

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Данные, которым можно доверять

Как измерять качество Threat Intelligence
и превращать фиды в решения

Валерия Чулкова

PO Threat Intelligence Platform
R-Vision



Главный вопрос

Не «сколько индикаторов у нас есть?»,
**а «насколько уверенно мы можем
принять решение на их основе?»**

Ценность TI измеряется влиянием на действие

Ценность СТИ теряется между данными и решением

91%

считают ТИ важной

26%

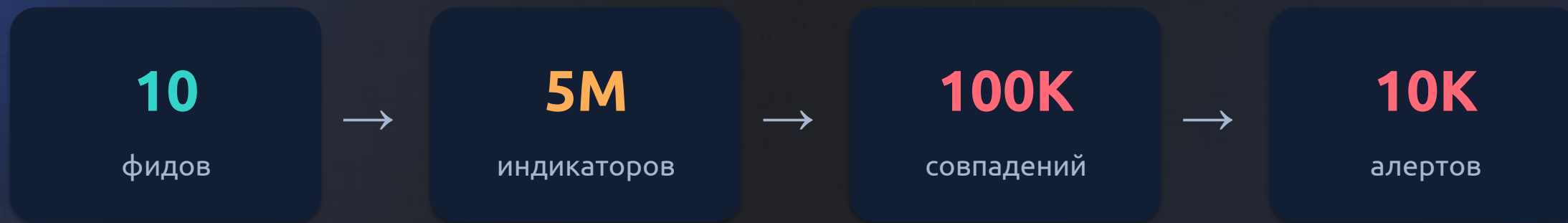
говорят о влиянии
на решения

57%

не отслеживают
зрелость

Проблема — не только в нехватке данных.
Она в доверии, контексте и обратной связи.

Больше данных ≠ больше защиты



Дубли • устаревание • разные форматы • отсутствие контекста

Один IP — несколько возможных решений

203.0.113.10

- Когда замечен?
- Кто сообщил?
- Есть ли подтверждения?
- С какой кампанией связан?
- Используется ли сейчас?

Без контекста

индикатор

не отвечает на вопрос
«что делать?»

Шесть измерений качества

01

Актуальность

02

Точность

03

Уникальность

04

Обширность

05

Релевантность

06

Применимость

Качество — это система взаимосвязанных свойств

Актуальность и точность

АКТУАЛЬНОСТЬ

Когда замечен?
Как быстро обновляется?
Когда устаревает?

ТОЧНОСТЬ

Есть ли подтверждения?
Есть ли история
сканирований?
Что говорит первоисточник?

Уникальность — не то же самое, что ценность

Важно различать:

- Дублирование данных
- Независимое подтверждение
- Дополнительный контекст

**Уникальный,
но шумный фид**

не обязательно лучше
менее уникального, но точного

Контекст отвечает на вопрос «почему?»

- Кампания и группировка
- Инструменты и вредоносное ПО
- Первое и последнее наблюдение
- Связанные домены, IP, хэши и TTP
- Источники и доказательства



Релевантность и применимость

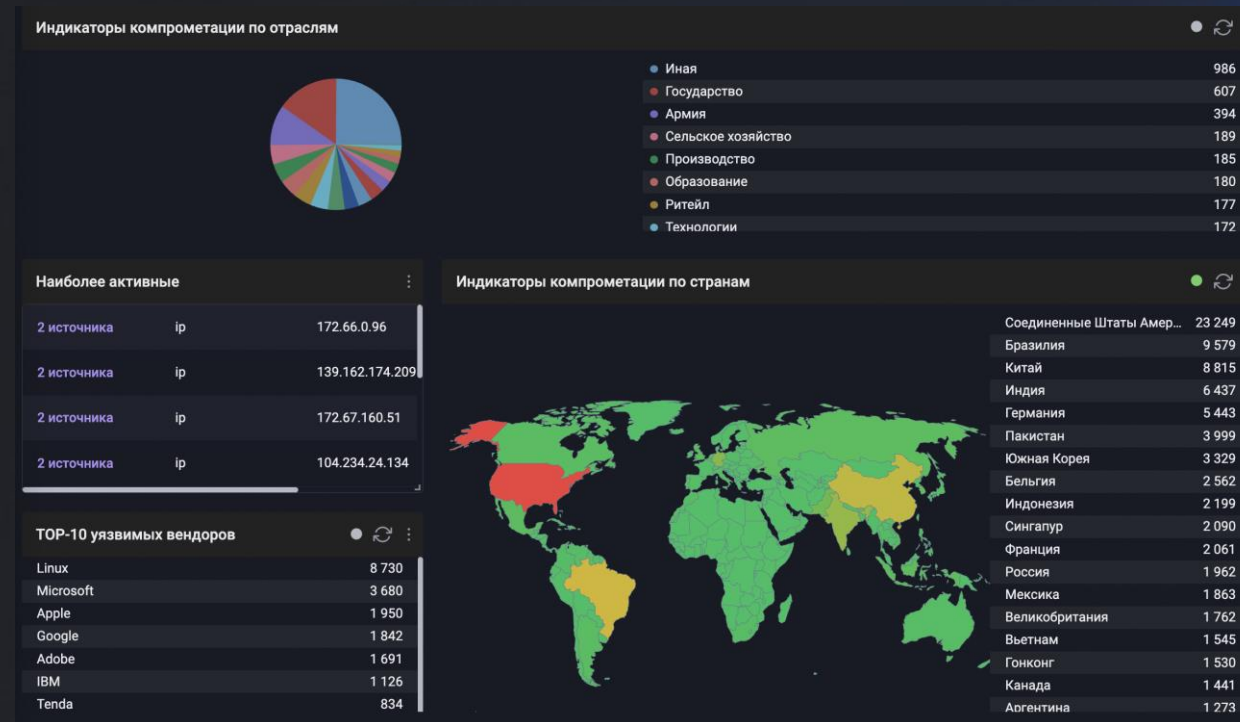
Один и тот же индикатор
может иметь разный
приоритет

