

Создание ТАА-алертов в KUMA с KATA

Введение

При отправке событий из KATA в KUMA есть известная проблема: KATA отправляет сообщение о ТАА-сработке только при первой сработке на хосте, а само Syslog сообщение не содержит достаточной информации. События из телеметрии KEDR в свою очередь не содержат идентификатора алерта в KATA в связи с чем отсутствует возможность создания ссылки на карточку алерта в KATA.

В этой статье представлен вариант решения этой проблемы, который позволяет создавать алерт в KUMA идентичный ТАА-алерту в KATA, со всеми связанными событиями телеметрии.

Требования

Для работы метода требуется установленная KUMA версии 2.1 или выше, а также KATA версии 5.0 или выше.

На KUMA должна быть настроены коллекторы для приема Syslog сообщений от [KATA](#) и телеметрии от [KEDR](#). Информацию по настройке данных источников можно найти в соответствующих статьях (ссылки приведены для последних версий).

Оба коллектора должны отправлять события в коррелятор.

Реализация

1. Загрузить пакет ресурсов по ссылке: https://github.com/KUMA-Community/kuma_taa_alert
2. Импортировать все ресурсы из пакета в KUMA.
3. Перейти в Коррелятор, перейти на шаг Корреляция и привязать правила корреляции D007 и D008

Редактирование коррелятора

Общие

Глобальные переменные

Корреляция

Обогащение

Реагирование

Маршрутизация

Корреляция

С помощью правил корреляции задаются условия, по которым анализируются поступающие события и, если выполняются условия правил, создаются обнаружения. Подробнее см. [в онл справке](#).

+ Добавить

Привязать

Удалить

↑ Поднять

↓ Опустить

<input type="checkbox"/>	Правила корреляции	Тип
<input type="checkbox"/>	D007;KATA;Send alert info to active list	operational
<input type="checkbox"/>	D008;KEDR,KATA;TAA-detect telemetry	simple

4. Перейти на шаг Проверка параметров и обновить параметры сервиса коррелятора

Редактирование коррелятора

Общие

Глобальные переменные

Корреляция

Обогащение

Реагирование

Маршрутизация

Проверка параметров

Проверка параметров

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

Чтобы начать коррелировать события, сервис этого коррелятора необходимо установить на сервере, предназначенном для обработки 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 коррелятор

Тип	Название
correlator	Correlator

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

5. Перейти в веб-интерфейсе в Параметры -> Алерты -> Сегментация и нажать Добавить параметры для нового тенанта (если в KUMA не настроены никакие правила сегментации), либо нажать на соответствующий тенант в списке (если в KUMA уже настроены какие-либо правила сегментации).



Unified Monitoring and Analysis Platform

Выбрано тенантов: 2

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры

Состояние источников

Доменная аутентификация

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

Параметры алертов по тенантам

Сегментация

Добавить параметры для нового тенанта

Удалить

<input type="checkbox"/>	Тенант	Обновлено ↓
<input type="checkbox"/>	Main	26.01.2024 13:10:04

6. Создайте связь правила корреляции и правила сегментации как на рисунке ниже:

Изменить связь правила сегментации ×

Тенанты и правила корреляции*

[-] Main

[-] DEMO

[-] ENG

- ☐ D001: [KATA] Malicious email attachment detected
- ☐ D004: KATA Malicious email attachment detected
- ☐ D002: KATA, TAA detected
- ☐ D003: [APT] Amazon AWS APT URL is blocked
- ☐ D005: [APT] Amazon AWS APT URL
- ☐ D006: [Windows] Successful attempt to log in using administrator account
- ☐ D007: [Windows] Attempt to log in using blocked user
- ☐ D007: KATA, alert info to action list
- ☒ D008: KEDR, KATA, TAA-detect telemetry
- ☐ D009: KATA, Multiple TAA-detects on single host
- ☐ D001: [KATA] Cybercrime response center is blocked
- ☐ D001: [KATA] Cybercrime response center is blocked
- ☐ D002: KATA Cybercrime TAA-detect
- ☐ D003: [APT] Cybercrime APT URL
- ☐ D004: [APT] Cybercrime APT URL
- ☐ D005: [Windows] Successful attempt to log in using administrator account
- ☐ D006: [Windows] Attempt to log in using blocked user
- ☐ D007: KATA, alert info to action list

[+] KUMA Packages

☐ Successful BlockForce

Правило сегментации*

KATA telemetry segmentation rule



Сохранить

7. Сохраните все внесенные изменения.

