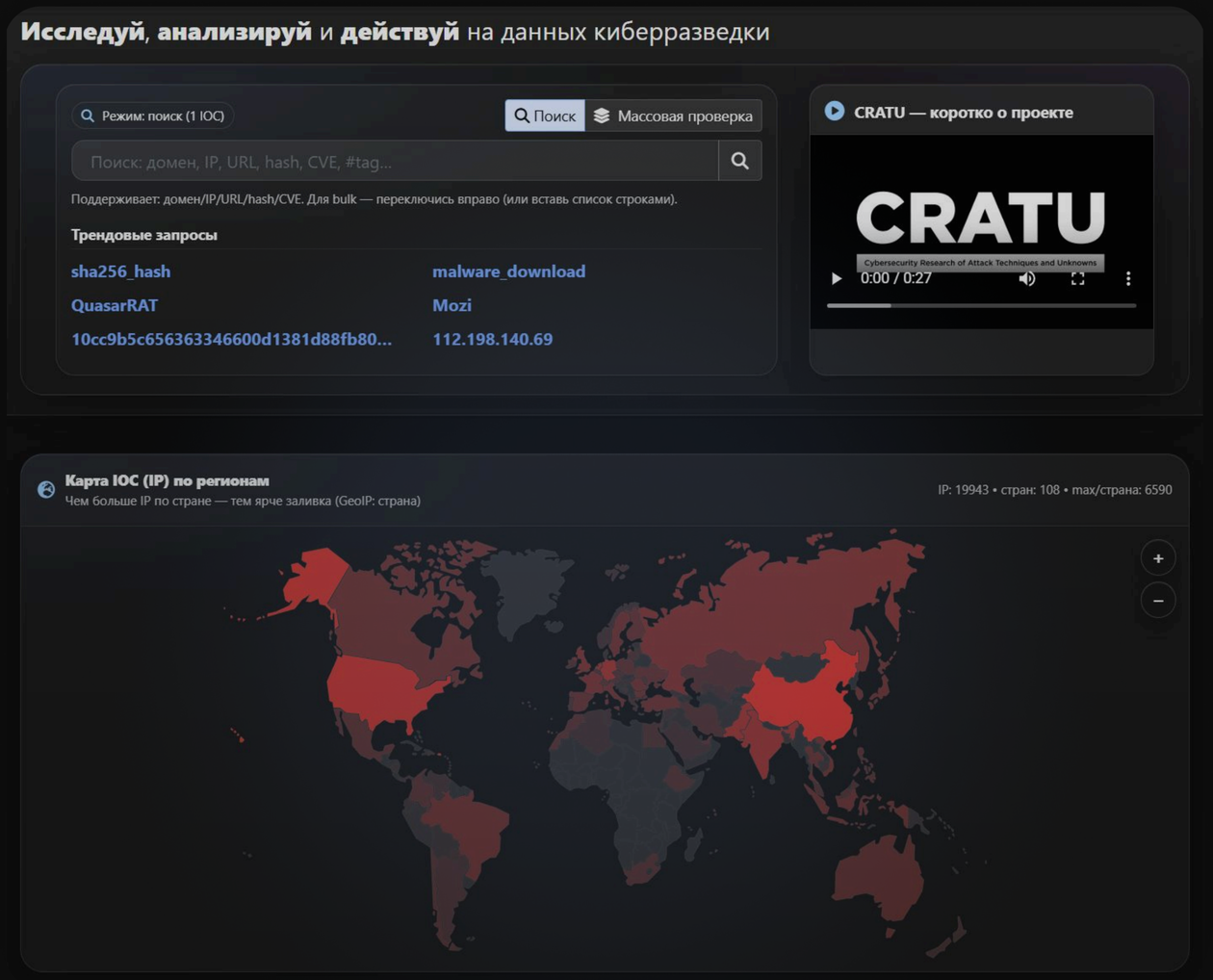
CRATU ThreatLens

Портал киберразведки для поиска, анализа и мониторинга IOC

IOC | Контекст | Мониторинг | API



IOC без контекста превращают анализ в шум

Разрозненные источники, ручная корреляция и отсутствие приоритета замедляют первичную оценку и перегружают SOC.

