Регламент работы

CRATU
ThreatLens

Дата редакции документа: 13.03.2026

Версия документа: 1

АННОТАЦИЯ

Регламент работы с порталом киберразведки (Threat Intelligence) CRATU ThreatLens.

Статус	Для пользователей с действующей подпиской и авторизованным доступом
Для кого	Подписчики портала, аналитики SOC, специалисты IR/Threat Hunting, инженеры интеграции
Назначение	Описать порядок работы с UI и персональными функциями портала, правила безопасного доступа и рекомендации по использованию данных TI.

СОДЕРЖАНИЕ

1 Назначение документа

Настоящий документ устанавливает рекомендуемый порядок работы пользователя с порталом CRATU ThreatLens после оформления подписки, входа в систему и получения доступа к персональным функциям.

Регламент предназначен для практического использования в операционной деятельности: при проверке IOC, анализе связей, мониторинге изменений, использовании API и взаимодействии с поддержкой.

2 Термины и определения

Термин	Определение
IOC	индикатор компрометации: IP-адрес, домен, URL, файловый хэш, CVE и другие наблюдаемые признаки угрозы.
Обогащение	добавление к IOC контекста: связей, классификации, географии, публикаций, данных внешних источников.
Триаж	первичная оценка сигнала или инцидента для принятия дальнейшего решения.
Actor	группировка или субъект угрозы, связанный с деятельностью в каталоге портала.
Family	семейство вредоносного программного обеспечения.
API-ключ	токен программного доступа к данным портала.
Allowlist	список доверенных IP-адресов, с которых разрешены запросы к API.
Bulk lookup	массовая проверка списка IOC одним действием или запросом.
Digest	ежедневная email-сводка по обновлениям IOC.

3 Роли и модель доступа

3.1 Категории пользователей

Категория	Доступ
Неавторизованный пользователь	Публичная карта и публичный поиск с ограниченным просмотром результатов.
Пользователь с активной подпиской	Полный доступ к разделам портала, персональным функциям и, при наличии тарифа, к API.
Инженер интеграции / API-потребитель	Работа с API-ключами, настройкой allowlist и интеграцией с внешними системами.

3.2 Роли заказчика вне портала

Роли SOC L1/L2, Incident Response, Threat Hunting, инженер интеграции и руководитель ИБ относятся к внутренней организации работы заказчика. Портал не навязывает распределение этих ролей, но поддерживает их типовые сценарии.

3.3 Роль поставщика сервиса

а) поддержка доступности портала и базовой работоспособности пользовательских функций;

б) развитие каталога данных, нормализации и контекстного обогащения;

в) обработка обращений пользователей по вопросам доступа, ошибок и эксплуатации.

4 Политика доступа и безопасности

4.1 Учетные записи

а) доступ предоставляется персональным пользователям с активной подпиской;

б) рекомендуемая минимальная длина пароля - 8 символов;

в) общие учетные записи и передача доступа третьим лицам не рекомендуются;

г) при первом входе пользователь меняет временный пароль на постоянный.

4.2 Восстановление доступа

Если пароль утерян, пользователь инициирует восстановление через форму входа, получает ссылку на email и задает новый пароль. При ошибках входа необходимо проверить корректность учетных данных, статус подписки и сетевую доступность портала.

4.3 API-ключи и IP allowlist

а) API-ключи используются только в рамках тарифа, где предусмотрен программный доступ;

б) запросы к API выполняются только с доверенных IP-адресов, указанных в allowlist;

в) ключи нельзя публиковать в репозиториях, пересылать по незащищенным каналам или передавать третьим лицам;

г) при подозрении на компрометацию ключ должен быть немедленно отозван и заменен.

4.4 Журналирование и аудит

Для целей эксплуатации и расследования инцидентов могут фиксироваться события аутентификации, действия в UI, обращения к API, IP-адрес источника, user-agent и результаты запросов. Пользователь обязан соблюдать внутренние правила ИБ при работе с передаваемыми в портал данными.

4.5 Корректное использование

а) портал не предназначен для неконтролируемого скрейпинга или попыток выгрузить полную базу данных;

б) использование сервиса должно соответствовать тарифным ограничениям и договорным условиям;

в) в запросы не следует передавать персональные данные или лишние чувствительные сведения, если они случайно присутствуют в URL и иных артефактах.

5 Интерфейс и разделы портала

5.1 Верхняя панель навигации

Верхняя панель содержит переходы к дашборду, индикаторам, обзору, семействам, группировкам, индикатор состояния сервиса, кнопку уведомлений, доступ к техподдержке и личному кабинету.

