Настройка централизованного управления образами контейнеров и контейнерами

С помощью модулей Opensearch и Neuvector обеспечивается чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора и выгрузку данных. Специальных настроек для реализации данного функционала не требуется. Изделие анализирует возникающие события безопасности и выявляет инциденты безопасности с помощью модуля Neuvector. Модуль Nevector поставляется преднастроенным и содержит следующие интеграции, доступные сразу после его установки:

- Интеграция со службой непрерывного развертывания FluxCD, с помощью которой выполняется установка, настройка и поддержание консистентности модуля в кластере Kubernetes;
- Интеграция с Nova OAuth: после установки модуля администратор кластера может выполнить вход в Neuvector с помощью OIDC и существующих учетных записей;
- Интеграция с Secrets Manager: конфигурационные файлы Neuvector, содержащие чувствительные данные, не хранятся в Kubernetes, а генерируются “на лету” из секретов в Secrets Manager;
- Преднастроенные правила Admission Control, определяющие базовые политики контроля операций в Kubernetes;
- Преднастроенные политики автоматического сканирования узлов и кластера Kubernetes;
- Дополнительный сервис Neuvector API Docs с офлайн-документацией по работе с Neuvector API.

Настройка контроля целостности

Проверка целостности образов контейнеров осуществляется с использованием механизма цифровой подписи образа контейнера с помощью криптографических методов.

Цифровая подпись образа контейнера требуется для подтверждения, что образ контейнера:

- не был изменен или подделан – образ остался неизменным с момента его создания и подписания;
- создан доверенным источником – образ выпущен доверенным разработчиком или организацией;
- соответствует политике безопасности - средством контроля и анализа защищенности автоматически отклоняет неподписанные или недоверенные образы.

При сборке контейнера вычисляется его хеш-сумма, и на ее основе создается цифровая подпись с помощью закрытого ключа владельца. Подпись сохраняется в реестре контейнеров. Перед развертыванием образа средством контроля и анализа защищенности использует открытый ключ для проверки цифровой подписи, чтобы убедиться в его подлинности.

Самостоятельный контроль целостности образов контейнеров реализуется в платформе следующими компонентами:

- система безопасности Neuvector;
- система сбора журналов событий Opensearch.

Проверка цифровой подписи образов контейнеров в системе безопасности Neuvector основана на решениях открытого проекта Sigstore, реализующего техники и рекомендации SLSA для контроля цепочки поставок.

Инфраструктурные компоненты для осуществления полного цикла цифровой подписи по умолчанию доступны в сети Интернет, однако вы можете установить их локально:

- **Rekor** – сервер журналирования артефактов;
- **Fulcio** – служба выдачи временных сертификатов;
- **Cosign** – инструмент подписи образов контейнеров и артефактов;
- Доверенный репозиторий **TUF**.

1. Настройка проверки целостности образов с использованием публичной инфраструктуры Sigstore

Для настройки проверки целостности образов контейнеров и исполняемых файлов контейнеров необходимо выполнить следующие действия:

1. Подготовить отдельный внешний реестр контейнеров для хранения образов контейнеров;
2. Подготовить анализируемый образ контейнера без цифровой подписи и загрузить его в реестр контейнеров.
3. Установить и настроить модуль системы безопасности Neuvector согласно процедурам, описанным в документации:
    - Ознакомиться с системными требованиями к модулю Neuvector и спланировать установки согласно руководству Планирование и системные требования.
    - Выполнить установку модуля Neuvector согласно статье Установка в конфигурации по умолчанию.
    - Сгенерировать пару ключей для цифровой подписи и выполнить настройку проверки подписи в Neuvector согласно руководству.

2. Настройка проверки целостности образов с использованием собственной инфраструктуры Sigstore

Для настройки проверки целостности образов контейнеров и исполняемых файлов контейнеров с использованием собственной инфраструктуры Sigstore необходимо выполнить следующие действия:

1. Подготовить отдельный сервер для установки компонентов Sigstore с техническими характеристиками:
    - Количество ядер процессора: не менее 4 шт.;
    - Количество ОЗУ: не менее 8 ГБ;
    - Объем хранилища: не менее 32 ГБ.
2. Установить на сервер ПО Docker согласно документации.
3. Установить сервер Rekor, выполнив команды:

```bash
$ git clone https://github.com/sigstore/rekor.git
$ cd rekor
```

```
$ git checkout tags/v1.3.9
$ docker compose -f docker-compose.yml up -d
```

4. Выполнить проверку доступности сервера Rekor, выполнив команду:

```
$ curl http://localhost:3000/api/v1/log
{"inactiveShards":null,"rootHash":"……960","treeSize":0
}
```