Разрозненные источники

Контекст по IOC приходится собирать из нескольких систем и публикаций.

Ручная корреляция

Связи между индикаторами, инфраструктурой и вредоносным ПО часто приходится проверять вручную.

Нет приоритета

Без понятного риска и контекста шумовые сигналы конкурируют с реально важными.

Аналитик тратит время не на решение, а на сбор картины.

CRATU ThreatLens превращает IOC в рабочий контекст для аналитика

Платформа объединяет поиск, обогащение, связи, мониторинг и программный доступ в одном рабочем контуре.

Проверка

Одиночный и массовый поиск IOC для быстрой первичной оценки

Контекст

Карточка IOC, связи, MITRE, MISP, группировки, семейства и метки

Мониторинг

Закладки, отслеживание, уведомления и ежедневный дайджест

Интеграция

REST API для интерфейса, SIEM, SOAR и внутренних процессов

Поиск → Контекст → Мониторинг → Интеграция

Аналитик тратит время не на решение, а на сбор картины.

От источников угроз — к действиям SOC

CRATU ThreatLens собирает IOC из внешних источников, нормализует и связывает их, обогащает контекстом и передаёт результат через интерфейс и API.

Потоки данных

- Внешние потоки индикаторов
- Репутационные сигналы
- Исследовательские материалы
- Сервисы верификации и обогащения

Ядро платформы

- Сбор и нормализация
- Хранение и индексация
- Связи и корреляция
- Единая модель данных

Обогащение

- Классификация и контекст
- ATT&CK и тактики
- Семейства вредоносного ПО и группировки
- Риск и аналитические признаки
- AI-пояснение и summary

Использование

- Портал аналитика
- Карточки IOC
- Массовая проверка
- API и интеграции
- SOC / IR / Hunting / SIEM

Результат для аналитика: быстрее первичная оценка, больше контекста, безопасная интеграция

Модальная карточка IOC: весь контекст в одном окне

Аналитик получает ключевые атрибуты IOC, связи, MITRE, MISP, публикации, группировки и рабочие действия без перехода между несколькими экранами.

1 Действия аналитика

Отслеживание, закладка и переход к расширенному просмотру IOC.

2 Ключевые атрибуты IOC

Значение, тип, угроза, доверие, даты появления и обновления.

3 Теги и контекст

Инфраструктурные, поведенческие и тематические признаки для первичной оценки.