5.2 Дашборд

а) поисковая область с режимами "Поиск" и "Массовая проверка";

б) трендовые запросы и ознакомительный блок;

в) KPI-плитки по объему IOC, новым данным за 24 часа и доступности сервиса;

г) интерактивная карта распределения IP-индикаторов;

д) лента публикаций, суточные всплески активности и обзор покрытий обогащения;

е) таблица-обозреватель IOC с фильтрами, сортировкой и пагинацией.

5.3 Публичный поиск и публичная карта

Даже после подписки пользователю доступны публичные страницы: стартовая карта и упрощенная страница поиска. Они полезны для обмена ссылками и предварительного ознакомления, но не заменяют работу в полном интерфейсе.

5.4 Карточки IOC

а) поддерживаются карточки для IP, domain, hash и CVE; адрес карточки зависит от типа IOC;

б) в заголовке карточки отображаются значение IOC, тип, уровень угрозы и уровень доверия;

в) доступны действия: копировать IOC, поделиться, отслеживать, закладки, JSON;

г) вкладки карточки могут включать обзор, поля БД, дубли, MITRE, MISP, связи, публикации, ссылки, ИИ-ассистент и типоспецифичные данные обогащения.

5.5 Каталоги группировок и семейств

Разделы actors и families предназначены для навигации по известным группировкам и семействам ВПО. Пользователь может искать сущность по имени, открывать карточку и переходить по связанным объектам.

5.6 Просмотр по тегу

Страница просмотра по тегу позволяет открыть все IOC, связанные с конкретной меткой, изучить статистику и быстро перейти к связанным карточкам.

5.7 Личный кабинет и уведомления

В личном кабинете собраны вкладки с общей информацией, API-ключами, лимитами, закладками, отслеживанием, подпиской на дайджест и сменой пароля. Через значок колокольчика открываются уведомления.

6 Стандартные сценарии работы

6.1 Поиск одиночного IOC

а) на дашборде убедиться, что выбран режим "Поиск";

б) ввести IOC: IP, домен, URL, MD5, SHA1, SHA256, CVE или тег с префиксом #;

в) запустить поиск клавишей Enter или кнопкой запуска;

г) при необходимости отфильтровать результаты по типу IOC;

д) открыть модальное окно и перейти к полной карточке по кнопке "Подробнее".

6.2 Массовая проверка IOC

а) переключиться в режим "Массовая проверка";

б) вставить список индикаторов - по одному на строку или через запятую;

в) запустить проверку и дождаться таблицы результатов;

г) использовать статусы, тип, уровень угрозы и доверия для дальнейшей обработки списка.

6.3 Работа с полной карточкой IOC

а) изучить обзор и ключевые поля: тип, угроза, доверие, даты, статус, теги, семейство и страну для IP;

б) посмотреть тренды обнаружения и вспомогательные диаграммы;

в) переключаться между вкладками деталей для углубленного анализа;

г) использовать граф связей и фильтры качества связей, если они доступны для данного типа IOC;

д) при необходимости скопировать IOC, выгрузить JSON или создать временную публичную ссылку.

6.4 Работа с группировками, семействами и тегами

а) в разделе "Группировки" искать actor по имени или синониму и открывать его карточку;

б) в разделе "Семейства" изучать семейства ВПО, связанные группы и правила YARA, если они доступны;

в) щелчком по тегу переходить к списку IOC с таким тегом и фильтровать результаты.

6.5 Закладки

Закладки используются для сохранения интересующих IOC. Добавление выполняется кнопкой в карточке или модальном окне, а просмотр - через отдельную вкладку личного кабинета с фильтрами по типу и строке поиска.

6.6 Отслеживание

Отслеживание позволяет ставить IOC на мониторинг и получать уведомления об изменениях. Индикатор можно добавить кнопкой в карточке или вручную на вкладке отслеживания.

6.7 Поделиться

Кнопка "Поделиться" создает временную публичную ссылку, которую можно безопасно использовать для отправки коллеге ограниченного представления данных по IOC.

6.8 Экспорт данных

Из карточки IOC доступен просмотр и выгрузка JSON. Дополнительно пользователь может подписаться на ежедневный дайджест свежих IOC в текстовом формате (defanged) или JSON.

6.9 Ежедневный дайджест

Подписка на дайджест управляется во вкладке "Подписка" личного кабинета. Функция может быть временно отключена администратором, о чем пользователь получает явное уведомление в интерфейсе.

6.10 Уведомления

Через значок колокольчика пользователь просматривает список системных уведомлений, может отмечать их прочитанными и удалять отдельные записи, если такая операция доступна интерфейсом.

