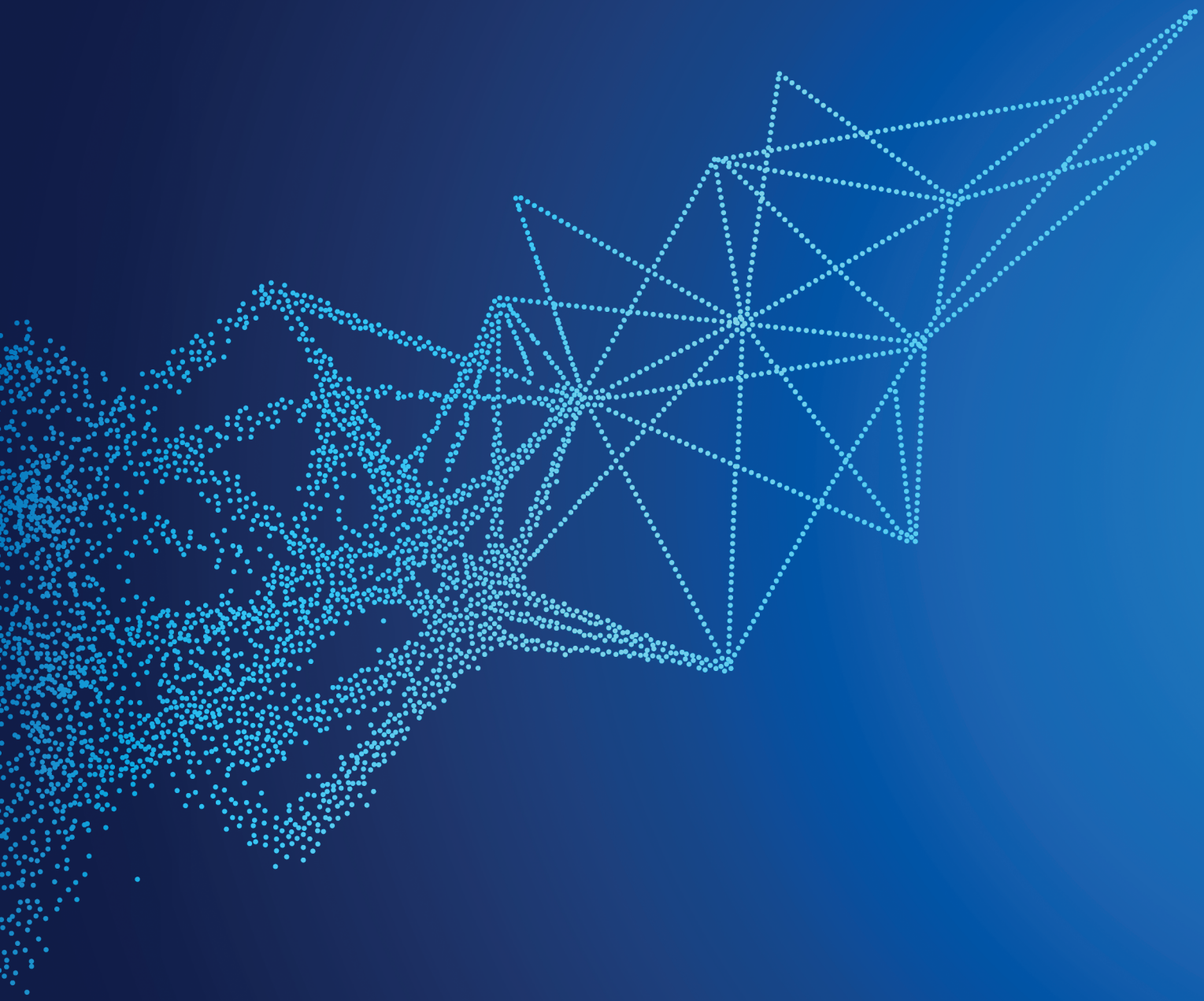
R-Vision Threat Intelligence Platform

Платформа анализа информации об угрозах



R-Vision

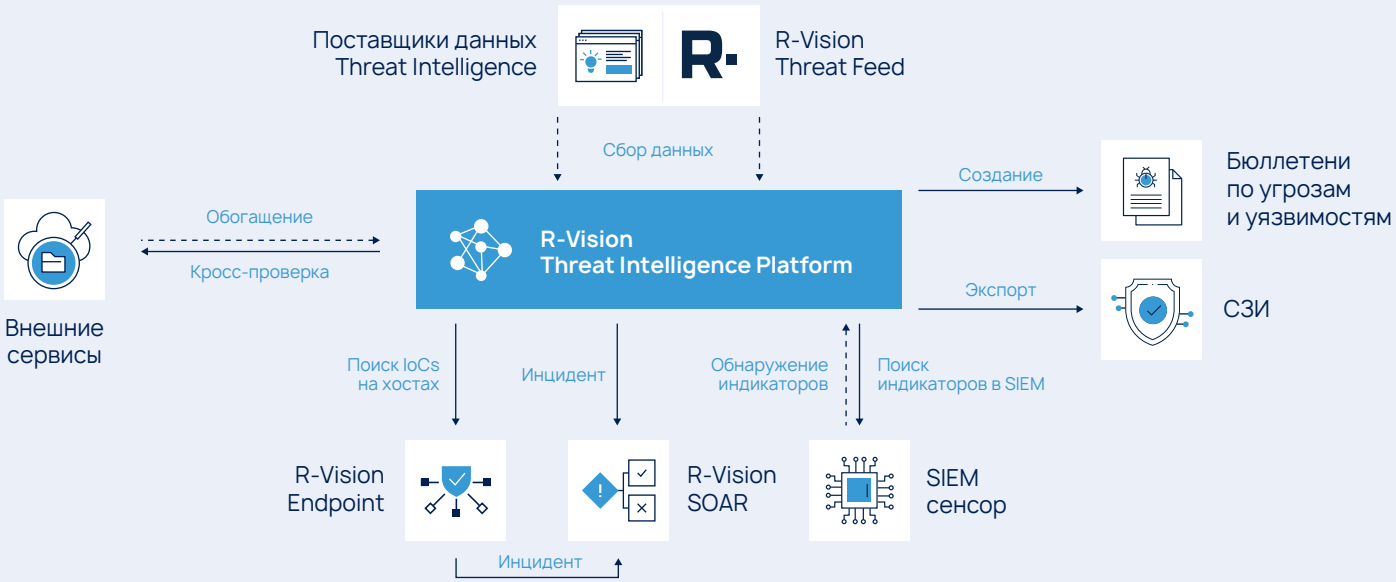
R-Vision Threat Intelligence Platform (TIP) – платформа анализа информации об угрозах. Обеспечивает сбор данных Threat Intelligence (TI) в автоматическом режиме, поиск и обнаружение индикаторов в инфраструктуре организации, а также передачу обработанных данных напрямую на внутренние средства защиты.

Задачи	Решение
Агрегировать данные Threat Intelligence из разных источников	Встроенная интеграция с ключевыми коммерческими и open-source-площадками обмена данными об угрозах обеспечивает автоматический сбор, нормализацию, обогащение и хранение данных киберразведки из различных источников в единой базе
Автоматизировать рутинные процессы работы с данными TI	Разработанный механизм правил помогает сформировать выборки индикаторов, которые автоматически обнаруживаются в потоке данных из SIEM, обогащаются, экспортируются 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 другими продуктами R-Vision позволяет обогатить данными киберразведки такие процессы информационной безопасности, как управление уязвимостями, оценка рисков ИБ, управление событиями и инцидентами ИБ.

При совместном использовании с R-Vision Endpoint позволяет:

- ✓ Осуществлять поиск индикаторов компрометации на конечных устройствах
- ✓ Обогащать найденные индикаторы дополнительным контекстом из R-Vision TIP
- ✓ Передавать инциденты для дальнейшего расследования и реагирования в R-Vision SOAR



Сбор данных Threat Intelligence

R-Vision Threat Intelligence Platform **агрегирует данные об угрозах** из различных источников в автоматическом режиме. Система **обладает встроенной интеграцией** с площадками обмена данными об угрозах 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 компрометации присваивается рейтинг и определяются политики устаревания** индикаторов. R-Vision TIP позволяет обогащать индикаторы компрометации дополнительным контекстом, который отсутствует в исходных данных от поставщика. Поддерживается > 20 сервисов обогащения:

- 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 имеющуюся у поставщика информацию об индикаторе и связанные с ним:

- ВПО
- Отчеты
- Уязвимости
- Субъекты угроз
- Техники, тактики и другой контекст из MITRE ATT&CK®

Экспорт на СЗИ

Предварительная обработка помогает снизить количество ложных срабатываний, которые часто возникают при использовании сырых данных. Обработанные **данные автоматически передаются** на имеющиеся внутренние средства защиты информации:

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

Дополнительно есть возможность обмена данными с помощью распространенных форматов: STIX 2.1, CSV, JSON.

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 **настроить выполнение регулярно повторяющихся операций** с индикаторами компрометации в автоматическом режиме. Задав последовательность правил обработки, можно полностью автоматизировать определенный сценарий работы с набором данных: от их получения до блокировки средствами защиты.

Формирование бюллетеней

Удобный конструктор бюллетеней помогает сформировать **информационные материалы по угрозам и уязвимостям**, разослать бюллетени по дочерним организациям, а также экспортировать на внешние системы с помощью API.

R-Vision

О компании

R-Vision – российский разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают организациям эффективно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии R-Vision применяются в государственных учреждениях, финансовой сфере, телекоммуникациях, а также в нефтегазовой, энергетической и металлургической отраслях промышленности в России и странах СНГ.

Система R-Vision TIP зарегистрирована в Реестре отечественного ПО и сертифицирована ФСТЭК России по 4 уровню доверия.

rvision.ru

sales@rvision.ru

+7 (499) 322 80 40

t.me/rvision_pro

vk.ru/rvision_ru

youtube.com/@rvision_ru