

Интеграция с ГосСОПКА

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

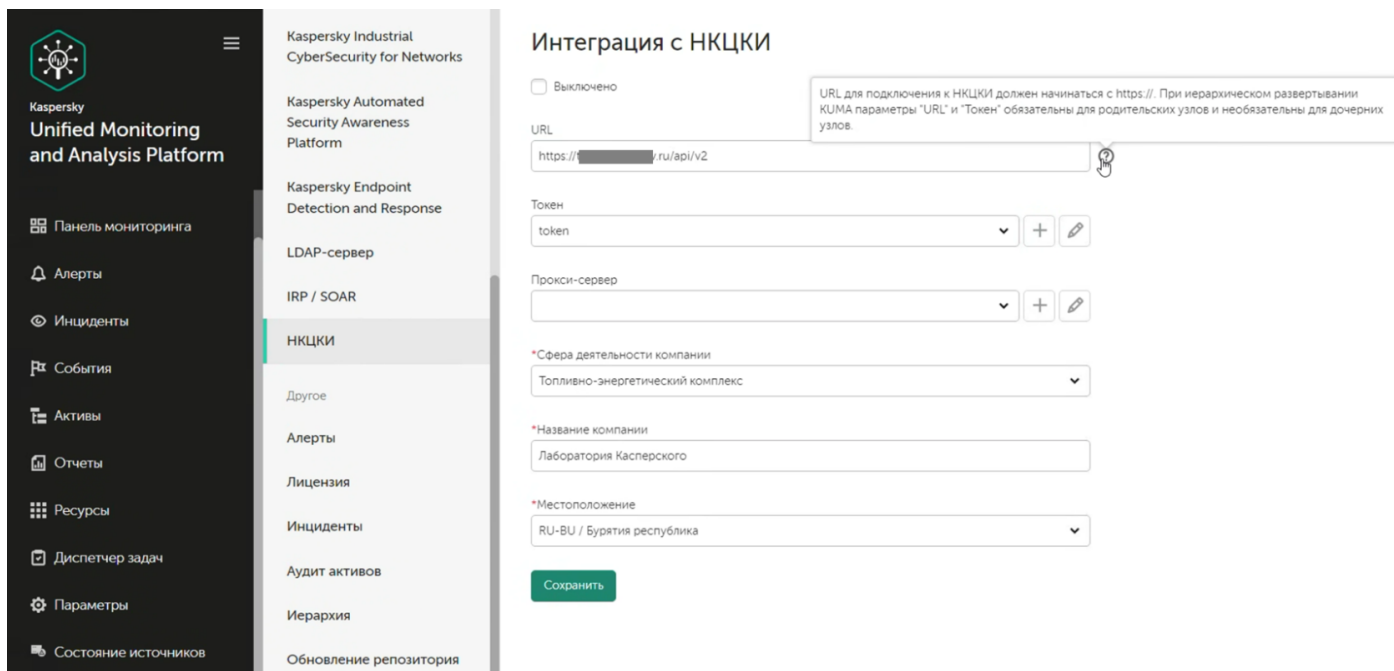
Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/KUMA/2.1/ru-RU/221777.htm>

Настройка интеграции

Для возможности отправки инцидентов в ГосСОПКА должна быть выполнена настройка, в разделе **Параметры - НКЦКИ** нужно указать параметры подключения:

