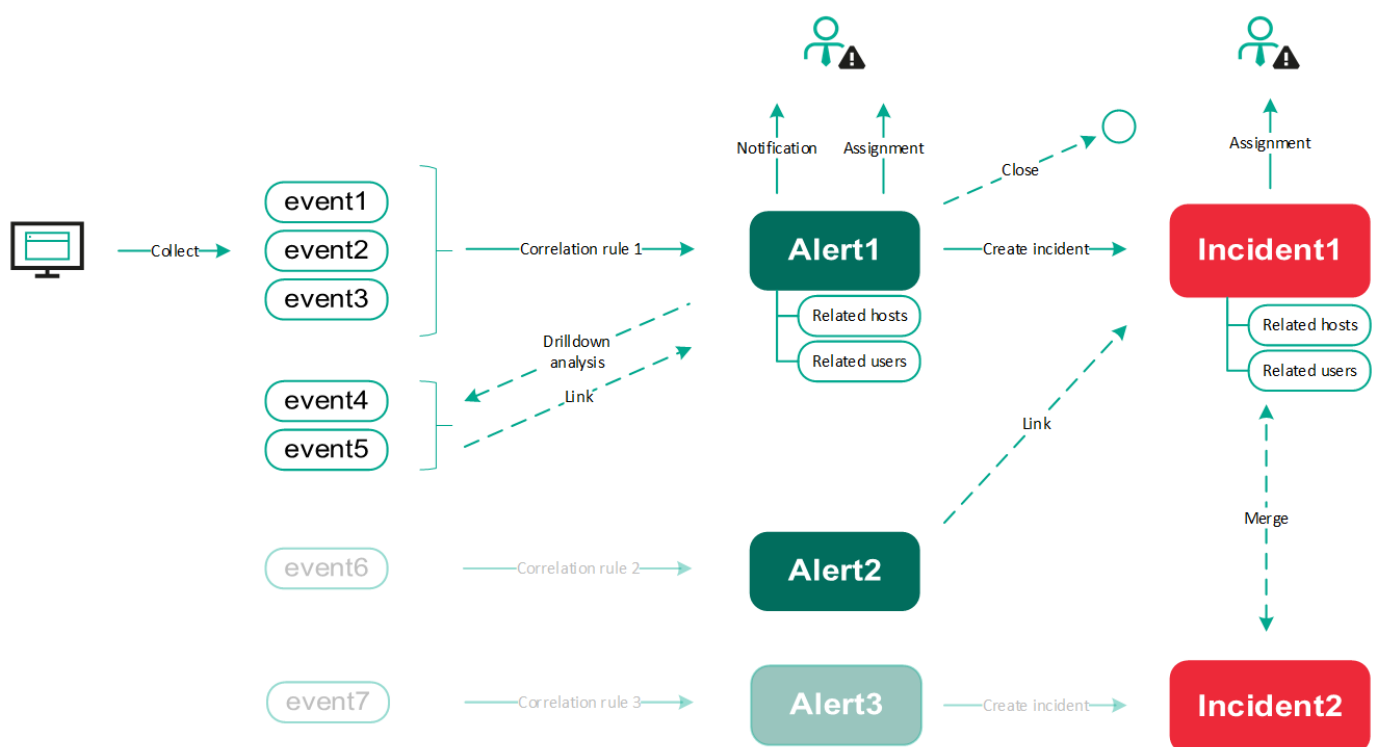


Описание процесса работы с инцидентами в KUMA

Ниже приведено описание основного функционала KUMA задействованного в управлении инцидентами.



