

R-Vision

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

Версия 1.17

ОГЛАВЛЕНИЕ

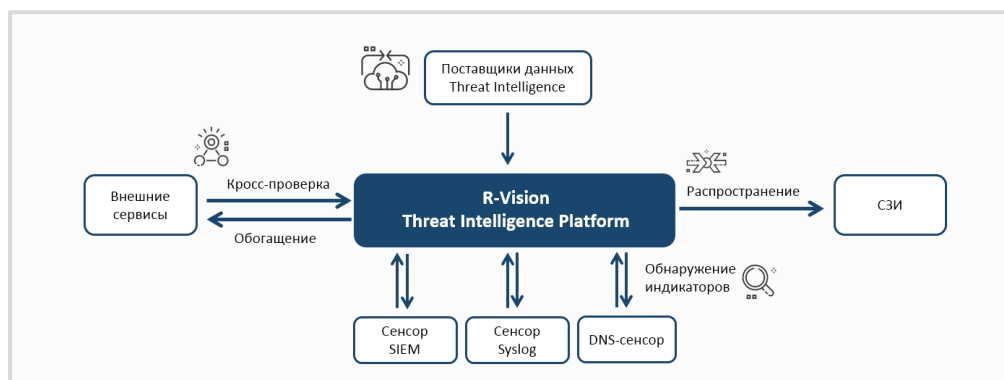
1. О продукте.....	3
2. Установка платформы	4

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. УСТАНОВКА ПЛАТФОРМЫ

Чтобы установить платформу из образа ISO:

1. Скачайте образ системы по ссылке. Для получения ссылки обратитесь в компанию R-Vision по адресу sales@rvision.pro.
2. Установите для виртуальной машины ISO-образ системы R-Vision в качестве установочного диска.
3. Запустите виртуальную машину. Операционная система CentOS 7 будет установлена и настроена автоматически. Установка операционной системы займет некоторое время. После установки, инсталлятор автоматически отключит виртуальную машину.
4. Демонтируйте образ, из которого выполнялась установка.
5. Повторно запустите виртуальную машину.
6. Следуйте шагам, описанным в документе «Руководство по администрированию R-Vision TIP».
7. Запустите систему. Веб-интерфейс продукта доступен по адресу <http://<ip-address>> или <https://<dns-name>>, если есть внутреннее доменное имя.