с инцидентами

Для работы с инцидентами перейдите в раздел «Инциденты»

3.1. Выберите интересующий тикет инцидента;

3.2. Возможно назначать инцидент на себя путем нажатия кнопки «Назначить на меня»;

3.3. Возможно изменение Статуса инцидента;

3.4. Возможно изменение Статуса закрытия инцидента;

3.5. Возможно добавление вердикта инцидента.

5. Генерация рекомендаций ловушек

В системе присутствует возможность генерации рекомендаций серверов ловушек, которые генерируются на основе анализа сетевых портов и протоколов сегментов сети. Для генерации рекомендацией необходимо

5.1. Перейти в раздел «Активы»;

5.2. Нажать кнопку «Сканировать»;

5.3. Ввести сеть для сканирования;

5.4. После проведения сканирования сеть появится во вкладке «Сканированные сети»;

5.5. Перейдите в интересующую вас сеть;

5.6. Нажмите кнопку «Составить рекомендацию». Рекомендация будет создана и будет доступна во вкладке «Рекомендации узлов ловушек».

6. Управление пользователями

6.1. Перейдите в раздел «Общие» во вкладку «Управление пользователями»;

6.2. Доступные операции над пользователями: отключить, включить, удалить и создать;

6.3. В системе доступны две роли:

А) Администратор – возможно выполнение всех доступных действий в системе;

Б) Пользователь – доступ только на просмотр, без возможности осуществлять внесение изменений в систему.

7. Управление ключами

Управление ключами необходимо для возможности управления узлами ловушек. Для этого необходимо предварительно сгенерировать ключевую пару ключей. Например, на операционной системе Debian 12 — это возможно осуществить командой

```
ssh-keygen -t rsa -b 4096
```

7.1. Предварительная настройка Узла ловушек

7.1.1. Создайте пользователя

```
useradd -m -s /bin/bash agent
```

7.1.2. Добавьте пользователя в группу sudo

```
usermod -aG sudo agent
```

7.1.3. Настройте sudo без пароля

```
echo "agent ALL=(ALL) NOPASSWD:ALL" > /etc/sudoers.d/agent
chmod 440 /etc/sudoers.d/agent
```

7.1.4. Добавьте пользователя в группу sudo

```
usermod -aG sudo agent
```

7.1.5. Добавьте ваш публичный ssh ключ в authorized_keys в /home/agent/.ssh

7.2. Добавление ключа

7.2.1. Перейдите в раздел «Общие» во вкладку «Управление SSH-ключами»

7.2.2. Заполните поле «Тег» и либо вставьте закрытый ключ в форму системы, либо добавьте файл закрытого ключа

7.2.3. После выполнения функций

8. Настройка передачи событий

В системе есть возможность передавать данные об инцидентах в SIEM. Для этого:

8.1. Перейдите в раздел «Передача событий»;

8.2. Нажмите «Добавить»;

8.3. Заполните необходимую информацию для передачи логов;

8.4. Нажмите «Создать».

9. Настройка уведомлений

В системе есть возможность передавать данные об инцидентах в виде оповещений. Для этого

9.1. Перейдите в раздел «Уведомления»;

9.2. Выберите канал для уведомлений;

9.3. В зависимости от типа канала заполните необходимые поля;

9.4. Нажмите «Создать».

10. Добавление исключений

В системе есть возможность добавлять исключения IP-адресов, по которым не будут генерироваться инциденты. Это необходимо для добавления различных сканеров безопасности или хостов для проведения анализа защищенности. Для добавления IP в исключения:

10.1. Перейдите в раздел «Исключения»;

10.2. Нажмите кнопку «Создать»;

10.3. Введите IP-адрес вручную или добавьте пул адресов через добавление файла.