4 MITRE ATT&CK

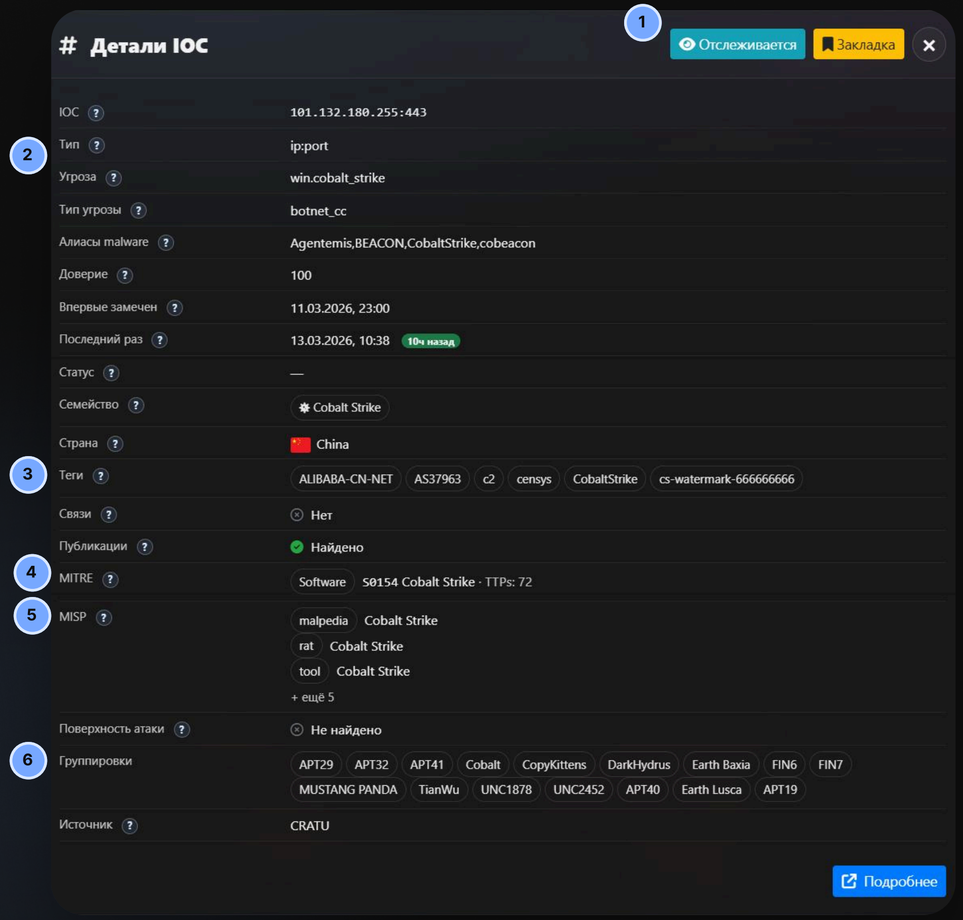
Связь IOC с техникой, ПО и тактиками противника.

5 MISP и классификация

Категории, таксономии и дополнительные контекстные сущности.

6 Связанные группировки

Сопоставление IOC с группировками и исследовательским контекстом.



Глубокая карточка IOC: не просто индикатор, а его связи и смысл

Карточка IOC помогает быстро понять угрозу, доверие, связи, классификацию и возможные действия аналитика.

1 Hero и риск

Значение IOC, тип, уровень угрозы, доверие и ключевые признаки для быстрого первичного понимания.

2 MITRE ATT&CK и MISP

Связь индикатора с техниками, тактиками и таксономиями для более точной аналитической интерпретации.

3 Связи и Pivot

Переход к связанным IOC, инфраструктуре и сущностям для расширения расследования.

