Платформа анализа информации об угрозах R-Vision TIP. Руководство по эксплуатации.

Версия 1.17

ОГЛАВЛЕНИЕ

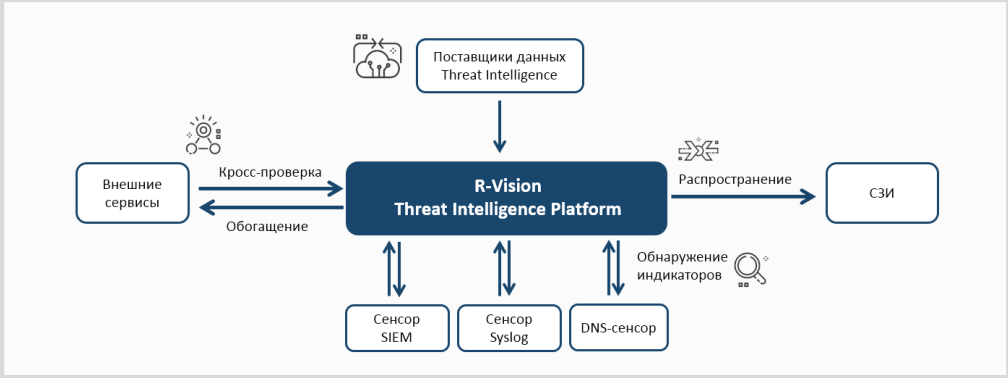
Пользовательская документация по продукту "Платформа анализа информации об угрозах R-Vision TIP" (далее - R-Vision Threat Intelligence Platform, TIP) содержит рекомендации по работе с продуктом.

1. О ПРОДУКТЕ

Платформа анализа информации об угрозах R-Vision TIP собирает, обрабатывает и обогащает индикаторы компрометации, получаемые из фидов Threat Intelligence.

Threat Intelligence Platform:

- Получает индикаторы компрометации от поставщиков данных для анализа угроз IBM X-Force Exchange и AlienVault Open Threat Exchange, с Threat Intelligence фидами компаний Group-IB и Лаборатория Касперского.
- Проверяет данные по отдельным индикаторам во внешних источниках. Обработанные данные напрямую передаются на внутренние средства защиты, тем самым снижая количество ложных срабатываний, которые возникают при использовании сырых данных, полученных из фидов.



Преимущества использования платформы:

- Упрощает работу с данными TI, непрерывно получая, обрабатывая и сохраняя данные из различных источников в единой базе.
- Облегчает выявление скрытых угроз, обеспечивая автоматический мониторинг индикаторов в SIEM.
- Ускоряет процессы ИБ за счет быстрого поиска информации в доступных источниках и автоматизации ключевых сценариев.
- Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб, благодаря автоматической выгрузке обработанных данных напрямую на СЗИ

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Полный перечень технических требований см. в документе «Руководство по администрированию R-Vision TIP».

Платформа работает в следующих веб-браузерах:

Название	Версия
Google Chrome	50 и выше
Mozilla Firefox	50 и выше

Для работы платформы требуется доступ к сети Интернет (напрямую или через прокси - сервер) и к DNS-серверу (внешнему или внутреннему).

3. АВТОРИЗАЦИЯ И ВХОД

После перехода по ссылке на интерфейс в окне браузера отобразится окно авторизации. Для выполнения авторизации и входа в систему укажите логин и пароль учетной записи пользователя и нажмите на кнопку **Войти**.

Если вход в систему выполнен успешно, то в окне браузера отобразится стартовый раздел системы.

Настройки входа описаны в документе «Руководство по администрированию R-Vision TIP».

4. ВЫХОД ИЗ СИСТЕМЫ

Чтобы выйти из системы:

1. Откройте меню, щелкнув на учетной записи в главном меню платформы.
2. Выберите опцию **Выход**.

5. УВЕДОМЛЕНИЯ О СОБЫТИЯХ СИСТЕМЫ

Раздел **Уведомления** содержит уведомления о событиях, произошедших в системе. Этот раздел могут просматривать все пользователи.

Чтобы просмотреть уведомления, перейдите в раздел **Уведомления**. Список уведомлений в разделе можно сортировать и фильтровать.

В карточке уведомлении отображается информация о событии.

Подробное описание настройки уведомлений см. в документе «Руководство по администрированию R-Vision TIP».

6. НАСТРОЙКА ПЛАТФОРМЫ

Подробное описание настройки платформы см. в документе «Руководство по администрированию R-Vision TIP».

6.1. Лицензирование

Лицензия предоставляет доступ к функциям Threat Intelligence Platform и ограничивает время использования.

После истечения срока лицензии возможности сбора данных становятся недоступны.

Лицензия выдается на идентификатор, созданный при установке Threat Intelligence Platform. Только одна лицензия может быть активна в системе. Лицензия действительна до указанной в ее свойствах даты.

Подробное описание установки лицензии см. в документе «Руководство по администрированию R-Vision TIP».

6.2. Работа с журналом системы

В журнале хранится информация о действиях пользователей в системе.

Система присваивает событиям уровни критичности:

1. Информационные — сведения информационного характера. Не требуют немедленной реакции.
2. Важные — события, на которые нужно обратить внимание. Эти события могут потребовать реакцию.
3. Опасные — потенциально опасные события. Эти события требуют реакции.