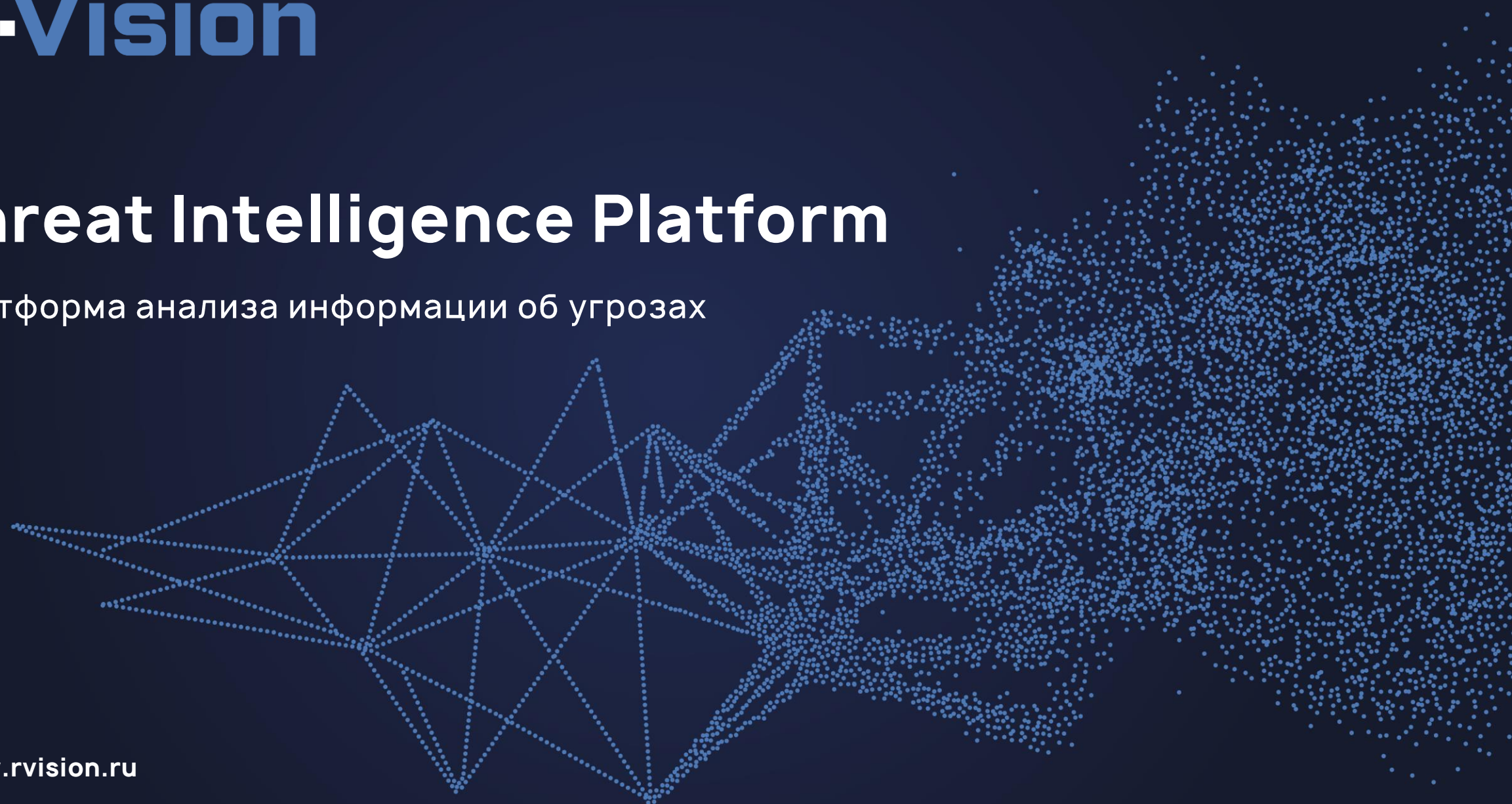


R-Vision

Threat Intelligence Platform

Платформа анализа информации об угрозах

www.rvision.ru



Что такое Threat Intelligence?

Threat intelligence – это знания об угрозах, полученные в результате анализа и интерпретации данных



Операционный уровень

Индикаторы компрометации
(IP адреса, домены, хэши,
C&C адреса ботнетов и т.д.)



