

CRATU ThreatLens

Портал киберразведки для поиска, анализа и мониторинга IOC

IOC

Контекст

Мониторинг

API

Исследуй, анализируй и действуй на данных киберразведки

Режим: поиск (1 IOC)

Поиск Массовая проверка

Поиск: домен, IP, URL, hash, CVE, #tag...

Поддерживает: домен/IP/URL/hash/CVE. Для bulk — переключись вправо (или вставь список строками).

Трендовые запросы

sha256_hash

malware_download

QuasarRAT

Mozi

10cc9b5c656363346600d1381d88fb80...

112.198.140.69

CRATU — коротко о проекте

CRATU

Cybersecurity Research of Attack Techniques and Unknowns

0:00 / 0:27

Карта IOC (IP) по регионам

Чем больше IP по стране — тем ярче заливка (GeoIP: страна)

IP: 19943 • стран: 108 • max/страна: 6590



ИОС без контекста превращают анализ в шум

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



Разрозненные источники

Контекст по ИОС 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 АТТ&СК 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.

The screenshot shows a modal window titled "# Детали IOC" with a close button and two action buttons: "Отслеживается" (highlighted with callout 1) and "Закладка". The main content is a table of attributes for an IOC, with callouts 2-6 pointing to specific sections:

IOC	101.132.180.255:443
Тип	ip:port
Угроза	win.cobalt_strike
Тип угрозы	botnet_cc
Алиасы malware	Agentemis, BEACON, CobaltStrike, cobeacon
Доверие	100
Впервые замечен	11.03.2026, 23:00
Последний раз	13.03.2026, 10:38 10ч назад
Статус	—
Семейство	Cobalt Strike
Страна	China
Теги	ALIBABA-CN-NET AS37963 c2 censys CobaltStrike cs-watermark-666666666
Связи	Нет
Публикации	Найдено
MITRE	Software S0154 Cobalt Strike - TTPs: 72
MISP	malpedia Cobalt Strike rat Cobalt Strike tool Cobalt Strike + ещё 5
Поверхность атаки	Не найдено
Группировки	APT29 APT32 APT41 Cobalt CopyKittens DarkHydrus Earth Baxia FIN6 FIN7 MUSTANG PANDA TianWu UNC1878 UNC2452 APT40 Earth Lusca APT19
Источник	CRATU

At the bottom right, there is a "Подробнее" button.

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.

CRATU ThreatLens TI-портал ← На главную

123.13.1.45

Детальная карточка (ip)

Тип: ip | Угроза: malware_download | Доверие: — ?

Обзор Ключевые поля

IOC	123.13.1.45
Тип	ip
Угроза	malware_download
Тип угрозы	malware_download
Алиасы malware	—
Доверие ?	—
Впервые замечен	2026-03-06 23:02 +00:00
Последний раз замечен	—
Теги	32-bit elf mips Mozi
Источник	CRATU
Страна	China

60 / 100 **Высокий**

Причины 4

Соотношение угроз внутри текущего типа IOC

7 350	8 369
-------	-------

Детали Технические данные, источники и дубли

Описание | Дубли | MISP | Поверхность атаки | Pivot

JSON | Связи | Публикации | ИИ-ассистент

Pivot

Сильные: низкий шум | Средние: рабочий сигнал | Шумные: высокий шум

Показать: Все

- IOC с тем же ASN (AS4837) (Шумные)
- IOC с теми же портами (Шумные)
- IOC с продуктом ftp (Средние)
- IOC с тем же Domain/Hostname (adsl.) (Сильные)
- IOC с тем же Domain/Hostname (hn.kd.ny.adsl) (Сильные)
- IOC в том же netblock (123.13.1.0/24) (Средние)
- IOC в том же netblock (123.13.0.0/20) (Средние)

Выберите pivot для списка IOC.