Алерты

Создание алерта

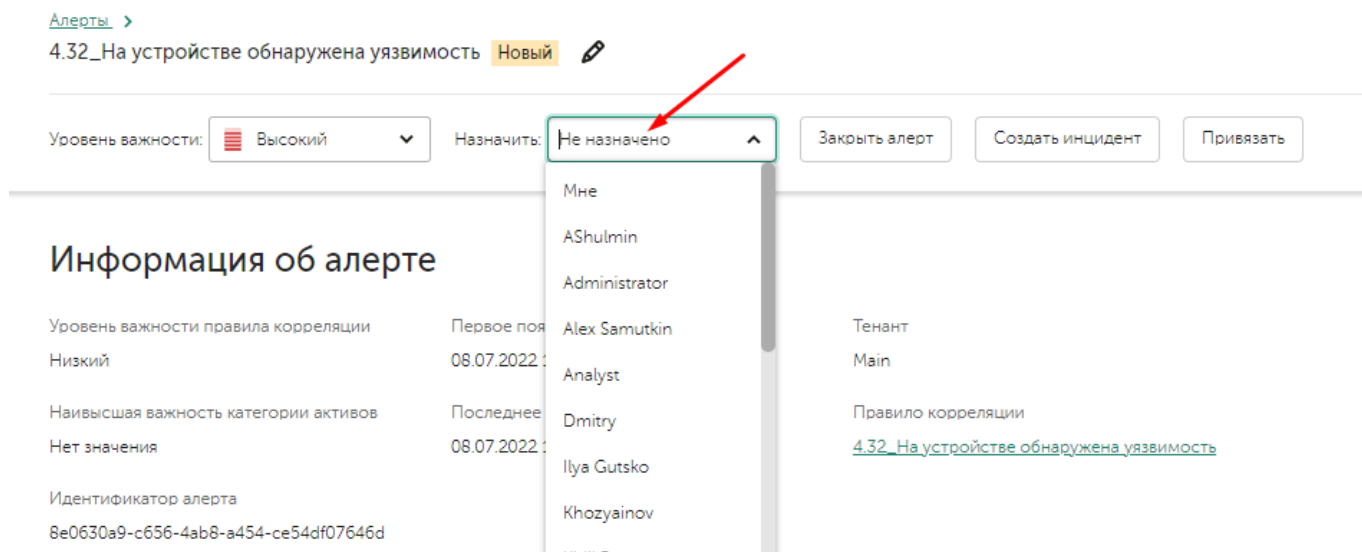
Алерт создается в результате сработки корреляционного правила на основе поступивших событий, он является подозрением на инцидент. Чтобы создать алерт, необходимо настроить корреляционное правило и в секции Actions не включать опцию Do not create alert, в таком случае при срабатывании этого правила, создастся новый алерт.

Оповещение об алерте

При появлении алерта есть возможность настроить оповещение на почту. Для этого необходимо перейти в `Settings -> Alerts -> Notification rules`. При создании нового правила оповещения можно указать свой шаблон для письма. С помощью правил оповещения есть возможность настроить разные сценарии в зависимости от того какое корреляционное правило сработало, и исходя из этого оповещение уйдет разным получателям.

Назначение ответственного на алерт

Обнаружив новый алерт, аналитик может взять его в обработку, назначив на себя, для этого в окне алерта необходимо на верхней панели в **поле Assigned to** выбрать Me, либо выбрать другого пользователя, чтобы назначить алерт на него.



The screenshot shows the alert management interface. At the top, there's a breadcrumb [Алерты >](#) and the alert title **4.32_На устройстве обнаружена уязвимость** with a 'Новый' (New) tag and an edit icon. Below this is a toolbar with 'Уровень важности: Высокий' (Priority: High), 'Назначить:' (Assign to), 'Закрыть алерт' (Close alert), 'Создать инцидент' (Create incident), and 'Привязать' (Attach). The 'Назначить:' dropdown is open, showing a list of users: 'Не назначено' (Not assigned), 'Мне' (Me), 'AShulmin', 'Administrator', 'Alex Samutkin', 'Analyst', 'Dmitry', 'Ilya Gutsko', and 'Khozyainov'. A red arrow points to the 'Не назначено' option. The main content area is titled 'Информация об алерте' (Alert information) and contains details about the alert's priority, category, and correlation rule.