5. Получить публичный ключ сервера Rekor, выполнив команду:

```
$ curl http://localhost:3000/api/v1/log/publicKey

-----BEGIN PUBLIC KEY-----
MFkwEwYH….wezl==
-----END PUBLIC KEY-----
```

6. Установить сервер Fulcio, выполнив команды:

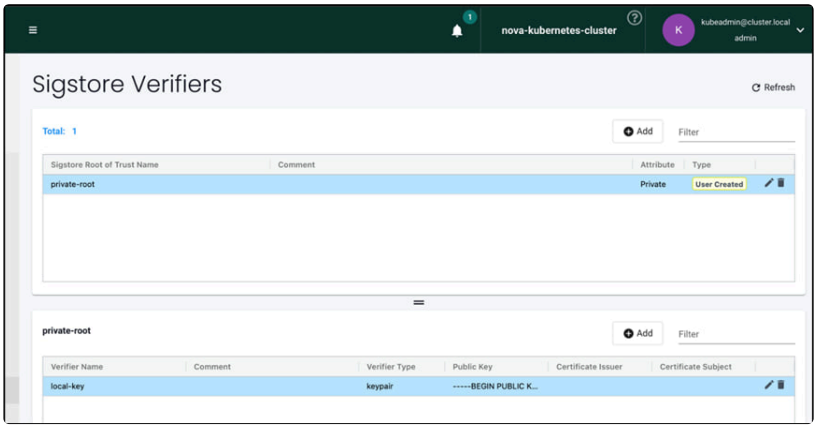
```
git clone https://github.com/sigstore/fulcio.git
cd fulcio
git checkout tags/v1.6.6
docker compose -f docker-compose.yml up -d
```

7. Получить корневой сертификат Fulcio, выполнив команду:

```
$ curl -X GET http://localhost:5555/api/v1/rootCert

-----BEGIN CERTIFICATE-----
MIICFjC…==
-----END CERTIFICATE-----
```

8. Выполнить дополнительную настройку системы Neuvector:
    - В разделе **Sigstore Verifiers** добавить новый доверенный источник:
        - Указать имя, например, **private-root**;
        - Указать атрибут **Private**;
        - Указать публичный ключ сервера Rekor в качестве **Rekor Public Key**;
        - Указать корневой сертификат Fulcio в качестве **Root Certificate**;
        - Добавить публичный ключ ранее сгенерированной ключевой пары.



- Используя закрытую часть ранее сгенерированной ключевой пары выполнить подпись образа контейнера с использованием утилиты Cosign с помощью команды ниже:

```bash
$ cosign sign \
   --key cosign.key \
   --fulcio-url=http://<fulcio-server-ip-address>:5555 \
   --rekor-url=http://<rekor-server-ip-address>:3000 \
   <image:tag>
```

- Выполнить повторное сканирование образов контейнеров и проверить результаты определения цифровой подписи.

Информирование администраторов ИС и администратора безопасности Платформы о нарушении целостности образов контейнеров выполняется, когда фиксируются попытки запуска контейнеров, не прошедших проверку цифровой подписи. Для просмотра событий безопасности необходимо выполнить следующие действия:

1. Открыть в браузере веб-интерфейс системы безопасности Neuvector.
2. Перейти в раздел **Notifications**, далее в раздел **Risk Report**s. События с типом **Admission.Control.Denied** и местом возникновения (**Location**) **Image** содержат подробную информацию о нарушении политики безопасности, включая уникальный идентификатор пользователя.

Для настройки контроля целостности сведений о событиях безопасности необходимо выбрать целевую систему для хранения событий безопасности, поступающих из платформы Kubernetes в виде журналов аудита, а также из системы безопасности Neuvector.

События безопасности в системе Neuvector могут быть направлены во внешний SYSLOG-сервер для дальнейшего контроля и анализа, а также в систему хранения журналов событий (логов) Opensearch (модуль платформы).

Целостность сведений о событиях безопасности в Opensearch контролируется с помощью настройки незименяемости индексов, что гарантирует повышенную безопасность и защиту данных, исключает возможность их случайного или преднамеренного изменения.

Для настройки проверки целостности сведений о событиях безопасности в Opensearch необходимо установить и настроить модуль Opensearch согласно процедурам, описанным в статье, а также выполнить следующие шаги:

- Ознакомиться с системными требованиями к модулю Opensearch и спланировать установки согласно руководству Планирование установки и системные требования
- Выполнить установку модуля Opensearch по инструкции Установка модуля OpenSearch
- Выполнить настройку неизменяемости индексов данных в Opensearch согласно руководству Запрет на удаление индексов

> Администратор безопасности должен проверять журналы систем NeuVector и Opensearch на предмет наличия отображения события попытки запуска неподписанного контейнера и определять причины возникновения ситуации.

3. Рекомендуется к ознакомлению

- Настройка регистрации событий безопасности и управления доступом