6.11 Техподдержка

Форма обращения в техподдержку доступна авторизованному пользователю. Основные поля профиля подставляются автоматически, а в самом запросе рекомендуется описывать проблему максимально конкретно.

6.12 Лимиты

Во вкладке "Лимиты" пользователь контролирует текущие квоты по учетной записи и ограничения тарифа. Для API-ключей также отображаются сведения о лимитах, области доступа и времени последнего использования.

6.13 AI-ассистент

а) объяснение угроз и контекста - разбор характера угрозы и имеющихся связей;

б) подсказки и рекомендации - практические замечания по дальнейшим действиям;

в) аналитическая карточка IOC - структурированная сводка по ключевым фактам.

Для AI-анализа используются данные текущей карточки IOC; качество ответа зависит от полноты доступного обогащения.

7 Рекомендации по аналитической работе

а) используйте портал как ускоритель триажа и расследования, а не как единственный источник решений;

б) сопоставляйте результаты TI с телеметрией SIEM, EDR, DNS, Proxy, firewall и внутренним контекстом инцидента;

в) фиксируйте в тикете или карточке инцидента, какой IOC проверялся, какой контекст был получен и какие гипотезы подтверждены;

г) при работе со связями отделяйте сильные сигналы от шумных и не расширяйте гипотезу без дополнительных подтверждений;

д) поддерживайте отдельные рабочие списки IOC через закладки и отслеживание для длительных расследований.

8 API и интеграции

8.1 Общие принципы

а) актуальная техническая спецификация API публикуется в разделе API Docs внутри портала;

б) доступ к API предоставляется по HTTPS и требует действующего API-ключа;

в) для всех интеграций следует использовать allowlist доверенных IP-адресов.

8.2 Управление ключами

На вкладке API-ключей пользователь видит идентификатор, название, префикс, дату создания, дату последнего использования, лимит запросов, области доступа (scopes), белый IP-адрес и статус ключа. Время на вкладке может отображаться в MSK (UTC+3).

8.3 Аутентификация интеграции

Для подключения к API используются заголовки X-API-Key или Authorization: Bearer с полным значением действующего ключа. Конкретные примеры запросов и ответов следует брать из актуальной документации API.

8.4 Рекомендации по безопасной эксплуатации API

а) использовать отдельные ключи под разные интеграции и сценарии;

б) хранить секреты в защищенном secret-store, Vault, KMS или переменных окружения с ограниченным доступом;

в) реализовать ротацию и немедленный отзыв ключей при подозрении на компрометацию;

г) логировать время запроса, endpoint, результат, код ответа, корреляционный идентификатор и источник запроса на стороне интеграции;

д) реализовать контролируемые повторы для временных ошибок и защиту от бесконечных ретраев.

8.5 Типовые классы ответов

При проектировании интеграции рекомендуется предусмотреть стандартную обработку HTTP-ответов: 200 - успех; 400 - ошибка формата или параметров; 401/403 -

проблема авторизации или IP allowlist; 402 - отсутствие активной подписки; 429 - превышение лимита; 5xx - временная ошибка сервиса. Точные поля ошибок и полезные нагрузки определяются актуальной документацией API.

9 Поддержка и эксплуатационные обращения

а) при обращении в поддержку указывайте дату и время проблемы, часовой пояс, описание действия и ожидаемого результата;

б) для API-сценариев прикладывайте публичный IP, название интеграции, код ответа, correlation-id и фрагмент журнала;

в) если проблема связана с конкретным IOC, укажите значение IOC, тип и страницу, где возникла ошибка;

г) каналы поддержки, время реакции и SLA определяются договором и условиями подписки.

10 Основные экраны и сущности

Сущность / экран	Назначение
/	Публичная карта и обзорный вход в портал.
/search	Публичный поиск IOC без авторизации.
/portal	Главный дашборд авторизованного пользователя.
Карточка IOC	Детальная информация по IP, домену, hash или CVE.
Actors	Справочник группировок и их связей.
Families	Справочник семейств ВПО.
Browse by tag	Просмотр IOC по конкретному тегу.
Личный кабинет	Профиль, API-ключи, лимиты, закладки, отслеживание, подписка.
Уведомления	Оповещения об изменениях и системных событиях.

11 Заключительные положения

Настоящий регламент отражает пользовательский порядок работы с порталом в его актуальной редакции и должен применяться совместно с действующими коммерческими условиями, внутренними правилами ИБ заказчика и опубликованной в портале документацией API.

При обновлении функциональности портала документ подлежит пересмотру. Для задач внешнего ознакомления используется отдельная публичная версия регламента.