Выявление и блокировка
скрытых угроз, реагирование



Тактический уровень

Тактика, техники
и процедуры (TTPs)
злоумышленников



Прогнозирование атак,
защитные меры,
обнаружение



Стратегический уровень

Отчеты об угрозах



Принятие стратегических
решений в области ИБ

Использование Threat Intelligence

Кто: Люди



CISO



Риск-менеджер



Аналитик SOC



TI аналитик

Для чего: Процессы



Реагирование на инциденты



Управление уязвимостями



Мошенничество



Риски



Операционная безопасность



Метрики ИБ

Как: Технологии



Firewall



EDR



IPS



UEBA



Безопасность облаков



TI платформы

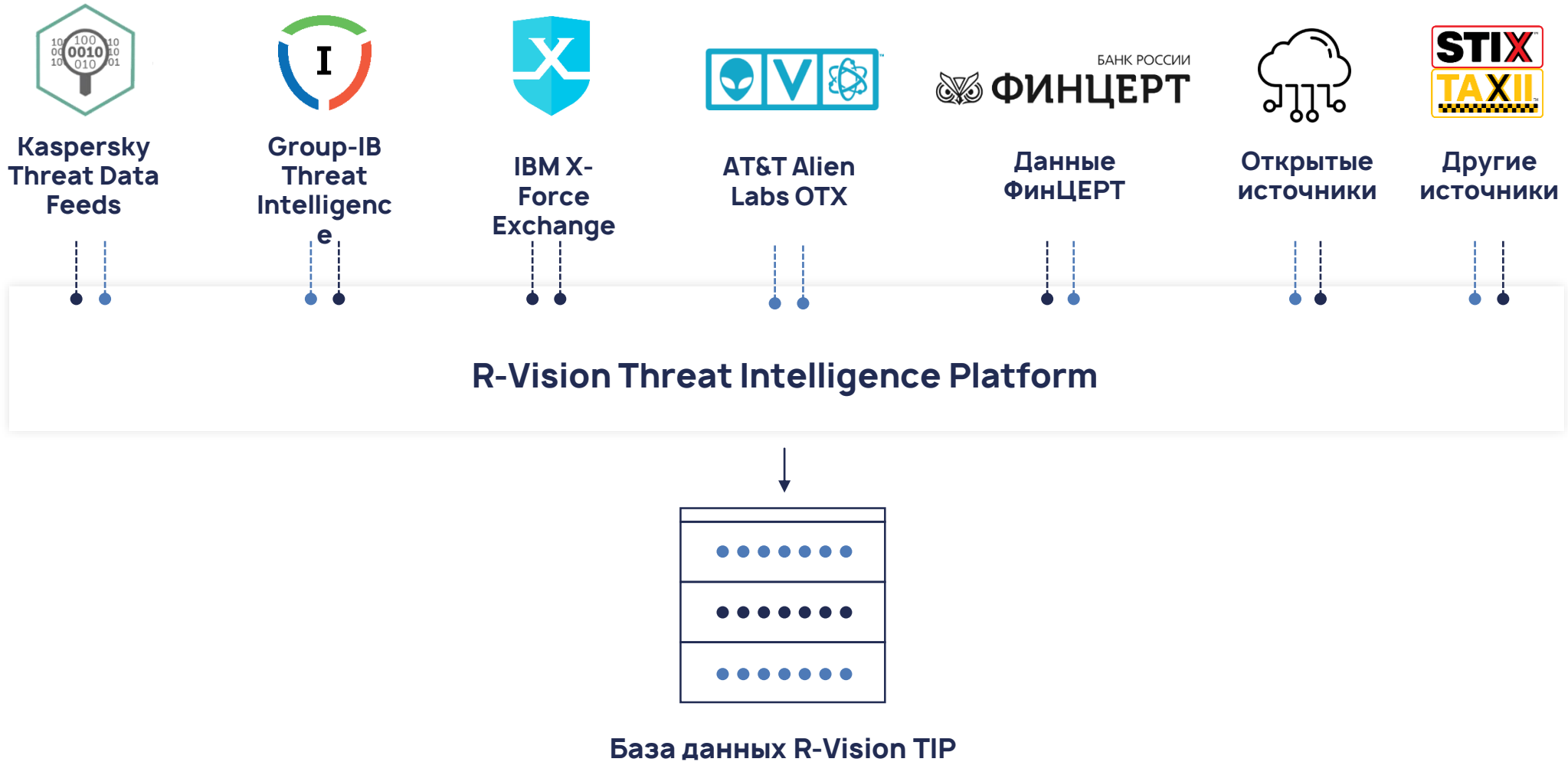
Схема работы R-Vision TIP



Возможности R-Vision TIP



Поставщики Threat Intelligence



Обработка и обогащение данных

Обработка = преобразование в пригодную для дальнейшего использования форму



Нормализация



Дедупликация



Приведение к единому структурированному формату

Обогащение контекстом с помощью внешних сервисов:

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