Информация об алерте		
Уровень важности правила корреляции	Первое поя	Тенант
Низкий	08.07.2022 :	Main
Наивысшая важность категории активов	Последнее	Правило корреляции
Нет значения	08.07.2022 :	4.32_На устройстве обнаружена уязвимость
Идентификатор алерта		
8e0630a9-c656-4ab8-a454-ce54df07646d		

Связанные активы

В рамках алерта в зависимости от событий могут быть связанные активы (хосты или аккаунты). Для автоматической актуализации активов можно настроить интеграцию, например, с Active Directory и Kaspersky Security Center. Если в событии встречается актив, то система автоматически связывает само событие с активом, а затем и алерт с активом. Список связанных активов находится в карточке алерта в полях Related endpoints и Related users.

Связанные активы

Количество ↓	Актив	Категории
185	Название: KATA 4.1 , IP-адрес: 10.68.85.70	Categorized assets/Device type/LinuxCategorized assets/DEMO
30	Название: WIN10_BN , IP-адрес: 10.68.85.128 , Полное доменное имя: win10_bn.sales.lab	Без категории
24	Название: WIN10_BN , IP-адрес: 10.68.85.128 , Полное доменное имя: win10_bn.sales.lab	Без категории
23	Название: BORIS-TEST , IP-адрес: 10.68.85.135 , Полное доменное имя: boris-test.sales.lab	Без категории

История изменений и ведение журнала

Для отслеживания всех действий, в карточке алерта есть раздел Change log, куда записываются все изменения алерта. Также для удобного взаимодействия внутри команды аналитиков, есть возможность оставлять записи в Change log, чтобы фиксировать ход расследования или записывать важную информацию.




Журнал изменений

Комментарий		
Время ↓	Пользователь	Действие
05.09.2023 18:24:51	boris	Комментарий: test 1

Связанные события

При срабатывании одного и того же правила новых алертов не создается, а наполняется существующий до тех пор, пока он не будет закрыт, либо если не создано правло сегментации для этого првила корреляции. В одном алерте может быть несколько вложенных событий, которые указаны в поле Related events. Для удобства расследования связанные события раскрываются в иерархическое дерево в зависимости от цепочки сработавших правил. Детали каждого события можно просмотреть прямо из карточки алерта, нажав на само событие.


Связанные события

 Время ↓	Информация о событии	Тенант
▼  22.08.2023 15:56:26	DeviceCustomString1: Test , SourceHostName: lena-centos-mokreev-2 , DeviceEventClassID: taaScanning	Main
22.08.2023 15:56:23	EndTime: 22.08.2023 15:56:23 , DeviceAddress: 10.68.85.180 , DeviceEventClassID: taaScanning , DeviceExternalID: https://10.68.85.180:8443/katap/#/alerts?id=18429 , DeviceHostName: kata-cn-51.evilcorp.local , DeviceProduct: KATA , DeviceReceiptTime: 22.08.2023 12:56:23 , DeviceTimeZone: +03:00 , DeviceVendor: Kaspersky , DeviceVersion: 5.1.0-6596	Main
Найти в событиях: 1		Main
>  22.08.2023 15:32:26	DeviceCustomString1: suspicious_service_execution_of_system_process , SourceHostName: dc.evilcorp.local , DeviceEventClassID: taaScanning	Main

Детализированный анализ


При необходимости детального анализа и изучения событий, которые произошли до и после инцидента, можно перейти ко всем событиям из алерта, нажав кнопку **Find in events** в разделе **Related events**. Перейдя во вкладку **Events** в результатах поиска, будут отображены все связанные события. Для отображения всех событий, которые были в данные промежутки времени, нужно сменить выбор с **Related to alert**, на All events. В результате отобразятся все события, среди которых можно выполнить поиск новых связанных событий и привязать их к алерту. Для этого выберете событие и в появившемся окне с детальной информацией нажмите Link to alert. Таким образом можно обогатить алерт новыми связанными событиями.