На этом настройка завершена.

Результат

В результате проделанных манипуляций в KUMA на каждую TAA сработку будет возводиться алерт, в который согласно правилу сегментации будут добавляться все события телеметрии связанные с данной сработкой. Сам алерт будет содержать ID алерта KATA, ссылку на алерт KATA (для этого необходимо на коллекторе для сбора Syslog с KATA добавить обогащение **[OOTB] KATA alert**), а также связанные события телеметрии от KEDR.

Ниже представлен скриншот алерта в KUMA

Алерты >

D008:KEDR.KATA:TAA-detect telemetry (KATA Alert #88548) Новый

Уровень важности: Средний

Назначить: Не назначено

Закреть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции: Средний

Первое появление: 20.05.2024 16:37:58

Наивысшая важность категории активов: Низкий

Последнее появление: 20.05.2024 16:37:58

Идентификатор алерта: c457913d-1122-48e6-91c0-35c0c46e36e7

Тенант: Main

Правило корреляции: D008:KEDR.KATA:TAA-detect telemetry

Связанные события

Время ↓	Информация о событии	Тенант
20.05.2024 16:37:58	DeviceAddress: 10.10.10.10, DeviceHostName: pc-4 demo.lab, DevicePayloadID: powershell_download_and_execute, Message: Событие телеметрии, связанное с алертом KATA #88548, DeviceExternalID: https://10.10.10.10:8443/katap/#/alerts?id=88548, EventOutcome: 88548	Main
20.05.2024 16:37:55	StartTime: 20.05.2024 16:41:10, EndTime: 20.05.2024 16:41:19, Message: Process C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe on pc-4 demo.lab, DeviceAddress: 10.10.10.10, DeviceAssetID: d97f9529-b744-404a-9e53-159923fba9cf, DeviceDnsDomain: demo.lab, DeviceEventCategory: process, DeviceExternalID: windows, DeviceHostName: pc-4 demo.lab, DevicePayloadID: powershell_download_and_execute	Main
Найти в событиях: 1		Main
20.05.2024 16:37:58	DeviceAddress: 10.10.10.10, DeviceHostName: pc-4 demo.lab, DevicePayloadID: powershell_download_and_execute, Message: Событие телеметрии, связанное с алертом KATA #88548, DeviceExternalID: https://10.10.10.10:8443/katap/#/alerts?id=88548, EventOutcome: 88548	Main

Информация о событии

TenantName	Main
Timestamp	20.05.2024 16:37:55 213
Name	Process
StartTime	20.05.2024 16:41:10 666
EndTime	20.05.2024 16:41:19 699
Message	Process C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe on pc-4 demo.lab
DeviceAddress	10.10.10.10
DeviceAssetID	PC-4
DeviceDnsDomain	demo.lab
DeviceEventCategory	process
DeviceExternalID	windows
DeviceHostName	pc-4 demo.lab
DevicePayloadID	powershell_download_and_execute
DeviceProduct	EDR
DeviceReceiptTime	20.05.2024 16:41:19 699
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
DeviceVersion	Microsoft Windows 10 Pro
SourceNTDomain	DEMO
SourceProcessID	9308
SourceProcessName	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n "C:\Users\bob\Downloads\doc2.docm" /o ""
SourceUserName	bob
SourceUserPrivileges	admin

А также соответствующий алерт в KATA

All alerts > Event details #88548 ☆

State: Closed

Importance: Medium

Data source: ENDPOINT (2024-05-20 16:41:25)

Time created: 2024-05-20 16:41:25

Time updated: 2024-05-20 16:41:28

Scan results

TAA powershell_download_and_execute

Hosts

Host name	IP	Number of events
pc-4 demo.lab	10.10.10.10	2

И связанные с ним события телеметрии

Threat Hunting

IOAId = "b85fdcf0-69a9-0a64-4daa-3d5dfbbc70ea" AND Host = "pc-4.demo.lab"

Refresh

All events (2 events) 

Event time ↑	Event type	Host name	Details
2024-05-20 16:41:25.150	Process started	pc-4.demo.lab	File: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Importance: High Hash: SHA256 MD5
2024-05-20 16:41:10.667	Process started	pc-4.demo.lab	File: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Importance: High Hash: SHA256 MD5

Revision #3
Created 30 May 2024 11:18:01 by Koala
Updated 19 July 2024 14:37:44 by Koala