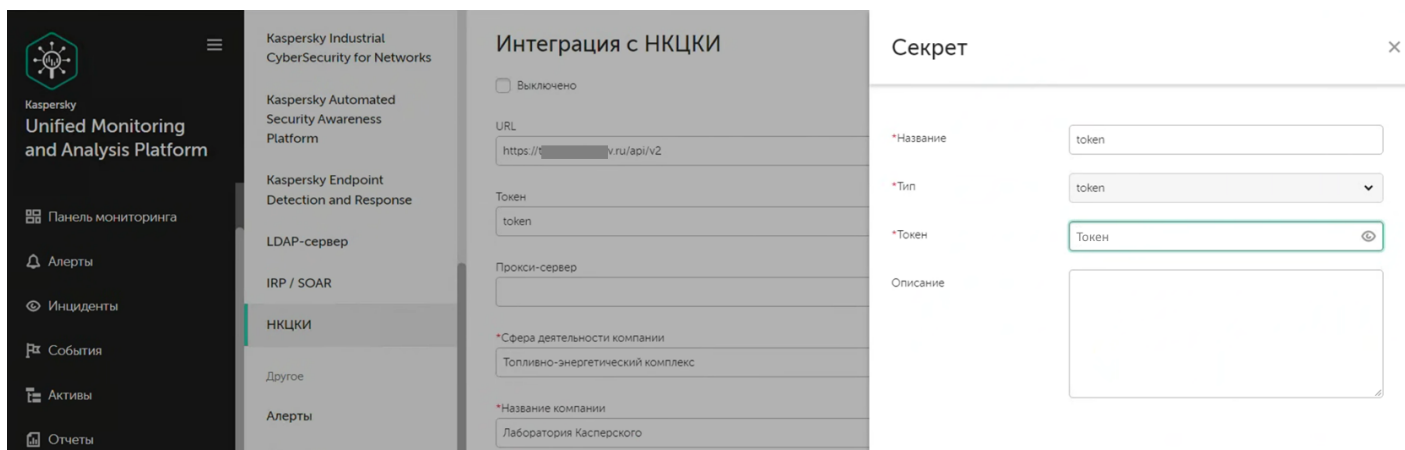
- Укажите URL, по которому доступен НКЦКИ.
- Токен, который был выдан Заказчику для подключения к НКЦКИ.

Далее укажите сферу деятельности, местоположение и название компании.



The screenshot displays the Kaspersky Unified Monitoring and Analysis Platform interface. On the left is a dark sidebar with the Kaspersky logo and a menu containing: Панель мониторинга, Алерты, Инциденты, События, Активы, Отчеты, Ресурсы, Диспетчер задач, Параметры, and Состояние источников. The main content area has a light gray header with 'Kaspersky Industrial CyberSecurity for Networks', 'Kaspersky Automated Security Awareness Platform', 'Kaspersky Endpoint Detection and Response', 'LDAP-сервер', 'IRP / SOAR', and 'НКЦКИ' (highlighted). Below this is a list of items: Другое, Алерты, Лицензия, Инциденты, Аудит активов, Иерархия, and Обновление репозитория. The 'Интеграция с НКЦКИ' section contains a toggle switch (currently 'Выключено'), a URL input field (containing 'https://[redacted]/ru/api/v2'), a Token dropdown (set to 'token'), a Proxy server dropdown, and three required fields: 'Сфера деятельности компании' (set to 'Топливо-энергетический комплекс'), 'Название компании' (set to 'Лаборатория Касперского'), and 'Местоположение' (set to 'RU-BU / Бурятия республика'). A green 'Сохранить' button is at the bottom. A tooltip explains that the URL must start with 'https://' and that 'URL' and 'Token' are mandatory for parent nodes.

Значение токена сохраняется в Секрете в KUMA:




Работа с инцидентом

После настройки взаимодействия с НКЦКИ и работа с инцидентом выполняется в разделе **Инциденты**. Для нового инцидента должны быть заполнены минимально **необходимые поля**:

- категория инцидента;
- тип инцидента;
- описание инцидента.

Описание взаимодействия с НКЦКИ в онлайн-справке:

<https://support.kaspersky.com/KUMA/2.1/ru-RU/221855.htm>



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Инциденты >

incident

Назн

Описание

Связанные алерты

Связанные активы

Связанные пользователи

Журнал изменений

Интеграция с НКЦКИ

Описание

Создан19.01.2023 15:05:38

*Название

incident

*Тенант

Main

Статус

Открыт

*Уровень важности

Средний

Категории затронутых активов

Без категории

Появление первого события

Появление последнего события

Категория инцидента

Уведомление о компьютерном инциде...

