

???????????? ???? KSMG
???????? ?? ??????????,
????????? ? ??????????

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

Для нормализации событий KSMG в KUMA применяется нормализатор [OOTB] KSMG 2.1+ syslog CEF

???????????? ???? KSMG

Хранилище предназначено для хранения поступающих почтовых сообщений перед их обработкой модулями KSMG. В случае если почтовое сообщение будет отклонено или удалено в результате работы одного из модулей KSMG, аналитик может получить доступ к оригинальному почтовому сообщению в Хранилище.

Для сохранения оригинала сообщения в Хранилище в параметрах модуля KSMG должен быть активирован параметр **Поместить исходное сообщение в Хранилище**. Сообщения помещаются в Хранилище вместе с вложениями.

Просмотреть правило

Создать копию

Удалить

Общие

Информация о правиле

Отправители и получатели

Модули проверки

AV Антивирус

LS Проверка ссылок

AS Анти-Спам

AP **Анти-Фишинг** 1

CF Контентная фильтрация

MA Проверка подлинности

KT Защита KATA

CD Обезвреживание
содержимого

Дополнительные параметры

Скрытая копия

Действия над заголовками

Примечание к сообщению

Анти-Фишинг

Статус Вкл

Если обнаружен фишинг

Действие Отклонить ⓘ

Поместить исходное
сообщение в Хранилище ⓘ Включено 2

Добавить в тему сообщения
следующий текст [Phishing]

Предупреждения и примечания ⓘ

Статус Выкл

Шаблон —

Уведомления

Уведомления не настроены

????????? ?????????? ?????????????? ? KUMA

Чтобы настроить обогащение событий KSMG ссылкой на почтовое сообщение, помещенное в Хранилище KSMG, создайте правило обогащения:

- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы ? Правила обогащения**.
- Нажмите на кнопку **Создать**.
- В появившемся окне **Создание правила обогащения**:
 - В поле **Название** введите уникальное имя правила.
 - В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.
 - В раскрывающемся списке **Тип источника данных** выберите шаблон.
 - В поле **Шаблон** укажите следующий шаблон ссылки:

```
https://{{.DeviceAddress}}/ru_RU/#/backup?filter=[{"field":"smtp_message_id","condition":"CONTAIN", "value":"{{.DeviceCustomString1}}"]}]
```

- В поле **Целевое поле** укажите **DeviceExternalID**.
- Опционально добавьте **Описание**.
- В секции **Параметры фильтра** укажите условия определения событий KSMG, в которые будет добавляться ссылка. Переключитесь на **Код** и укажите следующее условие:

```
Name = 'message backup result'  
OR (  
S.BackupResult = 'BackedUp'  
AND  
Name = 'message result'  
)
```

- Нажмите **Создать**.

Создание правила обогащения

Название* [PoC] KSMG Backup Link 1

Тенант* Main 2

Тип источника данных* шаблон 3

Шаблон* `https://{{.DeviceAddress}}/ru_RU/#/backup?filter=[{"field": "smtp_message_id", "condition": "CONTAIN", "value": "{{.DeviceCustomString1}}"]` 4

Целевое поле* DeviceExternalID 5

Отладка

Теги

Описание
 Хранилище. Гиперссылка размещается в поле DeviceExternalID.
 This enrichment rule is used to add to KSMG events hyperlink to the message stored in Backup. The hyperlink is placed in the DeviceExternalID field. 6

Параметры фильтра

Фильтр Создать

Сохранить фильтр

Конструктор </> Код

ИЛИ ▾ + Добавить условие + Добавить группу

- Если e: Name = message backup result ×
- И ▾ + Добавить условие + Добавить группу × 7
 - Если e: S.BackupResult = BackedUp ×
 - Если e: Name = message result ×

8

Создать Сохранить с комментарием Отмена

Далее созданное правило обогащения необходимо применить в Коллекторе для приема и обработки событий KSMG.

????????????? ?????????? ?????????????? ?
?????????????? KSMG

Чтобы добавить созданное правило обогащения в Коллекторе для приема и обработки событий KSMG:

- Перейдите в раздел **Ресурсы ? Активные сервисы.**
- Выберите **Коллектор**, который используется для приема и обработки событий KSMG.