4 Публикации и внешние ссылки

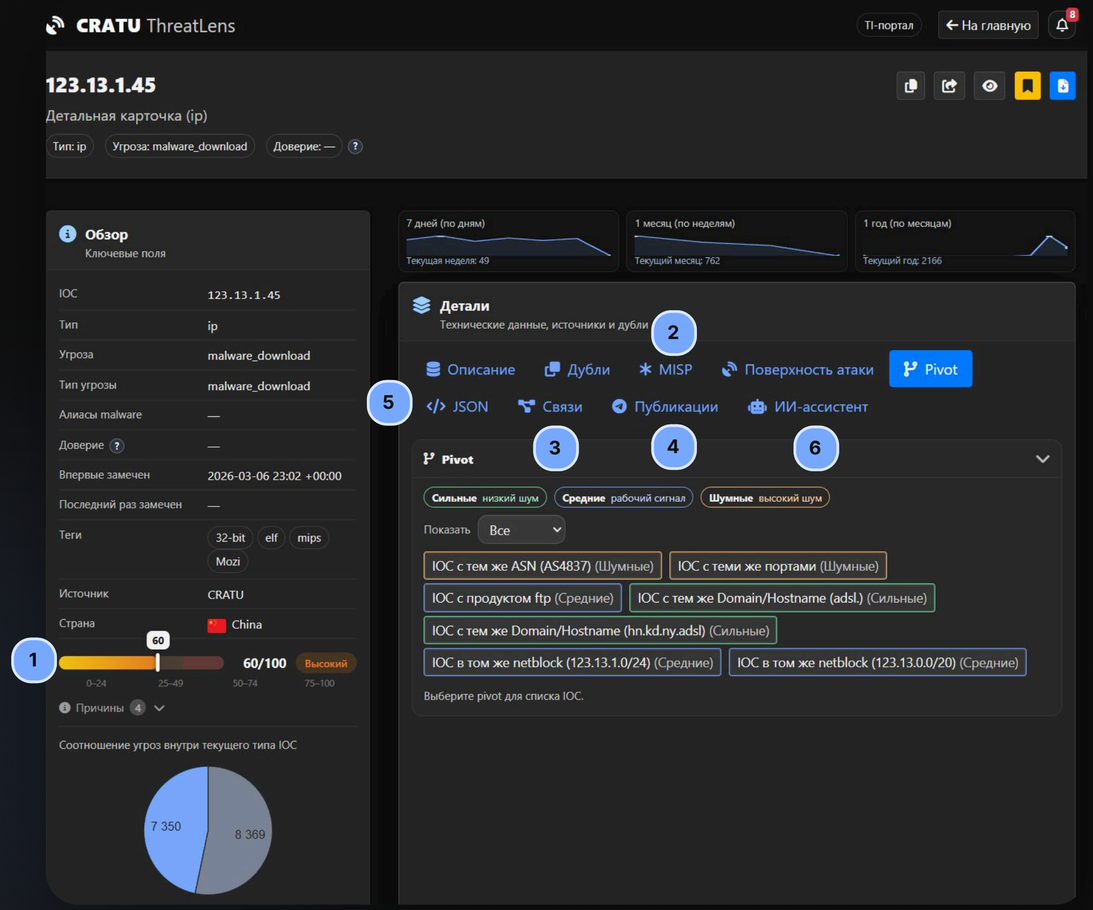
Дополнительные материалы, аналитические публикации и внешние источники для подтверждения контекста.

5 JSON / экспорт / отслеживание

Рабочие действия аналитика: экспорт, шаринг, закладки и постановка на отслеживание.

6 AI-ассистент

Быстрое пояснение контекста IOC и помощь в интерпретации данных для аналитика.



IOC, actors, families и tags — в одном контексте

Threat Intelligence полезна тогда, когда индикатор можно связать с инфраструктурой, семейством ВПО, группировкой и кампанией.

