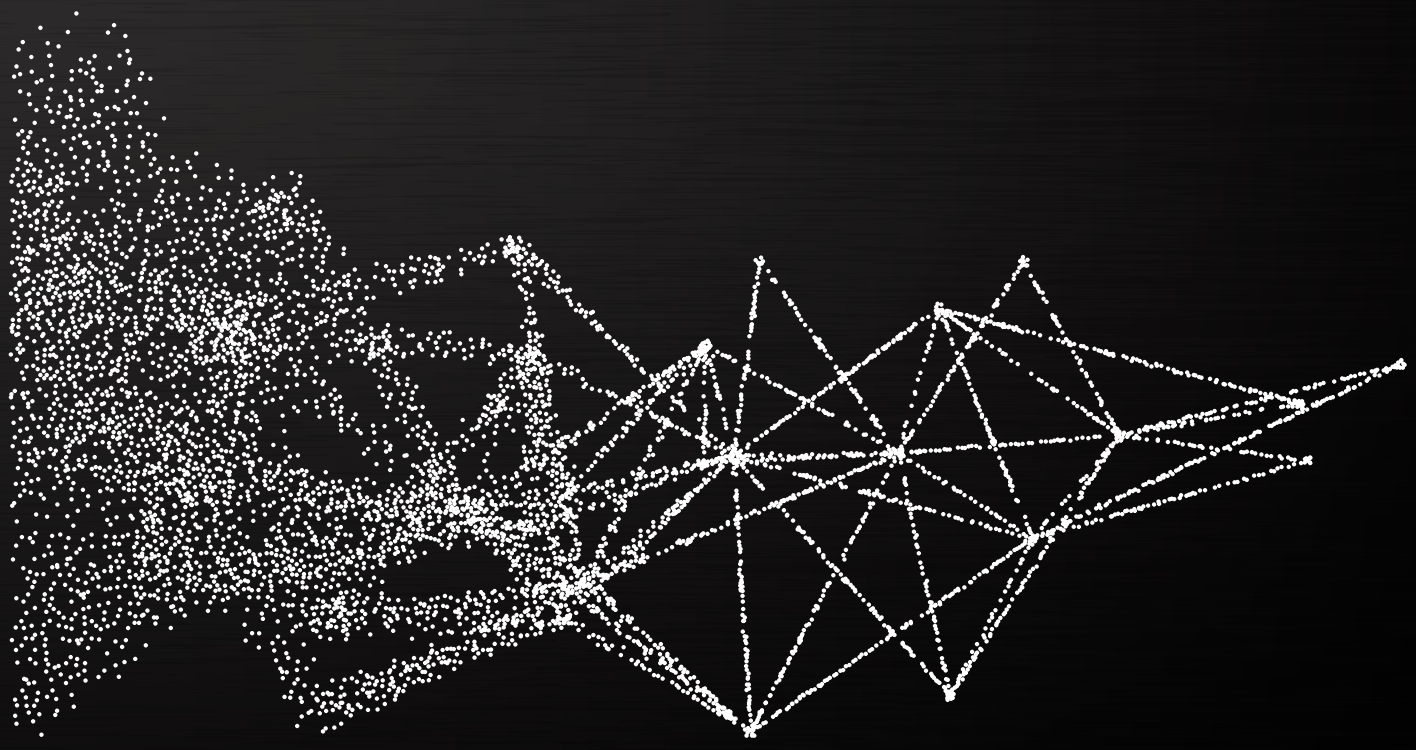
R-Vision

At the root of your security

Threat Intelligence Platform

Платформа управления данными киберразведки



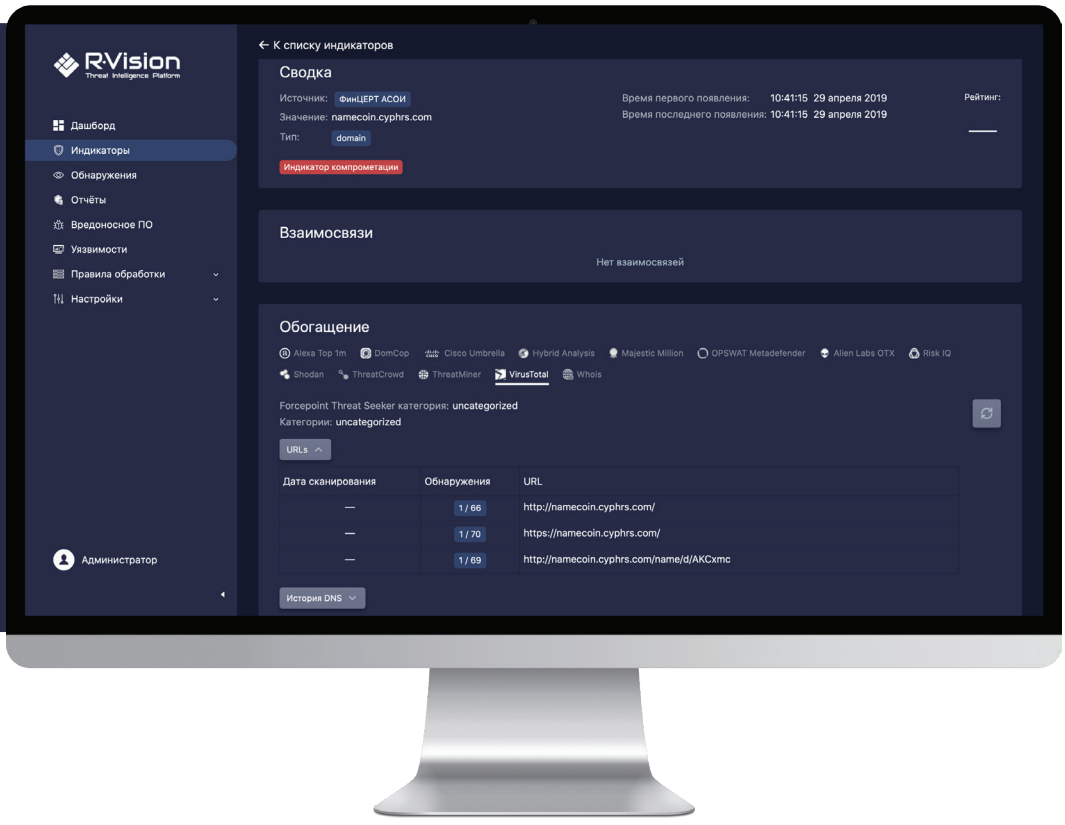
R-Vision Threat Intelligence Platform представляет собой специализированную платформу управления данными киберразведки. Продукт обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре организации с помощью сенсоров.

ПРЕИМУЩЕСТВА:

- **Упрощает работу с данными TI,** осуществляя непрерывный сбор, нормализацию 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 сценариев.
- **Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб,** благодаря автоматической выгрузке обработанных данных напрямую на СЗИ.

В карточке индикатора сохраняется вся доступная информация:

- исходные данные, предоставляемые поставщиком
- сведения, полученные в результате обогащения
- отчёты, вредоносное ПО и уязвимости, связанные с индикатором
- история обнаружений и обновлений



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
- Group-IB Threat Intelligence
- Kaspersky Threat Intelligence
- Финцерт
- Возможно подключение других

ОБРАБОТКА ДАННЫХ КИБЕРРАЗВЕДКИ

В процессе обработки индикаторы нормализуются и приводятся к единой модели представления, дублирующиеся индикаторы связываются и объединяются.

АНАЛИЗ ВЗАИМОСВЯЗЕЙ

Анализ взаимосвязей помогает аналитику правильно интерпретировать данные и сформировать целостную картину угрозы. R-Vision TIP собирает имеющуюся у поставщика информацию о связях индикаторов с другими индикаторами, а так же связанные:

- Отчеты
- Вредоносное ПО
- Уязвимости

ОБОГАЩЕНИЕ ИНДИКАТОРОВ