Ресурсы и сервисы / Сервисы

Сервисы

Статус	Тип	Сервис	Версия	Тенант	Полное доменное имя	IP-адрес	Порт API	Время работы	Создан
<input checked="" type="checkbox"/>	Коллектор	KSMG (TCP/5916) 1	4.0.213	Main	kuma.demo.lab		7234	2 месяца 29 дня 5 часа 54 минуты 17 секунды	13.12.2023 13:16:45

- В окне **Редактирование коллектора** перейдите на шаг **Обогащение событий** и нажмите **Добавить обогащение.**
- В поле **Правило обогащения** выберите ранее созданное правило обогащения.

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий **1**

Маршрутизация

Проверка параметров

Правило обогащения
[PoC] KSMG Backup Link **2**

Тип источника данных* шаблон

Шаблон*

```
https://{{.DeviceAddress}}/ru_RU/#/backup?filter=[{"field": "smtp_message_id", "condition": "CONTAIN", "value": "{{.DeviceCustomString1}}"]
```

Целевое поле* DeviceExternalID

Отладка

Параметры фильтра

Фильтр Создать

Сохранить фильтр

Конструктор </> Код

ИЛИ + Добавить условие + Добавить группу

Если e: Name = message backup result

И + Добавить условие + Добавить группу

Если e: S.BackupResult = BackedUp

Если e: Name = message result

+ Добавить обогащение

Сохранить
Сохранить с комментарием
Отмена

- Перейдите на шаг **Проверка параметров** и нажмите **Сохранить и обновить параметры сервисов.**

- Нажмите **Сохранить**.

Редактирование коллектора



Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров **1**

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

Сохранить и создать сервис

Сервисы, использующие этот коллектор

Тип	Название
коллектор	KSMG (TCP/5516)

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов **2**

3

Сохранить

Сохранить с комментарием

Отмена

????????? ?????????? ? ?????????????? KSMG ??
?????????? ?????????? KUMA

- В разделе **События** выполните поиск событий типа **message backup result** или **message result**

```
SELECT *  
FROM `events`  
WHERE Name = 'message backup result' AND DeviceProduct = 'KSMG'  
ORDER BY Timestamp DESC  
LIMIT 250
```

ИЛИ

```
SELECT *
FROM `events`
WHERE Name = 'message result' AND DeviceProduct = 'KSMG'
ORDER BY Timestamp DESC
LIMIT 250
```

- Откройте карточку события и убедитесь, что в поле **DeviceExternalID** появилась ссылка для перехода в Хранилище KSMG.

- Выполните переход по ссылке.

DeviceExternalID	<a field":"smtp_message_id","condition":"contain","value":"44569.6137353195-sendemail@kali-attacker"}]"="" href="https://10.68.85.65/ru_RU/#/backup?filter=[{">https://10.68.85.65/ru_RU/#/backup?filter=[{"field":"smtp_message_id","condition":"CONTAIN","value":"44569.6137353195-sendEmail@kali-attacker"}]
DeviceFacility	18
DeviceHostName	ksmg01
DeviceProcessName	ksmg

Показать информацию из Threat Lookup

Добавить в Internal TI в CyberTrace

Перейти по ссылке **1**

- В результате будет выполнен переход в Хранилище KSMG с фильтром по сообщению — будет отображаться только то почтовое сообщение, результаты анализа которого представлены в карточке события KUMA.

Хранилище

Исходные сообщения Очередь на повторную проверку

Перед обработкой сообщения электронной почты модулями проверки приложение сохраняет исходное сообщение в Хранилище, если эта опция настроена в параметрах правила. Сообщения, помещенные в Хранилище, могут быть небезопасны.

Отправить Удалить Количество сообщений: 1

Эмэй отправителя	Эмэй получателя	Тема	Технологии обнаружения	Размер сообщения	Вложения	Время получения	UUID сообщения	Отправка из Хранилища
attacker@fakeste.com	ivan@demo.lab	Блокировка учетной записи	AV LS ARP AS CF MA KT CP	1.05 КБ	0	01.06.2026 16:48:47	019E8371-B4D3-70B9-8019-E17FF0575BDD	● Не отправилось

UUID: Сообщения, как в заголовке события KUMA

- Далее аналитик в интерфейсе KSMG может:
 - Просмотреть свойства сообщения (причину блокировки сообщения, данные отправителя, сработавшие правила).