Связанные события

 Время ↓

Информация о событии

Тенант

▼  22.08.2023 15:56:26

DeviceCustomString1: Test , SourceHostName: lena-centos-mokreev-2 , DeviceEventClassID: taaScanning

Main

22.08.2023 15:56:23

EndTime: 22.08.2023 15:56:23 , DeviceAddress: 10.68.85.180 , DeviceEventClassID: taaScanning , DeviceExternalID: https://10.68.85.180:8443/katap/#/alerts?id=18429 , DeviceHostName: kata-cn-51.evilcorp.local , DeviceProduct: KATA , DeviceReceiptTime: 22.08.2023 12:56:23 , DeviceTimeZone: +03:00 , DeviceVendor: Kaspersky , DeviceVersion: 5.1.0-6596

Main


Скачать события

 [Найти в событиях](#)

Заккрытие алерта

В случае ложного срабатывания или, если нет необходимости создавать инцидент, есть возможность закрыть алерт. При закрытии алерта необходимо указать одну из трех причин: Отработан, Неверные данные, Неверное правило корреляции.

[Алерты](#) >

[KEDR] Сработка правила IOA Новый 

Уровень важности:  Средний ▼

Назначить: Не назначено ▼

Заккрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции
Низкий

Первое появление
08.11.2022 16:37:01

Тенант
Main

Наивысшая важность категории активов
Низкий

Последнее появление
22.08.2023 15:56:26


Правило корреляции
[\[KEDR\] Сработка правила IOA](#)

Идентификатор алерта

Создание инцидента

В случае необходимости повышения алерта до уровня инцидента, это можно сделать с помощью кнопки **Create incident**.

[Алерты](#) >

[KEDR] Сработка правила IOA Новый 

Уровень важности:  Средний ▼

Назначить: Не назначено ▼

Заккрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции
Низкий

Первое появление
08.11.2022 16:37:01

Тенант
Main

Наивысшая важность категории активов
Низкий

Последнее появление
22.08.2023 15:56:26


Правило корреляции
[\[KEDR\] Сработка правила IOA](#)

Привязка алерта к инциденту

В случае, если алерт является частью активности, расследуемой в рамках уже существующего инцидента, его можно привязать его с помощью кнопки **Link**.

Привязанный алерт становится недоступен для изменения – при необходимости изменения алерта (например добавления в него событий), нужно отвязать (unlink) алерт от инцидента, внести изменения, и привязать его обратно.

Уровень важности:

 Средний ▼

Назначить:

Не назначено ▼

Заккрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции

Низкий

Первое появление

08.11.2022 16:37:01

Тенант

Main

Наивысшая важность категории активов

Низкий

Последнее появление

22.08.2023 15:56:26

Правило корреляции

[\[KEDR\] Сработка правила IOA](#)

Идентификатор алерта

ec6559ab-d2b1-4539-bae3-fd6b90b419db

Инциденты

Создание инцидента

Инцидент можно создать на основе алерта или вручную с помощью кнопки **Create incident** во вкладке Incidents. При создании вручную необходимо заполнить обязательные поля, также при необходимости, есть возможность прикрепить к инциденту алерты или связанные активы.

Объединение инцидентов

Если в ходе расследования потребовалось объединить несколько инцидентов в один – это можно сделать с помощью функционала объединения. Для этого в окне инцидента нужно на верхней панели нажать на **Merge** и выбрать инцидент, с которым необходимо выполнить объединение.