R-Vision Threat Intelligence Platform позволяет обогащать индикаторы компрометации дополнительным контекстом, который отсутствует в исходных данных от поставщика. Более актуальные и полные сведения помогают аналитику в принятии решений о дальнейших действиях с индикаторами.

Поддерживаемые сервисы обогащения:

- VirusTotal
- Hybrid Analysis
- OPSWAT Metadefender
- Shodan
- RiskIQ
- MaxMind
- Sypex
- Ipgeolocation.io
- Whois

РАСПРОСТРАНЕНИЕ НА СРЕДСТВА ЗАЩИТЫ

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

Автоматическая выгрузка индикаторов на оборудование:

- Cisco
- PaloAlto Networks
- Check Point
- и другие средства защиты

ПОИСК И ОБНАРУЖЕНИЕ В 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 R-Vision Threat Intelligence Platform позволяет настроить выполнение регулярно повторяющихся операций с индикаторами компрометации в автоматическом режиме. Задав последовательность правил обработки (обогащения, обнаружения, распространения и оповещения), можно полностью автоматизировать определенный сценарий работы с набором данных, от их получения до блокировки средствами защиты.

R-Vision
At the root of your security

О компании R-Vision

Компания R-Vision – российский разработчик решений в области информационной безопасности. R-Vision с 2011 года разрабатывает продукты, предназначенные для автоматизации процессов управления информационной безопасностью, мониторинга и реагирования на инциденты и использования данных киберразведки.

Решения R-Vision используются в банках, государственных структурах, нефтегазовой отрасли, энергетике, промышленности, металлургии и других отраслях.

www.rvision.pro

sales@rvision.pro

8 (499) 322 80 40
8 (800) 350 77 57

Дайджест информационной безопасности: rvision.pro/blog

t.me/rvision_pro

/rvision.pro