Просмотреть информацию о сообщении



Искать связанные события Скачать ▾

1

Свойства сообщения Предпросмотр История отправки из Хранилища Очередь на повторную проверку

Причина	AP Анти-Фишинг 2
App ID сообщения	1890
Тема	Блокировка учетной записи
Email отправителя	attacker@fakesite.com 3
IP отправителя	192.168.1.1 4
Получено	01.06.2026 16:48:47
Узел	192.168.1.1:9045
SMTP Message-ID	<44569.6137353195-sendEmail@kali-attacker>
UUID сообщения	019E8371-B4D3-70B9-809B-E17FF0575BDD
Отправка из Хранилища	Не отправлялось
Вложения	—

Сработавшие правила

Borisov Link Test

Email получателя	ivan@demo.lab 5
CC	—
BCC	—
Действие	Отклонено 6
Причина	AP Анти-Фишинг 7
Результат проверки 8	
AV Антивирус	Не проверено (Отключено в параметрах защиты)

Отправить ▾

Закрыть

Удалить

- Выполнить предпросмотр сообщения, чтобы ознакомиться с оригинальным текстом сообщения.

Просмотреть информацию о сообщении



Искать связанные события

Скачать

1

Свойства сообщения

Предпросмотр

История отправки из Хранилища

Очередь на повторную проверку

Блокировка учетной записи

01.06.2026 16:48:47

2

Обычный текст

Исходное

HTML

Показать внешнее содержимое и ссылки

Received: from kali-attacker (unknown [192.168.1.1])
by [redacted] (Postfix) with ESMTP
for <ivan@demo.lab>; Mon, 1 Jun 2026 16:48:47 +0300 (MSK)
Message-ID: <44569.6137353195-sendEmail@kali-attacker>
From: "attacker@fakesite.com" <attacker@fakesite.com>
To: "ivan@demo.lab" <ivan@demo.lab>
Subject: Блокировка учетной записи
Date: Mon, 1 Jun 2026 13:48:47 +0000
X-Mailer: sendEmail-1.56
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----MIME delimiter for sendEmail-155954.272559942"

This is a multi-part message in MIME format. To properly display this message you need a MIME-Version 1.0 compliant Email program.

-----MIME delimiter for sendEmail-155954.272559942

Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

Ваша учетная запись заблокирована, перейдите по ссылке для восстановления:
<https://www.amtso.org/check-desktop-phishing-page/>

-----MIME delimiter for sendEmail-155954.272559942--

Отправить

Закреть

Удалить

- Скачать сообщение в формате eml.
- Выполнить отpravку сообщения пользователю в случае False Positive или отправить на повторную проверку.

Просмотреть информацию о сообщении



Искать связанные события Скачать ▾

Свойства сообщения Предпросмотр История отправки из Хранилища Очередь на повторную проверку

Причина	AP Анти-Фишинг
App ID сообщения	1890
Тема	Блокировка учетной записи
Email отправителя	attacker@fakesite.com
IP отправителя	██████████
Получено	01.06.2026 16:48:47
Узел	██████████ 9045
SMTP Message-ID	<44569.6137353195-sendEmail@kali-attacker>
UUID сообщения	019E8371-B4D3-70B9-809B-E17FF0575BDD
Отправка из Хранилища	Не отправлялось
Вложения	—

Сработавшие правила

Borisov Link Test

Email получателя	ivan@demo.lab
CC	—
BCC	—
Действие	Отклонено
Причина	AP Анти-Фишинг

Результат проверки

Не проверено (Отключено в параметрах защиты)

Отправить

Повторно проверить и отправить

Отправить Закрыть

Удалить

Revision #8

Created 2026-05-29 15:07:49 UTC by Dmitry Borisov

Updated 2026-06-01 14:52:09 UTC by Dmitry Borisov