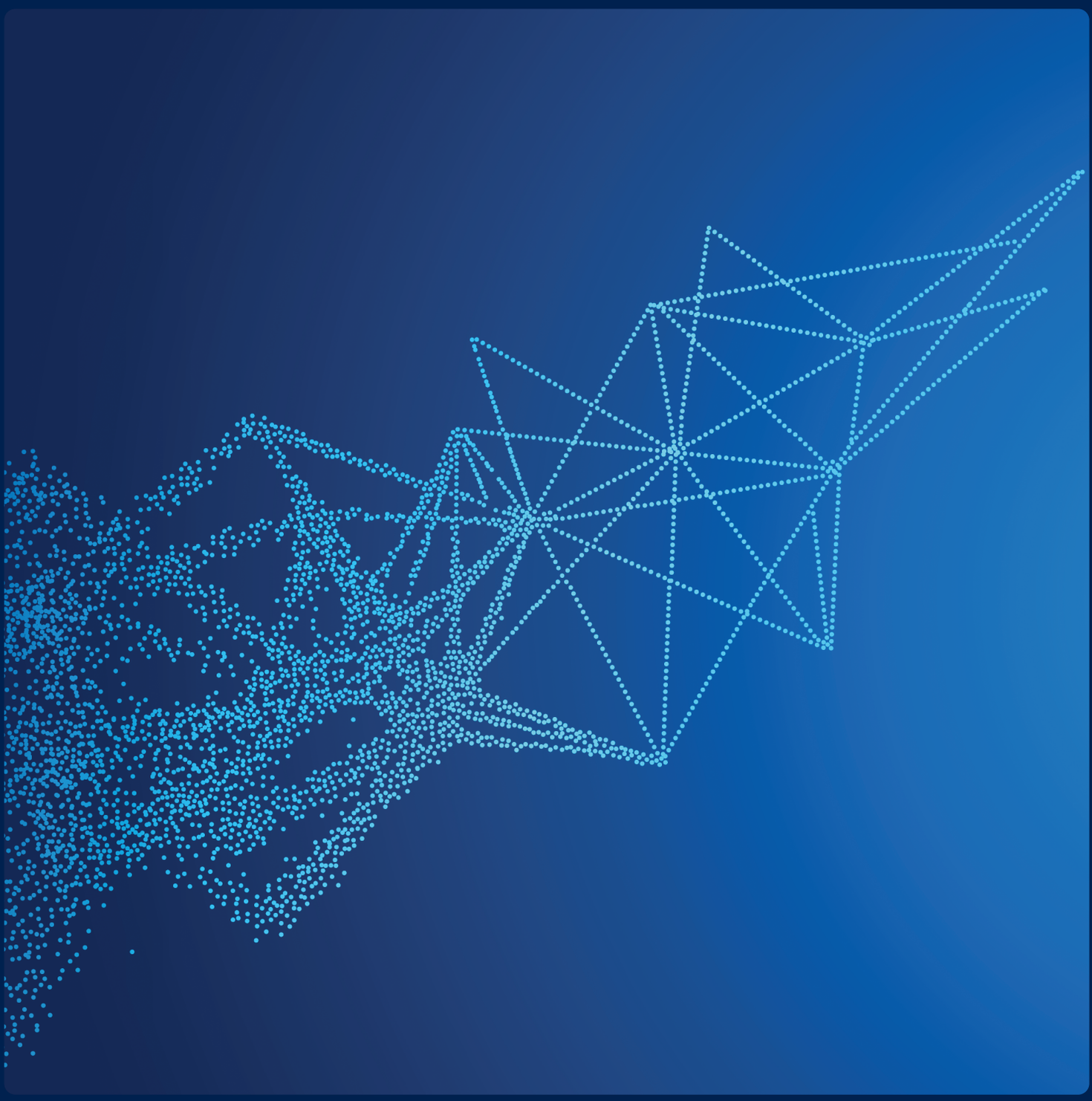
R-Vision TIP

Автоматизация управления данными
о киберугрозах

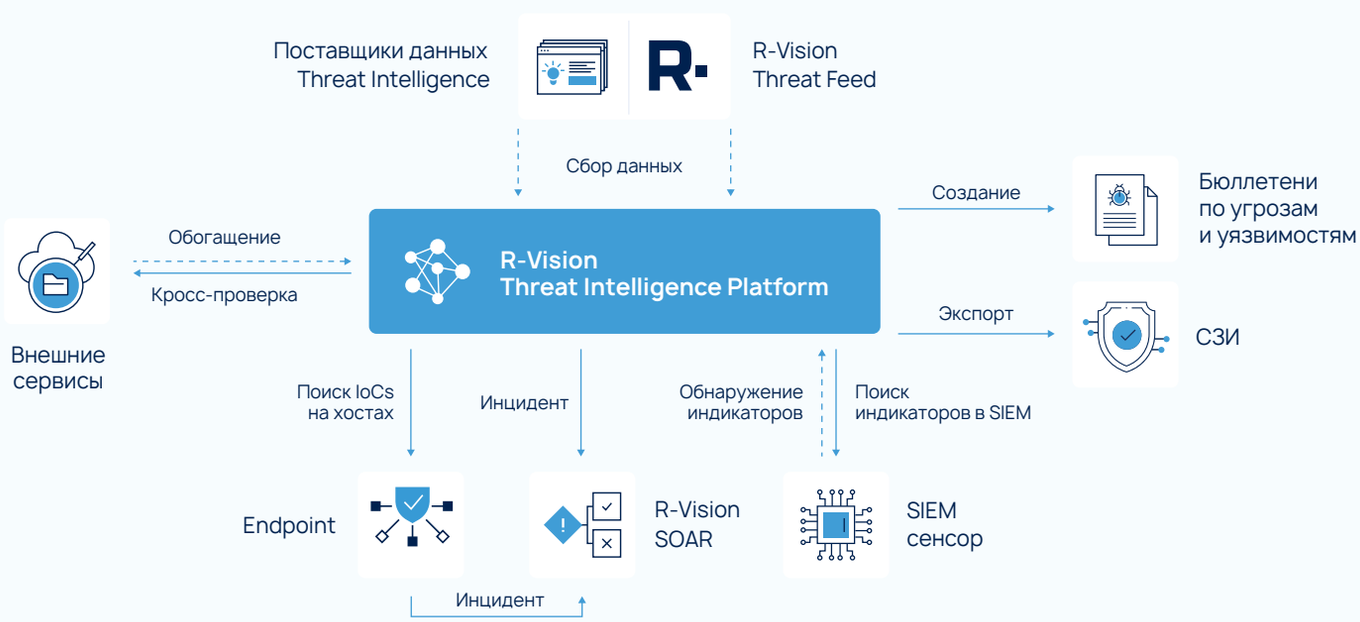


R-Vision Threat Intelligence Platform

R-Vision TIP (Threat Intelligence Platform) – платформа автоматизации управления данными о киберугрозах, которая объединяет коммерческие и некоммерческие источники. Она позволяет агрегировать данные из различных источников, экспортировать индикаторы компрометации для блокировки и мониторинга в системах защиты, а также искать следы компрометации в инфраструктуре. Платформа обеспечивает возможности работы с тактическим, операционным и стратегическим TI.

Задачи	Решения
Агрегировать данные Threat Intelligence из разных источников	Интеграция с ключевыми коммерческими и open-source площадками обмена данными об угрозах обеспечивает автоматический сбор, нормализацию, обогащение и хранение данных киберразведки в единой базе
Автоматизировать рутинные процессы работы с данными TI	Разработанный механизм правил помогает формировать выборки индикаторов, автоматически обнаруживаемых в потоке данных из SIEM, обогащать их и экспортировать на СЗИ для блокировки и в R-Vision SOAR для реагирования
Снизить нагрузку на SIEM-систему	Встроенные сенсоры позволяют получать данные из различных SIEM-систем и осуществлять автоматический реактивный и ретроспективный поиск релевантных индикаторов в инфраструктуре

Интеграция с другими продуктами R-Vision позволяет обогатить данными киберразведки такие процессы информационной безопасности, как управление уязвимостями, оценка рисков ИБ, управление событиями и инцидентами ИБ.