Тип инцидента

Несанкционированное разглашение и...

Описание

descr

После нажатия кнопки **Экспорт** открывается вкладка для заполнения карточки инцидента в формате, который требует НКЦКИ. При необходимости может быть выбран чек-бокс «Затронутая система имеет подключение к Интернету», это подразумевает заполнение дополнительных сведений на вкладке Технические данные.

Основные

Дополнительно

Технические данные

*Название компании

Лаборатория Касперского

*Владелец актива

Лаборатория Касперского

*Категория инцидента

Уведомление о компьютерном инциденте

*Тип инцидента

Компрометация учетной записи

*Описание

descr

*TLP

RED



*Дата создания инцидента

19.01.2023 15:05:38

*Статус

Проводятся мероприятия по реагированию

*Название информационной системы

*Категория КИИ системы

Объект КИИ третьей категории значимости



*Сфера деятельности компании

Топливо-энергетический комплекс

*Местоположение

RU-BU / Бурятия республика

☒ Затронутая система имеет подключение к Интернету

Экспорт

Отмена

Отмена

Вкладки Технические данные и Дополнительно не обязательно заполнять для запуска экспорта, но информация будет запрошена со стороны ГосСОПКА позже.

Экспорт в НКЦКИ

Основные

Дополнительно

Технические данные

Средство обнаружения инцидента

Требуется привлечение сил ГосСОПКА

Время завершения инцидента

Влияние на доступность

Влияние на целостность

Влияние на конфиденциальность

Иные последствия

Пород

Экспорт в НКЦКИ

Основные

Дополнительно

Технические данные

Технические сведения об атакованном ресурсе

IPv4-адрес

IPv6-адрес

Доменное имя

URI-адрес

Адрес электронной почты

Атакующий сервис с указанием порта и протокола

Технические сведения о вредоносной системе

IPv4-адрес

IPv6-адрес

Доменное имя

Использованная уязвимость

Подтверждение экспорта инцидента

Инцидент можно экспортировать в НКЦКИ только один раз, но вы можете дополнить инцидент данными, если со стороны НКЦКИ будет соответствующий запрос. Продолжить?

Нет

Да

Вся информация отображается в ЛК Заказчика. При этом в связи с особенностями работы портала перейти из интерфейса KUMA сразу в нужный инцидент в ГосСОПКА нельзя, придется искать в списке всех инцидентов.

>

⊕

ⓘ

🔍

🔗

🗨️

Организация

Лаборатория Касперского

Рег. номер уведомления

INC-23-01-176

Дата и время регистрации [UTC+03:00]

19.01.202315:20:01

▲ Ход обработки уведомления

Статус

Требуется дополнение

Изменить

▼ Общие сведения

▲ Местоположение контролируемого ресурса

Страна/Регион

Республика Бурятия

Населенный пункт или геокоординаты

▲ Общие сведения о контролируемом ресурсе

Наименование

name

Информация о категорировании ОКИИ

Объект КИИ третьей категории значимости

Сфера функционирования

Топливо-энергетический комплекс

☒ Наличие подключения к сети Интернет

▲ Технические сведения об атакованном ресурсе

IPv4-адрес

Нет данных

IPv6-адрес

Нет данных

Доменное имя

В интерфейсе KUMA можно отслеживать статус инцидента и изменения содержимого (если изменения были выполнены на портале, а не из KUMA).