IOC | Группировки | Семейства | Метки

1 Группировки

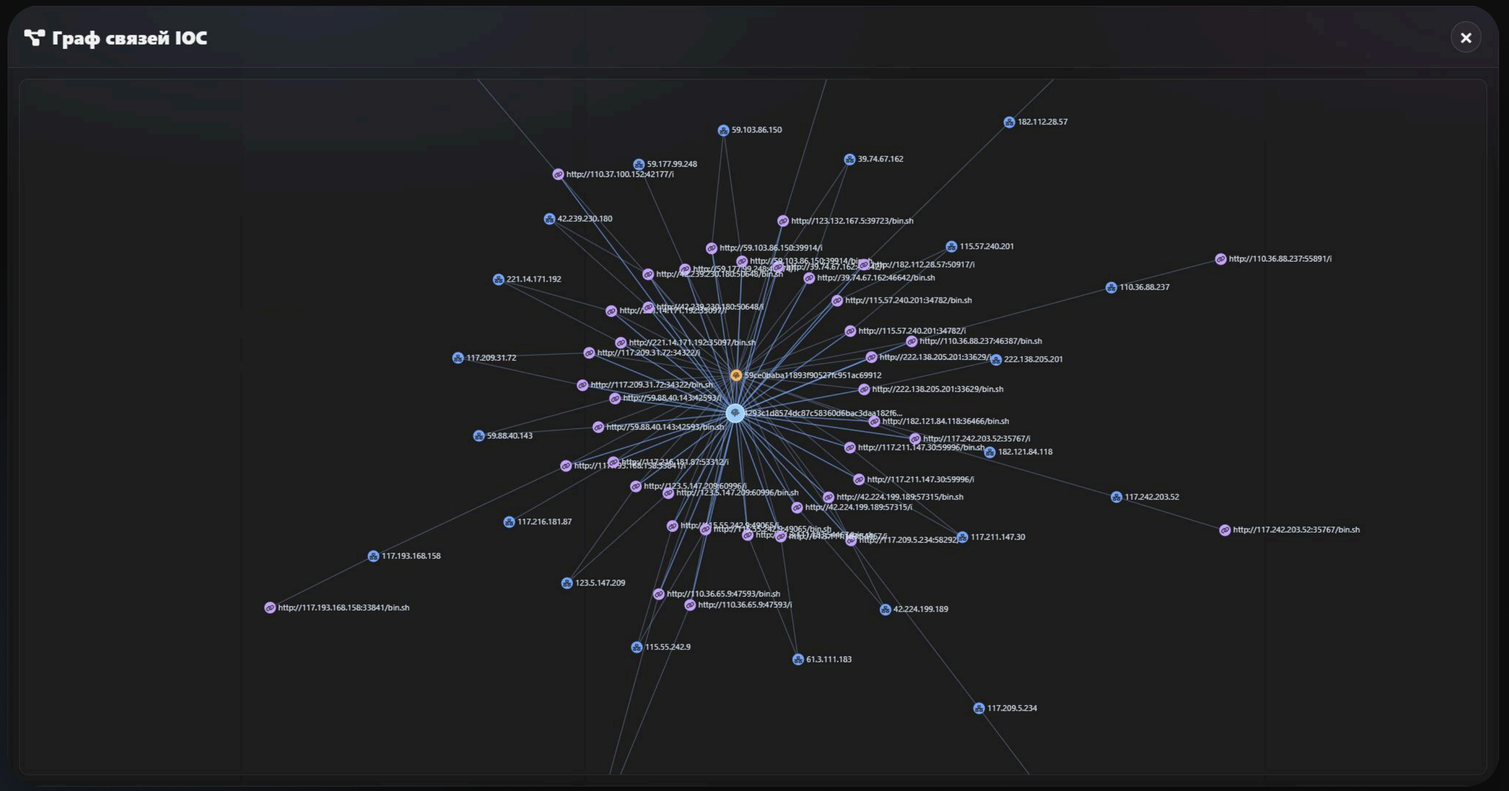
Карточки группировок, синонимы, публикации и связанные IOC

2 Семейства

Семейства ВПО, описания, YARA, публикации и связанные IOC

3 Метки

Навигация по кампаниям, темам и контекстным меткам



Ежедневные функции, которые ускоряют аналитику

CRATU ThreatLens полезен не только в момент поиска, но и в ежедневной операционной работе.

