


Где брать SOC Package и другой официальный контент?

Начиная с версии KUMA 2.1 контент от Лаборатории Касперского (правила корреляции, нормализаторы, коннекторы и т.п.) публикуются в репозитории ЛК:
<https://support.kaspersky.com/help/KUMA/3.2/ru-RU/242817.htm>

Как получить SOC Package и другой коробочный контент?

1. В Web-интерфейсе KUMA нужно настроить интеграцию с репозиторием



Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры 1

Состояние источников

Метрики

Анализ угроз

Kaspersky Threat Lookup

Kaspersky CyberTrace

Интеграции

Kaspersky Security Center

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Automated Security Awareness Platform

Kaspersky Endpoint Detection and Response

LDAP-сервер

IRP / SOAR

НКЦКИ

Другое

Алерты

Лицензия

Инциденты

Аудит активов

Обновление репозитория 2


Активы

Обновление репозитория

☐ Отключить автоматическое обновление

Интервал обновления в часах
24

Последнее обновление: 08.07.2024 16:49:04

 Запланированное обновление: 09.07.2024 16:49:04

Общее количество пакетов: 100

Общее количество ресурсов во всех пакетах: 2881

Запустить обновление

Источник обновления*

Серверы обновления "Лаборатории Касперского"

Адреса электронной почты для рассылки уведомлений

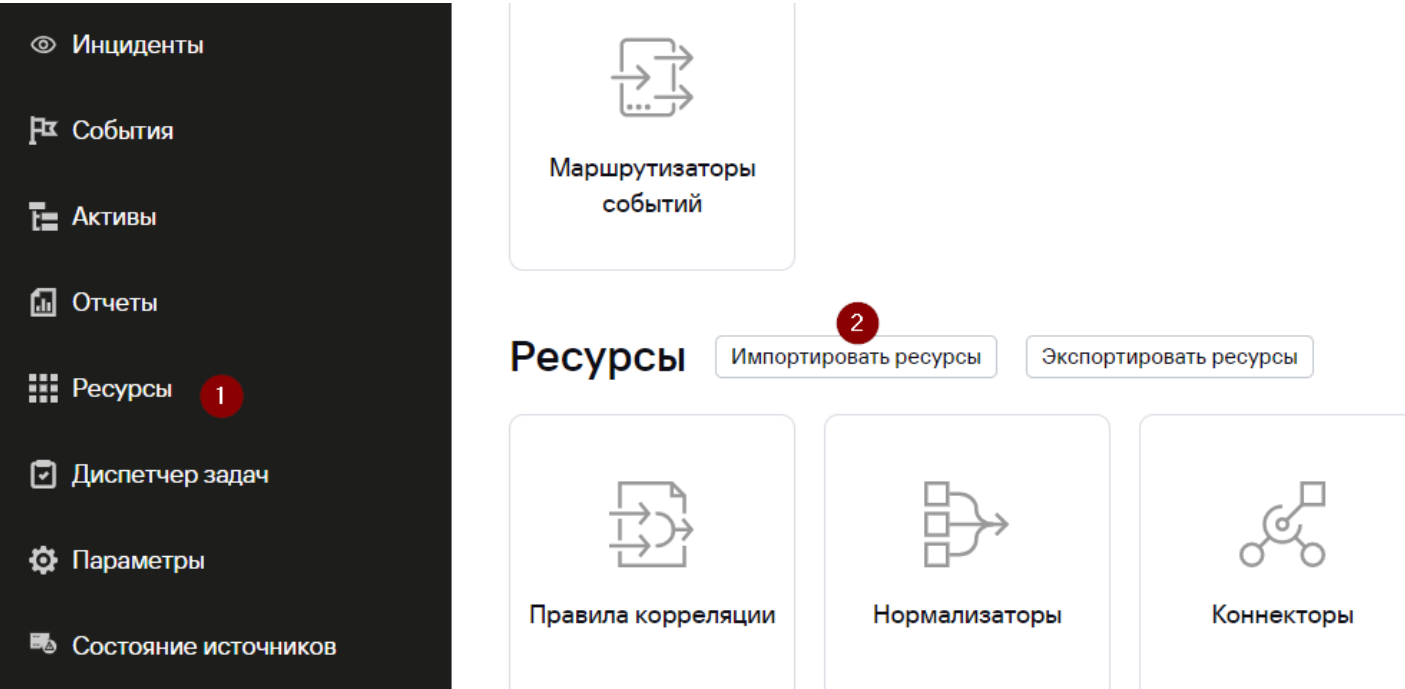
+ Добавить

Сохранить

Список серверов, до которых нужно предоставить доступ с KUMA представлен в официальной документации: <https://support.kaspersky.ru/common/start/6105>