Отрасль

География

Технологии

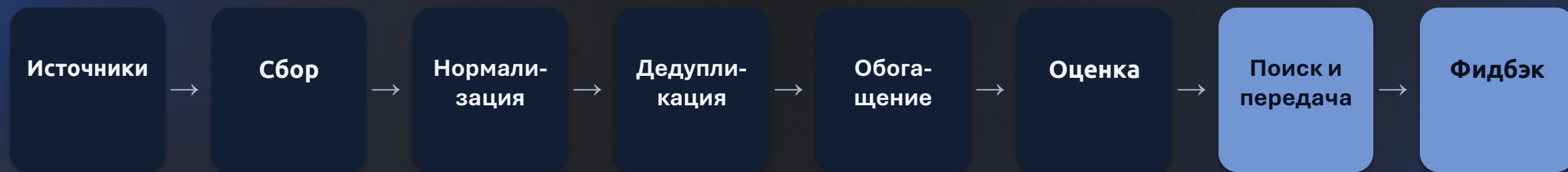
Критичные активы



Качественная TI всегда предлагает следующий шаг:

заблокировать · проверить · расследовать · мониторить · ничего не делать

TIP — это не только хранилище фидов



Цель — сделать путь от сигнала до действия прозрачным и управляемым

Детали индикатора



Источники

RST Cloud IP blocklistDeSSH

Статус

Активный

Значение

183.240.197.57

Тип

ip

Страна

Китай

Вид сущности

● Индикатор компрометации

Изменён

06.10.2026, 07:09:21

Первое появление

25.07.2026, 03:00:00

Последнее
появление

04.10.2026, 03:00:00

Получен

04.07.2021, 11:18:38

Источник по
данным источника

cinsscore_badguys

Описание

http://cinsscore.com/list/ci-badguys.txt?query_date=20261004

≠

две записи
без общего контекста

Один объект
с доказательствами

Метрики активности не равны метрикам пользы

Не только:

- Количество фидов
- Количество индикаторов
- Количество экспортов

Но и:

- Доля актуальных IoC
- Доля ложных срабатываний
- Время до действия
- Доля обнаружений с результатом

Измеряем не поток данных, а эффект для SOC

Как оценить источник до подключения

ПОКРЫТИЕ

География
Типы угроз
Сценарии
использования

ПРОИСХОЖДЕНИЕ

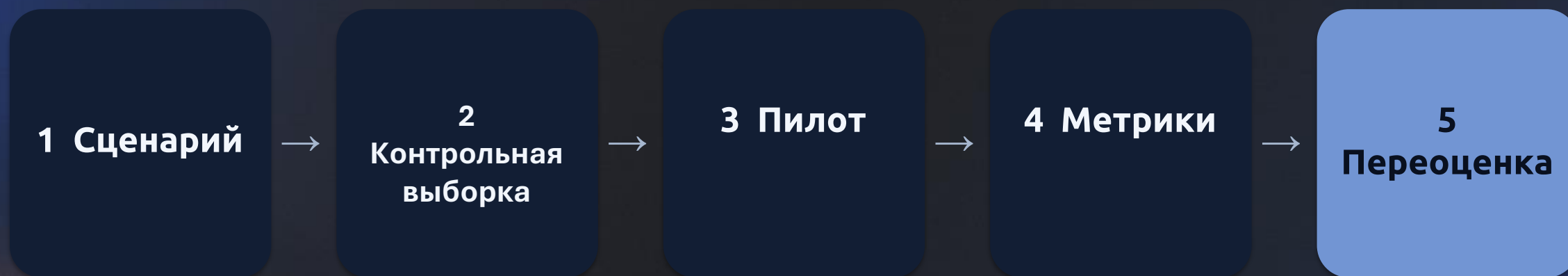
Телеметрия
Открытые источники
Собственная
аналитика

ИНТЕГРАЦИЯ

STIX/TAXII
JSON / CSV / API
Периодичность и
SLA

Для каких сценариев нужны данные?

Пять шагов оценки фида



Качество — это замкнутый цикл

Источник → Сигнал → Решение → Результат

**Результат расследования должен влиять на оценку источника
и правила обработки**

Три вывода

01 Объем не равен качеству

Актуальность, точность, контекст и применимость

02 Качество создается на пути данных

Нормализация, связи, обогащение и правила обработки

03 Главная метрика — результат

Влияние на решение и защиту

**Хорошая Threat Intelligence —
не самая большая база индикаторов.**

Это данные, которым аналитик доверяет настолько,
чтобы принять решение.

Благодарю за внимание

Валерия Чулкова

PO Threat Intelligence Platform

R-Vision



Ampire 360°