Анализ взаимосвязей

Формирование целостной картины угрозы для правильной интерпретации данных аналитиком.

Анализ связанных с индикатором данных:



Предусмотрено создание и изменение собственных индикаторов

Конструктор бюллетеней

Создание собственных информационных материалов для повышения осведомленности различных кругов заинтересованных лиц



Формирование бюллетеней двух типов: по угрозам и по уязвимостям



Автозаполнение данных



Добавление в бюллетень дополнительных свидетельств (изображения, аннотации)

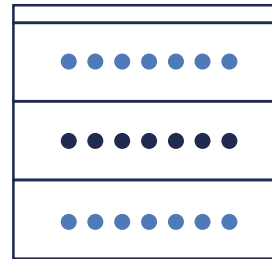


Рассылка бюллетеней по подведомственным структурам



Экспорт бюллетеней на внешние системы с помощью API

Интеграция с используемыми СЗИ



Автоматическая выгрузка индикаторов на СЗИ
для немедленной блокировки



Другие

Мониторинг индикаторов

Ретроспективный и реал-тайм поиск релевантных индикаторов в событиях SIEM



- — QRadar
- — ArcSight
- — MaxPatrol SIEM
- — Другие SIEM

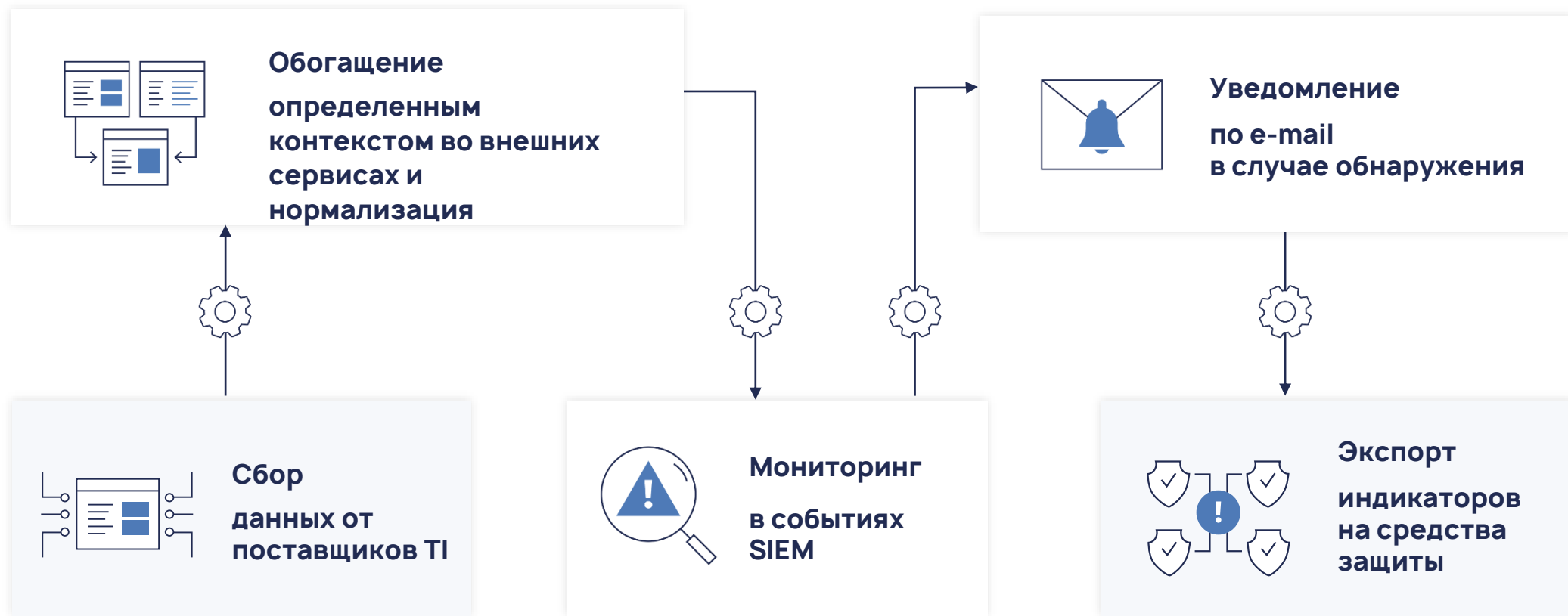
Распределенная инсталляция сенсоров SIEM