Инциденты > incident

ОписаниеСвязанные алертыСвязанные активыСвязанные пользователиЖурнал измененийИнтеграция с НКЦКИ

Комментарий

Время ↓	Пользователь	Действие
19.01.2023 15:16:53	lega	Инцидент экспортирован в НКЦКИ. INC-23-01-176 (id:333566-3c72-49a2-ada1-0bc8b6aeeb7e0)
19.01.2023 15:11:30	lega	Тип инцидента изменен на Компрометация учетной записи
19.01.2023 15:10:20	lega	Тип инцидента изменен на
19.01.2023 15:06:21	lega	Тип инцидента изменен на несанкционированное разглашение информации

Интеграция с НКЦКИ

Статус уведомления в НКЦКИСоздано

Регистрационный номерожидается получение

Сравнение инцидента KUMA с данными в НКЦКИ

ЧатФайлы

Пусто

Комментировать

НазваниеСравнение инцидента KUMA с данными в НКЦКИ

ОсновныеДополнительноТехнические данные

Если данные НКЦКИ и KUMA различаются, вариант НКЦКИ отображается под полем, значения которого не сходятся.

*Название компанииЛаборатория Касперского

*Владелец активаЛаборатория Касперского

*Категория инцидентаУведомление о компьютерном инциденте

*Тип инцидентаКомпрометация учетной записи

*Описаниеdesc

*TLPAMBER

*Дата создания инцидента19.01.2023 15:05:38

*СтатусПроводятся мероприятия по реагированию

*Название информационной системыname

Параллельно в НКЦКИОтмена

При получении обратной связи статус инцидента изменяется, при необходимости инцидент можно дополнить данными

Есть чат с НКЦКИ (не онлайн, примерно раз в 10 минут – особенности на стороне НКЦКИ).

Время ↓	Пользователь	Действие
19.01.2023 15:19:44	KUMA	К инциденту в НКЦКИ добавлен комментарий
19.01.2023 15:19:09	KUMA	Инцидент обновлен в НКЦКИ. Поле Время обновления. Тип обновления update
19.01.2023 15:19:09	KUMA	Инцидент обновлен в НКЦКИ. Поле regnumber. Тип обновления update
19.01.2023 15:19:09	KUMA	Инцидент обновлен в НКЦКИ. Поле Статус. Тип обновления update
19.01.2023 15:16:57	KUMA	Инцидент обновлен в НКЦКИ. Поле Время обновления. Тип обновления update
19.01.2023 15:16:57	KUMA	Инцидент обновлен в НКЦКИ. Поле Статус. Тип обновления update

Интеграция с НКЦКИ

Статус уведомления в НКЦКИТребуется дополнение

Регистрационный номерINC-23-01-176

Экспорт в НКЦКИ

ЧатФайлы

ТИ НКЦКИ 19.01.2023 15:20:22

Внесите в уведомление (группа полей «технические сведения об атакуемом/атакующем объектах») INC-23-01-176 технические сведения о событии информационной безопасности и поменяйте статус данного уведомления с «Требуется дополнение» на «Проверка НКЦКИ». После этого отслеживайте состояние и ход информационного взаимодействия по уведомлению INC-23-01-176 в блоке «Комментарии».

ТИ НКЦКИ 19.01.2023 15:20:25

Уведомление о компьютерном инциденте (Компрометация учетной записи) присвоен рег. номер: INC-23-01-176 (дата регистрации: 2023-01-19T15:20:01+03:00). В случае необходимости взаимодействия с НКЦКИ по данному уведомлению по альтернативным каналам связи (почта, телефон) просим использовать этот рег. номер.

Есть возможность оповещений по почте о необходимости доработки инцидента.

KUMA: Требуется дополнение инцидента "inc5" для НКЦКИ

kuma@domain.com

Отправлено: Пн 16.01.2023 18:02

Кому: siem@domain.com

Здравствуйте!

Статус инцидента "inc5" изменен в НКЦКИ на "Требуется дополнение".

Подробнее об инциденте можно узнать в веб-интерфейсе KUMA:

<https://kuma.domain.com:7220/incidents/INC-5>.

Автоматическое уведомление Kaspersky Unified Monitoring and Analysis Platform

Revision #2

Created 28 November 2023 14:49:22 by Boris RZR

Updated 3 February 2025 07:59:53 by Koala