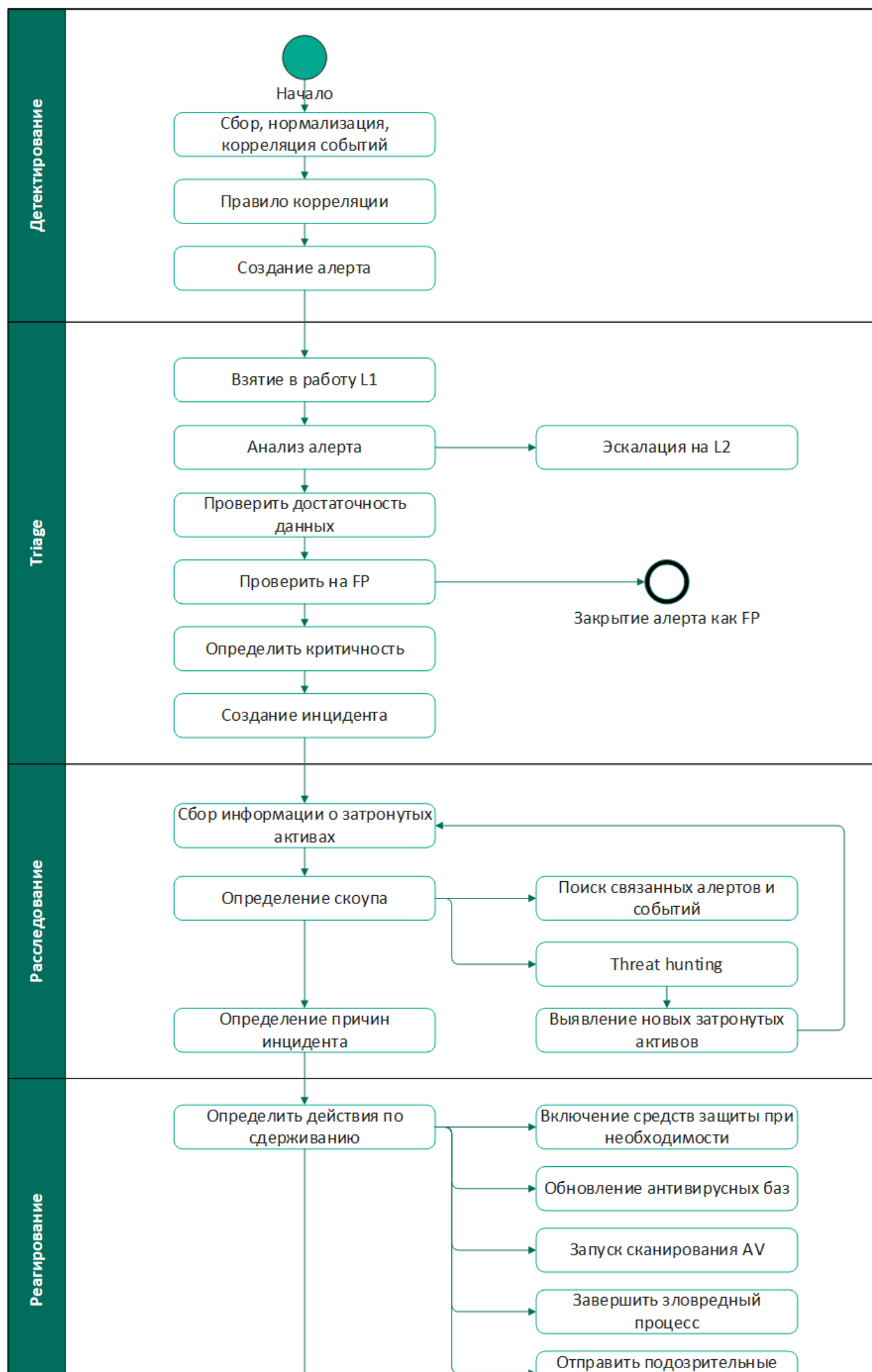
Назначение ответственного на инцидент

При создании нового инцидента, аналитик может взять его в обработку, назначив на себя, для этого в окне инцидента необходимо на верхней панели **в поле Assigned to** выбрать «Me», либо выбрать другого пользователя, чтобы назначить инцидент на него.