**Возможность
распределенной
установки сенсоров
интеграции с SIEM-
системами для сбора
индикаторов
компрометации
ближе к потокам
данных**

Автоматизация работы с индикаторами

Оперативное выполнение заданной цепочки действий



- Дашборд
- Индикаторы
- Обнаружения
- Отчёты
- Вредоносное ПО
- Уязвимости
- Автоматизация
- Настройки
 - Поставщики данных
 - Обнаружение
 - Обогащение
 - Интеграции
 - Оповещение
 - Экспорт
 - Система
 - Пользователи
 - Лицензия

admin

Поставщики данных

Фиды Внешние системы

AT&T Cybersecurity

Open Threat Exchange

Automatically created provider

5 / 31 активных каналов

IBM Security

X-Force Exchange

Automatically created provider

10 / 52 активных каналов

ФинЦЕРТ АСОИ

Банк России

Automatically created provider

1 / 1 активный канал

Group IB

Threat Exchange

Automatically created provider

2 / 6 активных канала

Канал	Статус	Последнее обновление	Рейтинг	Метод подсчёта рейтинга	Частота обновления
NVD Vulnerabilities	<input checked="" type="checkbox"/>	14:02:16 08.05.2020	—	Без рейтинга	2 часа
NVD CPE List	<input type="checkbox"/>	12:43:26 27.04.2020	—	Без рейтинга	2 часа
NVD CPE List	<input type="checkbox"/>	12:39:07 27.04.2020	—	Без рейтинга	2 часа

Open source fee...

Свободно распространяемые TI ф...

Automatically created provider

39 / 81 активных каналов

Kaspers...

Threat Intelligence Services

2 / 2 активных канала

NVD National Vulnerabilit...

NIST National Vulnerability Database

artur

1 / 3 активный канал

- Дашборд
- Индикаторы
- Обнаружения 14
- Отчёты
- Вредоносное ПО
- Уязвимости
- Бюллетени
- Автоматизация
 - Обогащение
 - Обнаружение
 - Экспорт
 - Интеграции
 - Оповещение
- Настройки

admin

Индикаторы

Поиск...

Источник	Значение	Тип	Страна	Вид сущности	Создан	Изменён
AT&T Cybersecurity	109.122.80.234	ip	SRB	Индикатор к...	13:44:13 08.05.2020	
AT&T Cybersecurity	166.148.65.54	ip	USA	Индикатор к...	13:44:13 08.05.2020	
AT&T Cybersecurity	103.57.80.55	ip	IND	Индикатор к...	13:44:13 08.05.2020	
AT&T Cybersecurity	95.0.183.16	ip	TUR	Индикатор к...	13:44:13 08.05.2020	
AT&T Cybersecurity	177.74.117.202	ip	BRA	Индикатор к...	13:44:13 08.05.2020	
AT&T Cybersecurity	177.73.250.160	ip	BRA	Индикатор к...	13:44:13 08.05.2020	
AT&T Cybersecurity	185.44.229.227	ip	ARM	Индикатор к...	13:44:13 08.05.2020	
2 источника	185.220.103.9	ip	DEU	Индикатор к...	13:35:42 08.05.2020	
AT&T Cybersecurity	212.73.73.234	ip	ARM	Индикатор к...	13:35:42 08.05.2020	
AT&T Cybersecurity	173.82.74.58	ip	USA	Индикатор к...	13:35:42 08.05.2020	
2 источника	198.251.80.214	ip	USA	Индикатор к...	13:35:42 08.05.2020	
2 источника	171.25.193.77	ip	SWE	Индикатор к...	13:35:42 08.05.2020	
AT&T Cybersecurity	163.172.120.141	ip	GBR	Индикатор к...	13:35:42 08.05.2020	
AT&T Cybersecurity	182.176.228.147	ip	PAK	Индикатор к...	13:35:42 08.05.2020	
2 источника	185.220.100.242	ip	DEU	Индикатор к...	13:35:42 08.05.2020	
2 источника	84.53.225.118	ip	RUS	Индикатор к...	13:35:42 08.05.2020	
Kirill test 1	170.80.22.12	ip	GTM	Индикатор к...	12:31:38 08.05.2020	