Сбор данных Threat Intelligence

R-Vision Threat Intelligence Platform **автоматически агрегирует данные об угрозах** из различных источников и **интегрируется с площадками обмена данными** и сервисами:

- Открытые источники (более 15)
- R-Vision Threat Feed
- F6 Threat Intelligence
- Гарда Threat Intelligence
- Kaspersky Threat Data Feeds
- CTT Threat Feed
- BI.ZONE Threat Intelligence
- АСОИ ФинЦЕРТ
- ФинЦЕРТ Антифрод
- MITRE ATT&CK®
- Возможно подключение других источников

Обработка и обогащение

В процессе обработки **индикаторы нормализуются и приводятся к единой модели представления, дублирующиеся индикаторы связываются и объединяются**. Каждому индикатору присваивается рейтинг и устанавливаются политики устаревания. R-Vision TIP обогащает индикаторы дополнительным контекстом, которого нет в исходных данных, поддерживая более 20 сервисов:

- VirusTotal
- Whois
- RiskIQ
- Ipgeolocation.io
- OPSWAT Metadefender
- MaxMind
- Shodan
- Другие

Анализ взаимосвязей

Анализ взаимосвязей помогает ИБ-специалисту правильно интерпретировать данные и сформировать **целостную картину угрозы**. R-Vision TIP собирает информацию об индикаторе и связанных с ним: ВПО, отчёты, уязвимости, субъекты угроз, техники, тактики и другой контекст из MITRE ATT&CK.

Экспорт на СЗИ

Предварительная обработка снижает количество ложных срабатываний, возникающих при использовании сырых данных. Обработанные данные **автоматически передаются** на внутренние средства защиты и могут обмениваться в форматах STIX 2.1, CSV, JSON:

- UserGate
- Cisco
- Palo Alto Networks
- Check Point
- McAfee
- Ideco UTM
- Другие СЗИ

Поиск и обнаружение в ИТ-инфраструктуре

R-Vision TIP обеспечивает ретроспективный и проактивный **поиск релевантных индикаторов в событиях SIEM** с помощью сенсоров и рассылает оповещения в случае обнаружения.

Автоматизация сценариев

Платформа позволяет **автоматизировать повторяющиеся операции** с индикаторами компрометации. Задав последовательность правил обработки, можно полностью автоматизировать сценарии работы с данными: от их получения до блокировки на СЗИ.

Формирование бюллетеней

Удобный конструктор бюллетеней позволяет создавать **материалы по угрозам и уязвимостям**, рассылать их дочерним организациям и экспортировать во внешние системы через API.

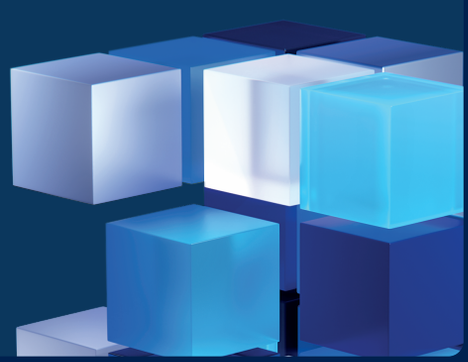
R-Vision

R-Vision - разработчик систем цифровизации и кибербезопасности. С 2011 года компания создаёт технологии, которые помогают организациям эффективно противостоять киберугрозам, поддерживать надёжность ИТ-инфраструктуры и обеспечивать цифровую трансформацию. Технологии R-Vision используются в крупнейших банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

R-Vision TIP зарегистрирован в Реестре отечественного ПО и сертифицирован ФСТЭК России по 4 уровню доверия.

Единая платформа R-Vision EVO

Продукты R-Vision разработаны на основе единой платформы. Общая технологическая база обеспечивает бесшовную интеграцию ИБ и ИТ-продуктов, позволяя выстраивать процессы, при которых автоматизация бизнеса и кибербезопасность работают как единое целое.



rvision.ru
sales@rvision.ru
+7 (499) 322 80 40
t.me/rvision_pro
vk.ru/rvision_ru
youtube.com/@rvision_ru

rvision.ru