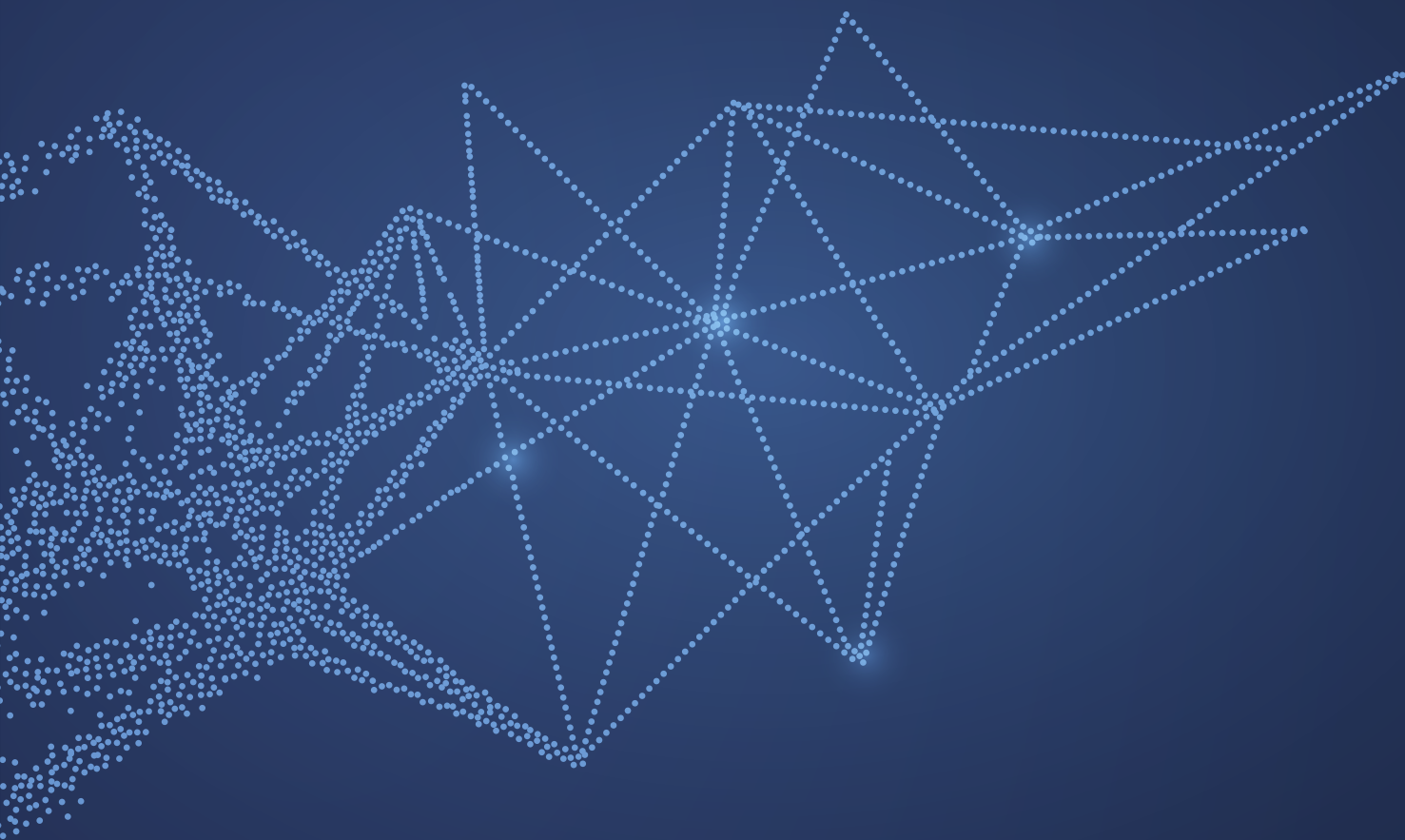


R-Vision Threat Intelligence Platform

Платформа анализа
информации об угрозах



R-Vision

R-Vision Threat Intelligence Platform 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 с помощью сенсоров.



Преимущества системы

- Упрощает работу с данными TI, осуществляя непрерывный сбор, нормализацию, обогащение и хранение данных из различных источников в единой базе.
- Облегчает выявление скрытых угроз, обеспечивая автоматический мониторинг релевантных индикаторов в SIEM с помощью сенсоров.
- Ускоряет расследование за счет быстрого поиска информации в доступных источниках и автоматизации ключевых рабочих процессов.
- Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб, благодаря автоматической выгрузке обработанных данных напрямую на СЗИ.
- Снижает количество ложных срабатываний за счет ранжирования индикаторов компрометации посредством скоринговой модели.
- Оперативно собирает индикаторы компрометации при территориально-распределенной инфраструктуре за счет установки сенсоров интеграции с SIEM-системами ближе к потокам данных.

Сводка

Источник

TI Phishing URL Data Feed

Статус

Активный ✓

Значение

106.12.178.83

Тип

Ip

Вид сущности

Индикатор компрометации

Получен

16:04:45 28 апреля 2022

Изменён

16:49:19 28 апреля 2022

40

средний

Взаимосвязи

Вид сущности	Имя	Источник	Тип
Объект наблюдения	bgznagh.cn	TI Phishing URL Data Feed	domain
Объект наблюдения	dckpehn.cn	TI Phishing URL Data Feed	domain

В карточке индикатора сохраняется вся доступная информация:

- ✓ исходные данные, предоставляемые поставщиком TI
- ✓ сведения, полученные в результате обогащения
- ✓ отчёты, вредоносное ПО, уязвимости, другие связанные индикаторы
- ✓ история обнаружений и обновлений

Основные функциональные возможности



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:

- IBM X-Force Exchange
- AT&T Alien Labs Open Threat Exchange (OTX)
- Group-IB Threat Intelligence
- Kaspersky Threat Intelligence
- RST Threat Feed
- ESET Threat Intelligence
- Shadowserver
- АСОИ ФинЦЕПТ
- 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. Поддерживаемые сервисы обогащения:

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



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:

- Вредоносное ПО
- Отчеты
- Уязвимости
- Иной контекст



Распространение на средства защиты

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

- Cisco
- Check Point
- UserGate
- Palo Alto Networks
- McAfee
- 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 информационных бюллетеней

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



О компании

Компания R-Vision – разработчик систем кибербезопасности. С 2011 года создает продукты и сервисы, 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.

 www.rvision.ru

 sales@rvision.ru

 +7 (499) 322 80 40

Дайджест информационной безопасности:
rvision.ru/blog

 t.me/rvision_pro

 [/rvision_ru](https://vk.com/rvision_ru)

 [/RvisionPro](https://www.youtube.com/RvisionPro)