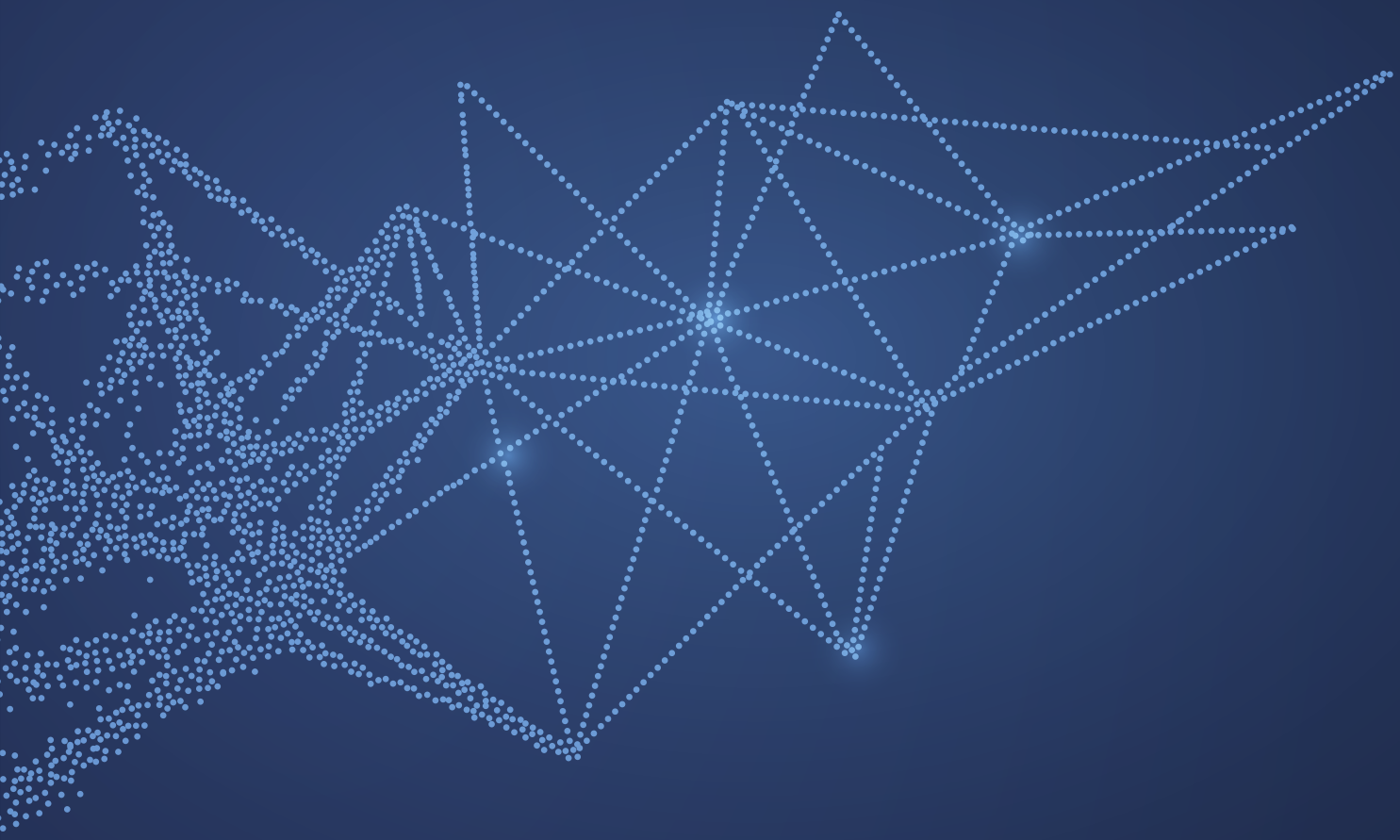
R-Vision Threat Intelligence Platform

Платформа анализа информации об угрозах



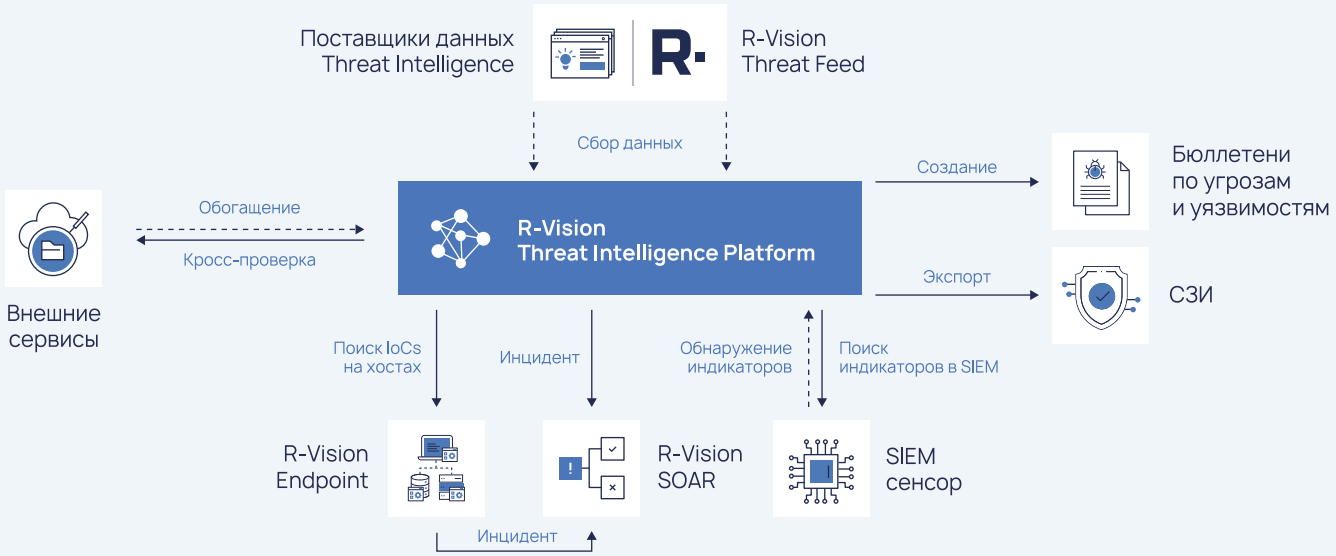
R·Vision

R-Vision Threat Intelligence Platform (TIP) представляет собой специализированную платформу анализа информации об угрозах. Продукт обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре организации.

Задачи	Решение
Автоматизировать получение данных киберразведки из различных источников в единой базе	R-Vision TIP обеспечивает автоматический сбор, нормализацию, обогащение и хранение данных TI из различных источников благодаря встроенной интеграции с ключевыми коммерческими и опен-сорсными площадками обмена данными об угро-зах и сервисами
Автоматизировать рутинные процессы работы с данными TI	Платформа автоматизирует ключевые рабочие сценарии при помощи правил: обогащение IoCs дополнительным контекстом, мониторинг в событиях SIEM, экспорт на СЗИ для блокировки, оповещения об обнаружениях по e-mail, отправка инцидентов в R-Vision SOAR для реагирования
Снизить нагрузку на SIEM-систему	Функционал сенсоров платформы R-Vision TIP позволяет получать данные из различных SIEM-систем и осуществлять автоматический реактивный и ретроспективный поиск релевант-ных индикаторов в инфраструктуре, снижая нагрузку на SIEM

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:

- R-Vision Threat Feed
- AT&T Cybersecurity
- Group-IB Threat Intelligence
- Kaspersky Threat Intelligence
- PT Threat Intelligence Feeds
- RST Threat Feed
- BI.ZONE ThreatVision
- АСОИ ФинЦЕРТ
- MITRE ATT&CK®
- Открытые источники
- 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
- pgeolocation.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 – разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают бизнесу и государственным организациям по всему миру уверенно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии **R-Vision** используются в банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

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

/rvision_ru

/RVisionPro

Дайджест информационной безопасности: **rvision.ru/blog**