Для обновления напрямую с репозитория **НЕЛЬЗЯ** использовать Proxu. Если для доступа к репозиторию требуется использование Proxu или у KUMA нет доступа в Интернет напрямую, то следует использовать Kaspersky Update Utility (KUU). Подробнее в статье: <https://kb.kuma-community.ru/books/ustanovka-i-obnovlenie/page/obnovlenie-resursov-s-pomoshhiu-kaspersky-update-utility-kuu>

2. После настройки интеграции с репозиторием и Запуска обновления перейдите в Ресурсы и выберите Импортировать ресурсы



3. Далее выберите Репозиторий в качестве источника

Импорт ресурсов

Подробнее об экспорте и импорте ресурсов смотрите [в онлайн-справке](#).

Тенант*

Main

Источник импорта*

Репозиторий

Пакеты репозитория

Вы можете запустить обновление в разделе [Обновление репозитория](#).

После импорта ресурсов требуется перезапустить использующие их сервисы, а также проверить наборы ресурсов, если вы их меняли.

⌚

Последнее обновление: 08.07.2024 16:49:04.

<input type="checkbox"/>	Название	Дата выпуска	Версия	Установленная версия	Количество ресурсов
<input type="checkbox"/>	[OOTB] Cisco ASA and IOS syslog	05.07.2024 15:37:27	3	2	1
<input type="checkbox"/>	[OOTB] SecurityCode Continent 4 ...	02.07.2024 13:09:28	2	1	2
<input type="checkbox"/>	[OOTB] Extreme Networks Summit...	01.07.2024 16:16:14	1	Не установлен	1
<input type="checkbox"/>	[OOTB] Kaspersky Security for MS ...	27.06.2024 13:55:57	1	Не установлен	3
<input type="checkbox"/>	[OOTB] Aruba Aruba AOS-S syslog	25.06.2024 17:31:38	1	Не установлен	1

4. Нажав на имя конкретного пакета, вы увидите информацию о пакете, журнал изменений и перечень импортируемых ресурсов.

Информация о пакете

Информация о пакете



О пакете >

Журнал изменений ▾

[OOTB] Cisco ASA and IOS syslog. Version 3

Change list:

- New extra normalizer was added "DHCP_SNOOPING".
- New extra normalizer was added "SEC".
- In the extra normalizer "113004" was added new regular expression.
- In the extra normalizer "SSH2_SESSION" was added new regular expression.
- In the extra normalizer "SSH2_USERAUTH" was added new regular expression.
- New conditions were added to the extra normalizer "SSH".
- New event mapping was added to the extra normalizer "717022". Event field "SN" was mapped to the KUMA field DeviceCustomString2, event field "email" was mapped to the KUMA field DeviceCustomString3, event field "cn" was mapped to the KUMA field SourceUserName. Mapping was removed from the KUMA field FlexString1.
- Event enrichment with constants to the DeviceCustom*label fields was removed in the extra normalizers: 106011, 111008, 111010, 113003, 113004, 113009, 113011, 113019, 210022, 302010, 303002, 313001, 313009, 502103, 602101, 606001, 606002, 711004, 716059, 717016, 717022, 717028, 717053, 720036, 720038, 720044, 720068, 720073, 721016, 721018, 722010, 722011, 722012, 722022, 722032, 722035, 722036, 722041, 722051, 722053, 722055, 733100, 734001, 737003, 737006, 737016, 737026, 737029, 737031, 737034.

[OOTB] Cisco ASA and IOS syslog. Version 2

Change list:

- Support of event parsing from generated by Cisco Firepower Threat Defense (version 7.2) was added.
- New extra normalizers were added: 106016, 106017, 109201, 109207, 109210, 111009, 113015, 113028, 113034, 199016, 199017, 199018, 305006, 317077, 317078, 321006, 419003, 430002, 430003, 500003, 710006, 716039, 716047, 716603, 717025, 717029, 717030, 717036, 717038, 722029, 722030, 722031, 725004, 725008, 725010, 725011, 725012, 725014, 725017, 725021, 725022, 725023, 725024, 734002, 734003, 734004, 737001, 737035, 737200, 737201, 737400, 737401, 746012, 746013, 771002, 815004, 852001, 852002, 6414004.