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

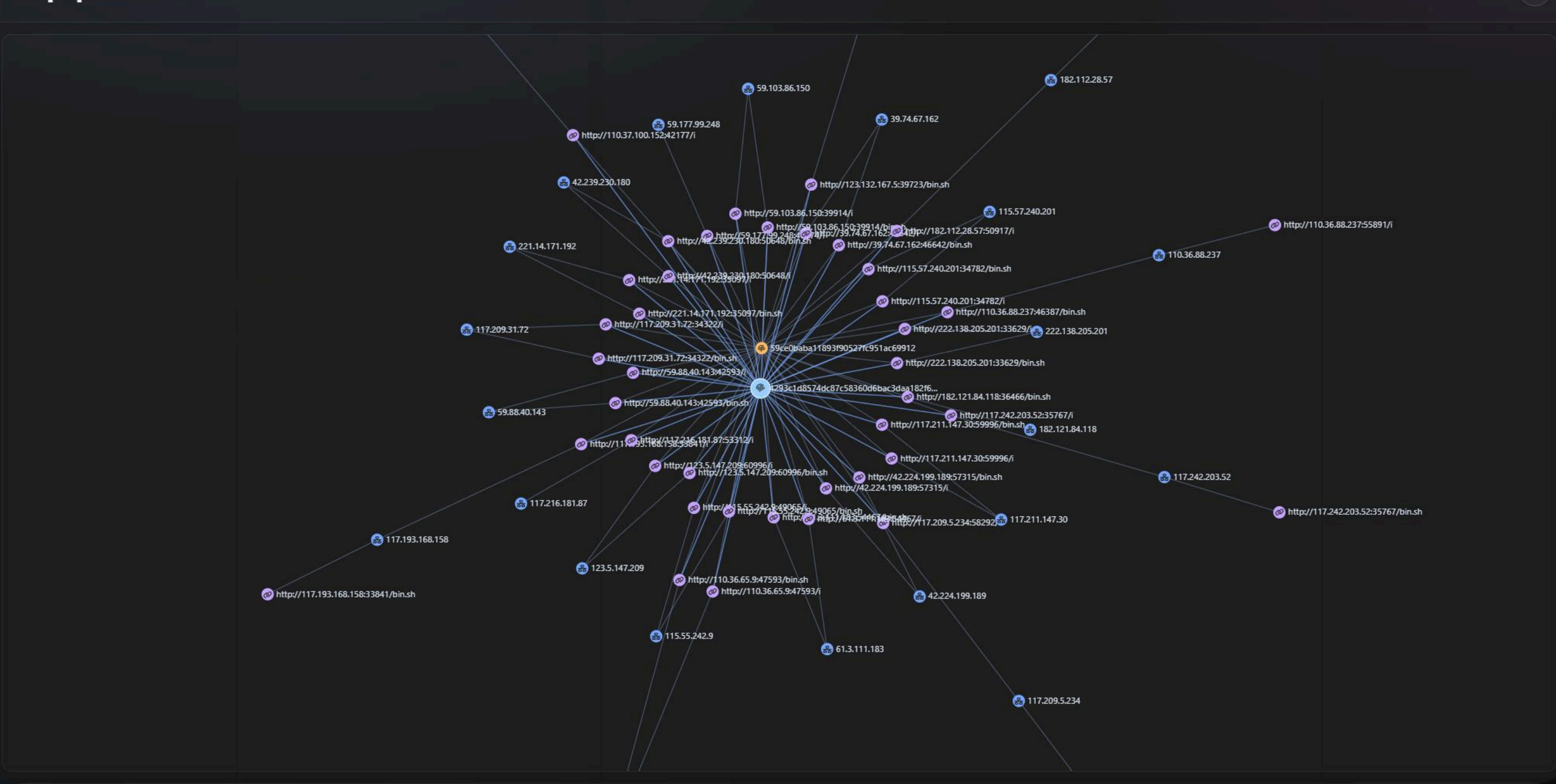
2 Семейства

Семейства ВПО, описания, YARA, публикации и связанные IOC

3 Метки

Навигация по кампаниям, темам и контекстным меткам

Граф связей IOC



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 интересных индикаторов для быстрой работы



Отслеживание

Мониторинг изменений по выбранным IOC



Уведомления

Оповещения о событиях и изменениях



Ежедневная сводка

Ежедневная выгрузка свежих IOC на email

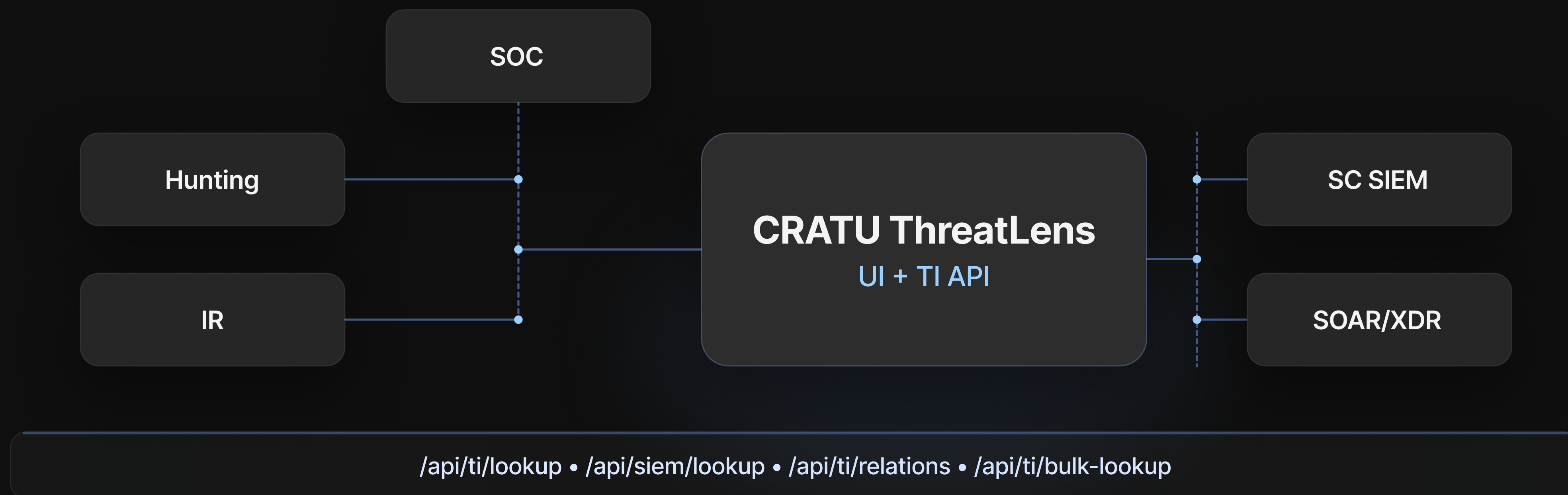


AI-ассистент

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

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

Начните с пилота и проверьте применимость на своих ИОС

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