Показывать удаленные каналы и индикаторы

1 из 70 20

Настройки фильтра

Фильтры Колонки

Источник: AT&T Cybersecurity ✕

Тип: ip, domain, sha256, sha1 ✕

Рейтинг: От 0 до 100

Страна: Выбрать страны ▾

Теги: Выберите теги ▾

Вид сущности: Выбрать вид сущности ▾

Первое появление: Выбрать даты ▾

Последнее появление: Выбрать даты ▾

Получен: Выбрать даты ▾

Применить

← К списку индикаторов

Сводка

Источник: ФинЦЕРТ АСОИ botnet c&c

Значение: 193.109.69.5

Тип: ip

Создан: 12:46:54 21 мая 2019

Изменён: 12:46:54 21 мая 2019

Получен: 09:55:50 27 марта 2020

Обновлён: 11:40:51 27 марта 2020

Рейтинг:

Подробная информация

ФинЦЕРТ АСОИ botnet c&c

Индикатор компрометации

Тип: ip

Создан: 12:46:54 21 мая 2019

Изменён: 12:46:54 21 мая 2019

Получен: 09:55:50 27 марта 2020

Обновлён: 09:55:50 27 марта 2020

Взаимосвязи

Отчёты (1)

Индикаторы (3)

Обогащение

GeolP: ipgeolocation.io

GeolP: MaxMind

OPSWAT Metadefender

Alien Labs OTX

Alien Labs Reputation

Страна: Netherlands

Регион: North Holland

Город: Amsterdam

Координаты: 4.89517 52.37020



- Дашборд
- Индикаторы**
- Обнаружения
- Отчёты
- Вредоносное ПО
- Уязвимости
- Автоматизация
- Настройки

admin

← К списку индикаторов

Сводка

Источник: `ddos attacks`
Значение: `84.77.166.221`
Тип: `ip`

Создан: 19:00:02 12 февраля 2018
Изменён: 19:00:02 12 февраля 2018
Получен: 12:36:52 27 марта 2020
Обновлён: 12:36:52 27 марта 2020
Первое появление: 19:00:02 12 февраля 2018
Последнее появление: 19:00:02 12 февраля 2018

Рейтинг:

Индикатор компрометации

Взаимосвязи

Индикаторы (1)

Обогащение

- GeoIP: ipgeolocation.io**
- GeoIP: MaxMind
- OPSWAT Metadefender
- Alien Labs OTX
- Alien Labs Reputation
- Risk IQ
- Shodan
- GeoIP: Sypex
- ThreatCrowd
- ThreatMiner
- TotalHash
- VirusTotal
- Whois

Страна: Spain
Регион: Community of Madrid
Город: Pozuelo de Alarcón
Координаты: -3.80371 40.42030



Обогащение индикатора

- Дашборд
- Индикаторы
- Обнаружения**
- Отчёты
- Вредоносное ПО
- Уязвимости
- Бюллетени
- Автоматизация ▾
 - Обогащение
 - Обнаружение
 - Экспорт
 - Интеграции
 - Оповещение
- Настройки ▾

admin

← К списку обнаружений

- ThreatMiner
- TotalHash
- VirusTotal
- Whois
- ИСТРА

Обнаружения

Сенсор: Microfocus ArcSight Дата обнаружения: 15:43:59 08 мая 2020	↔
Сенсор: Microfocus ArcSight Дата обнаружения: 15:43:43 08 мая 2020	↔
Сенсор: Microfocus ArcSight Дата обнаружения: 15:37:19 08 мая 2020	↔
Сенсор: Microfocus ArcSight Дата обнаружения: 15:37:05 08 мая 2020	↔
Сенсор: Microfocus ArcSight Дата обнаружения: 15:31:39 08 мая 2020	↔