[OOTB] Cisco ASA and IOS syslog. Version 1

Change list:

- Regular expressions in the extra normalizers "302013", "for302014", "302015", "302016" was fixed. Event field mapping was updated.
- Extra normalizer "ASA" was changed. Event enrichment for the field DeviceDirection was added (replace "outbound" with "0" and replace "inbound" with "1").
- Normalizer name was changed to "[OOTB] Cisco ASA and IOS syslog".
- Other minor improvements.

Будут импортированы следующие ресурсы: ▾

☐ Все ресурсы

☐ Нормализаторы

☐ KUMA Packages

☐ OOTB

☐ [OOTB] Cisco ASA and IOS syslog

5. Для импорта интересующих ресурсов выберите один или несколько пакетов галочкой слева от имени пакета и нажмите Импортировать внизу окна

Импорт ресурсов

Подробнее об экспорте и импорте ресурсов смотрите [в онлайн-справке](#).

Тенант*

Main

Источник импорта*

Репозиторий

Пакеты репозитория

Вы можете запустить обновление в разделе [Обновление репозитория](#). После импорта ресурсов требуется перезапустить использующие их сервисы, а также проверить наборы ресурсов, если вы их меняли.

<div><div></div></div>	Название	Дата выпуска	
1	<input checked="" type="checkbox"/> [OOTB] Cisco ASA and IOS syslog	05.07.2024 15:37:27	
	<input type="checkbox"/> [OOTB] SecurityCode Continent 4 ...	02.07.2024 13:09:28	
	<input type="checkbox"/> [OOTB] Extreme Networks Summit...	01.07.2024 16:16:14	
	<input type="checkbox"/> [OOTB] Kaspersky Security for MS ...	27.06.2024 13:55:57	
	<input type="checkbox"/> [OOTB] Aruba Aruba AOS-S syslog	25.06.2024 17:31:38	
	<input type="checkbox"/> [OOTB] Arbor Pravail syslog	25.06.2024 13:58:47	
	<input type="checkbox"/> [OOTB] Huawei VRP syslog	20.06.2024 15:02:46	
	<input type="checkbox"/> [OOTB] Garda Monitor syslog	19.06.2024 12:25:46	
	<input type="checkbox"/> [OOTB] Tionix Cloud Platform syslog	18.06.2024 10:52:21	
	<input type="checkbox"/> [OOTB] Avast IDN syslog	17.06.2024 16:05:18	
	<input type="checkbox"/> [OOTB] Avast FAM syslog	17.06.2024 11:11:57	
	<input type="checkbox"/> [OOTB] Zecurion DLP syslog	17.06.2024 10:33:41	
	<input type="checkbox"/> [OOTB] ...	05.07.2024 14:47:21	

2

Импортировать

Отмена

6. Выбранные ресурсы будут импортированы.

Где взять описание правил из SOC Package?

Описание правил из SOC Package можно скачать из официальной документации:
<https://support.kaspersky.com/help/KUMA/3.2/ru-RU/250594.htm>

Правила корреляции

В файле, доступном по ссылке для скачивания, описаны правила корреляции, включенные в поставку Kaspersky Unified Monitoring and Analysis Platform версии 3.2. Приводятся сценарии, покрываемые правилами, условия их использования и необходимые источники событий.

Описанные в этом документе правила корреляции содержатся в файле SOC_package дистрибутива KUMA и защищены паролем SOC_package1. Одновременно возможно использование только одной версии набора SOC-правил: или русской, или английской.

Правила корреляции можно импортировать в KUMA. См. раздел онлайн-справки "Импорт ресурсов":
<https://support.kaspersky.com/KUMA/3.2/ru-RU/242787.htm>.

Импортированные правила корреляции можно добавлять в используемые вашей организацией корреляторы. См. раздел онлайн-справки "Шаг 3. Корреляция": <https://support.kaspersky.com/KUMA/3.2/ru-RU/221168.htm>.

[Скачать Описание правил корреляции, содержащихся в SOC_package.xlsx](#)



Где взять мапинг коробочных нормализаторов?

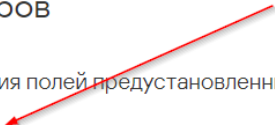
Сопоставление полей коробочных нормализаторов можно скачать из официальной документации: <https://support.kaspersky.com/help/KUMA/3.2/ru-RU/267237.htm>

Приложения > Сопоставление полей предустановленных нормализаторов

Сопоставление полей предустановленных нормализаторов

В файле, доступном по ссылке для скачивания, представлено описание сопоставления полей предустановленных нормализаторов.

[Скачать Описание сопоставления полей предустановленных нормализаторов.ZIP](#)



Revision #4

Created 8 July 2024 14:03:27 by Koala

Updated 8 July 2024 14:37:19 by Koala