Массовая проверка

Проверка списка IOC одним действием

Закладки

Сохранение интересующих индикаторов для быстрой работы

Отслеживание

Мониторинг изменений по выбранным IOC

Уведомления

Оповещения о событиях и изменениях

Ежедневная сводка

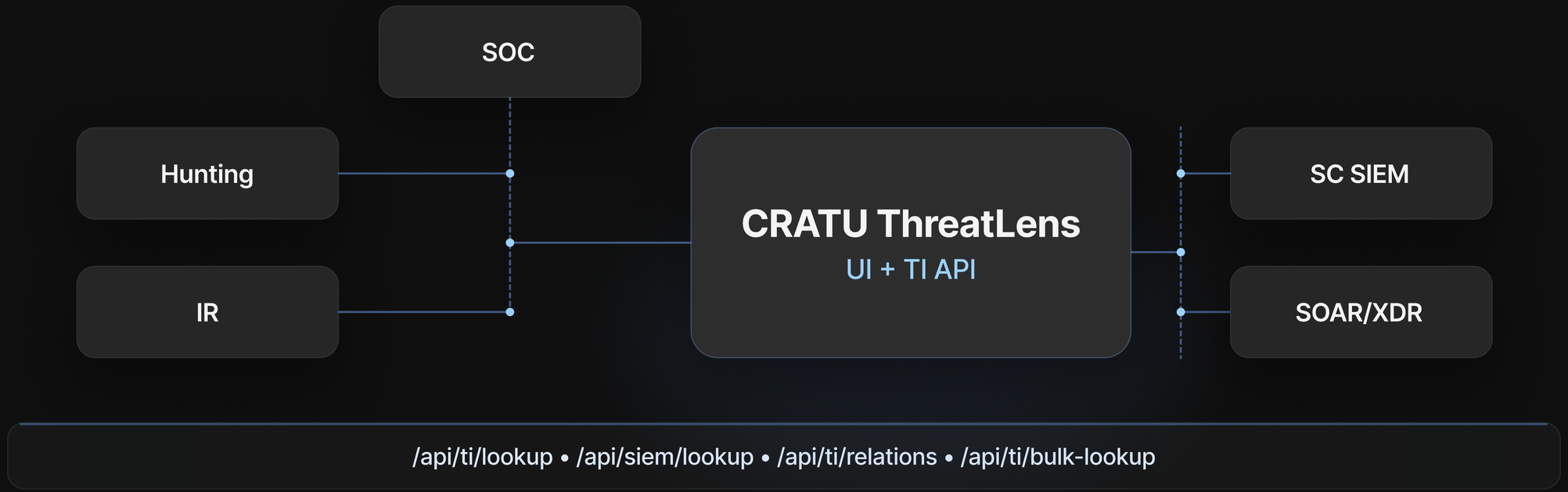
Ежедневная выгрузка свежих IOC на email

AI-ассистент

Объяснение контекста, рекомендации и аналитическая карточка IOC

Threat Intelligence, которая встраивается в ваш стек

Портал даёт UI для аналитика и API для интеграции с SIEM, SOAR, внутренними сервисами и рабочими процессами.



Ключ API / Bearer-токен / список разрешённых IP-адресов / лимиты

Разная роль — одна платформа

Аналитик SOC

Быстрее первичная оценка

Проверка IOC, массовый поиск, карта, обозреватель и базовый контекст за минуты.

Специалист по реагированию

Богаче расследование

Связи, публикации, семьи ВПО, группировки и полная карточка IOC для гипотез.

Threat Hunter

Больше связей и гипотез

Метки, переходы по связанным объектам, группировки, семейства и обогащение помогают расширять расследование.

Руководитель ИБ

Понятнее ценность TI

Видимость функций, интеграционный контур и практическая применимость для SOC и IR.

• Один продукт — несколько ролей и сценариев использования •

Почему CRATU ThreatLens — практичный TI-инструмент

01 Публичный вход и приватная глубина

02 От поиска к мониторингу в одном рабочем контуре

03 IOC, группировки, семейства и метки в одном контексте

04 AI-ассистент внутри карточки IOC

05 Интерфейс для аналитика и API для интеграции

Кибербразведка должна ускорять решение, а не добавлять ещё один экран с шумом.

Начните с пилота и проверьте применимость на своих IOC

Публичный поиск — для первого знакомства. Полный доступ — для ежедневной аналитики, мониторинга и интеграции.

1. Получить доступ
2. Проверить рабочие кейсы
3. Обсудить интеграцию

CRATU ThreatLens

Публичный поиск / Полный доступ

Запросить пилот

manager@itb.spb.ru · demo · integration
Ответим на запрос и согласуем пилотный сценарий

Публичный поиск → Полный доступ → Пилот