1 2

Жизненный цикл индикатора



- Дашборд
- Индикаторы
- Обнаружения
- Отчёты
- Вредоносное ПО
- Уязвимости**
- Автоматизация
- Настройки

admin

Уязвимости

Поиск...

Имя	CVE
CVE-2019-11510	CVE-2019-11510
CVE-2019-12426	CVE-2019-12426
CVE-2019-1242	CVE-2019-1242
CVE-2018-19974	CVE-2018-19974
CVE-2018-7586	CVE-2018-7586
Vulnerability Report Not Available	CVE-2019-14002
Vulnerability Report for Qualcomm...	CVE-2019-14014
Vulnerability Report for Qualcomm...	CVE-2019-14013
Vulnerability Report Not Available	CVE-2020-0003
Vulnerability Report for Google Android...	CVE-2020-0004
Vulnerability Report Not Available	CVE-2019-10602
Vulnerability Report Not Available	CVE-2020-0001
Vulnerability Report Not Available	CVE-2019-10611
Vulnerability Report for Linux Kernel...	CVE-2019-17666
Vulnerability Report for Qualcomm...	CVE-2019-14036
Vulnerability Report Not Available	CVE-2020-0006
Vulnerability Report Not Available	CVE-2019-10583
Vulnerability Report Not Available	CVE-2019-10579

Vulnerability Report for Qualcomm Snapdragon products buffer overflow

Qualcomm Snapdragon products are vulnerable to a buffer overflow, caused by a flaw when byte array receives incorrect input from reading source as array is not null terminated, elements within super index table. By sending a specially-crafted request, a remote attacker could overflow a buffer and execute arbitrary code on the system.

CVE: CVE-2019-14014
 Создана:
 Последнее изменение:

CVSSv3

Базовая оценка: 9,8
 Оценка эксплуатируемости: 0
 Оценка влияния: 0

Дополнительная информация

Сложность атаки: Низкая
 Вектор атаки: Сеть
 Влияние на доступность: Высокая
 Влияние на конфиденциальность: Высокая
 Влияние на целостность: Высокая
 Требуемый уровень привилегий: Нет
 Охват: Без изменений
 Взаимодействие с пользователем: Нет

Ссылки

[Qualcomm Web site CVE-2019-14014](#)

Взаимосвязи

Отчёты (1)

[Google January 2020 Android Security Bulletin](#)

- Дашборд
- Индикаторы
- Обнаружения
- Отчёты
- Вредоносное ПО
- Уязвимости
- Бюллетени
- Автоматизация
- Настройки
- Поставщики данных
- Обнаружение
- Обогащение
- Интеграции
- Оповещение
- Экспорт
- Бюллетени
- Система
- Пользователи
- Лицензия

Настройки фильтра

Поиск: Все наименования

Кластеризация:

- Отчёты 1
- Объекты наблюдения 5

Расширенная кластеризация:

- Тип индикатора
 - domain
 - url
- Поставщик данных
 - AT&T Cybersecurity
 - VirusTotal

Фильтрация:

- Вид сущности
 - Отчёт
 - Объект наблюдения
- Поставщик данных

Очистить Экспортировать

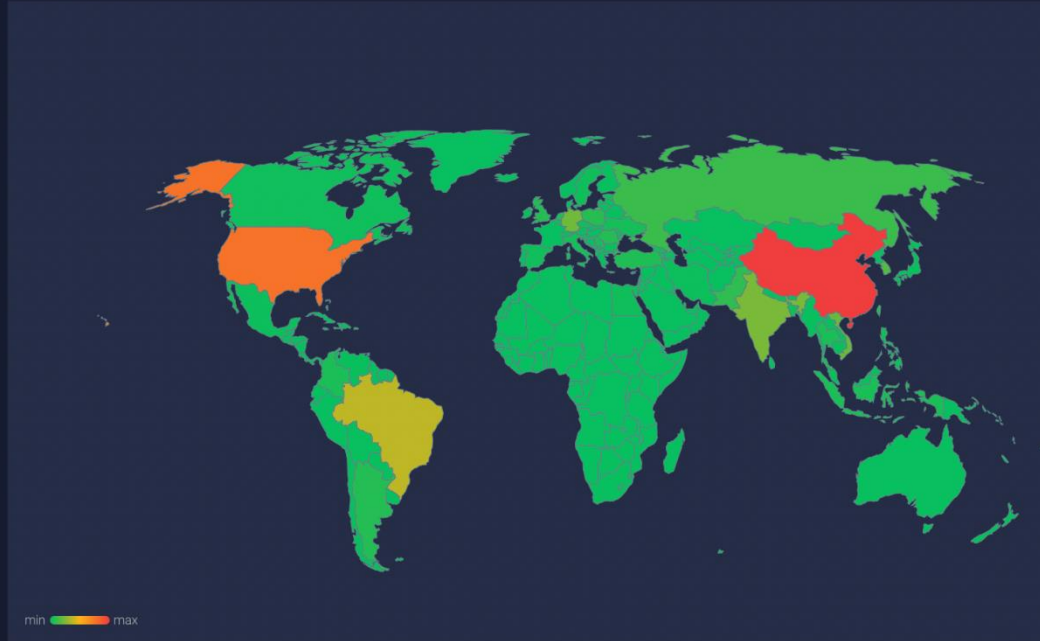
```
graph TD; VT((VirusTotal)) --- ATAT((AT&T Cybersecurity)); VT --- URL((url)); VT --- DOMAIN((domain)); ATAT --- SIEM[Arcsight SIEM Test]; URL --- IP[http://185.101.34.122/]; URL --- DDNS1[http://donchichi.ddns.net/]; DOMAIN --- PLESK2[plesk2.ariesdomain.no]; DOMAIN --- PLESK[plesk.ariesdomain.no]; DOMAIN --- DDNS2[donchichi.ddns.net];
```

- Дашборд
- Уведомления
- Индикаторы
- Аналитика
- Обнаружения
- Угрозы
- Бюллетени
- Автоматизация
- Настройки

admin

Индикаторы компрометации по странам

Карта + Список | Последние 30 дней



Китай	230
Соединенные Штаты Америки	177
Бразилия	86
Индия	55
Германия	51
Вьетнам	48
Южная Корея	38
Россия	27
Пакистан	21
Тайвань	19
Польша	18
Аргентина	16
Великобритания	16
Румыния	16
Турция	15
Нидерланды	15
Гонконг	14
Франция	13
Таиланд	13
Индонезия	13
Колумбия	13
Сингапур	9
Украина	9
Сербия	9
Италия	0

Наиболее активные

Индикаторы

ip	123.231.11.10
ip	123.231.11.11
url	123.231.11.11
ip	1.11.111.1
ip	132.12.33.1

Обогащенные индикаторы

Последние 30 дней



Обнаружения IoC

01.01.2020 - 04.10.2020



Результат



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



Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб благодаря автоматической выгрузке обработанных данных напрямую на СЗИ



Ускоряет процессы ИБ за счет быстрого поиска контекста в доступных источниках, анализа связанной информации и автоматизации ключевых сценариев

Кейсы использования R-Vision TIP



Нефтегазовый сектор

Threat Hunting, выявление и предотвращение APT-атак на ранних этапах в крупной компании нефтегазового сектора



Финансовый сектор

Формирование собственных бюллетеней угроз и уязвимостей в ряде крупных российских банков для информирования дочерних структур



Государственный сектор

Автоматическое обнаружение вредоносной активности, связанной с ИТ-активами организаций, которые обслуживаются внешним SOC



Промышленный сектор

Анализ данных об угрозах для повышения эффективности управления уязвимостями, рисками и стратегического планирования в компании промышленного сектора



R-Vision

 + 7 (499) 322 80 40

 sales@rvision.ru

 www.rvision.ru

Подписывайтесь на наш
дайджест ИБ: rvision.ru/blog