Пример процесса реагирования на инциденты

Рассмотрим пример плана реагирования на инцидент, в рамках которого можно выделить стадии:

- Мониторинг – сбор и анализ событий, выявление аномалий и подозрительной активности с помощью правил корреляции или threat hunting.
- Триаж – первичный анализ алертов с целью выявления инцидентов, ложных срабатываний и ошибок в рамках процесса мониторинга.
- Расследование – сбор информации об активах и вредоносной активности с целью определения скоупа, причин инцидента и всей цепочки атаки.
- Реагирование – противодействие вредоносным действиям с целью предотвратить дальнейшее продвижение злоумышленника и сократить влияние на инфраструктуру
- Восстановление – приведение инфраструктуры в первоначальное состояние и проверка работоспособности
- Закрытие – заключение или отчет об инциденте и закрытие инцидента



Пример реагирования на инцидент с помощью KUMA

Рассмотрим пример реагирования на инцидент с помощью Kaspersky Unified Monitoring and Analysis Platform. Для примера будет взят стенд со следующими параметрами:

- Рабочая станция на Windows 10
 - доменная авторизация
 - KES
 - KEA
- KEDR
- KSC
- KUMA
 - Установлен пакет правил SOC_package (см. пресейл пак или ссылку с архивом установки KUMA)
 - Настроена интеграция с AD
 - Настроена интеграция с KSC
 - Настроена интеграция с KEDR

В рамках стенда условный нарушитель, заметив незаблокированный компьютер администратора, воспользовался случаем и выполнил зловердные действия:

- Скачал вредоносный файл со своего сервера
- Выполнил команду для создания ключа реестра в ветке Microsoft\Windows\CurrentVersion\Run
- Добавил скаченный файл в автозапуск с помощью реестра
- Выполнил очистку событий в журнале Security
- Вышел из сессии, чтобы владелец учетной записи ничего не заподозрил
- Владелец учетной записи вошел в систему, после чего запустился вредоносный файл

Процесс мониторинга

В процессе мониторинга с рабочей станции поступили события из журнала Security, после чего сработали правила корреляции из пакета SOC_package.

Alerts								
					Search...		Found: 45	Filters
<input type="checkbox"/>	Name	Status	Assigned to	Incident	First seen	Last seen	Affected asset categories	Tenant
<input type="checkbox"/>	R223_Сбор информации о процессах	New			2022-08-23 17:28:40	2022-08-23 17:28:40	HQ/Categorized assets/Business impact/HIGH HQ/Categorized assets/Device type/Workstation	HQ
<input type="checkbox"/>	R050_Очистка журнала событий Windows	New			2022-08-23 17:27:20	2022-08-23 17:27:20	HQ/Categorized assets/Business impact/HIGH HQ/Categorized assets/Device type/Workstation	HQ
<input type="checkbox"/>	R295_Манипуляции с системой непривилегированным процессом	New			2022-08-23 17:27:05	2022-08-23 17:27:05	HQ/Categorized assets/Business impact/HIGH HQ/Categorized assets/Device type/Workstation	HQ
<input type="checkbox"/>	R097_Манипуляции с загрузочным скриптом	New			2022-08-23 17:27:05	2022-08-23 17:27:05	HQ/Categorized assets/Business impact/HIGH HQ/Categorized assets/Device type/Workstation	HQ
<input type="checkbox"/>	R093_Изменение критичных веток реестра	New			2022-08-23 17:27:05	2022-08-23 17:27:05	HQ/Categorized assets/Business impact/HIGH HQ/Categorized assets/Device type/Workstation	HQ

Каждый алерт имеет название правила корреляции, которое его породило. При повторном срабатывании правила в поле First seen будет время первого события, а в Last seen последнего.

Triage

При появлении нового алерта срабатывает правило оповещения и отправляется письмо на почту группе реагирования или конкретному аналитику.

Аналитики из L1 переходит по ссылке из письма и попадает сразу на карточку первого алерта:

Priority:

Medium

Assign to:

Unassigned

Close alert

Create incident

Link

Details on alert

Correlation rule priority	First seen	Tenant
High	2022-08-23 17:27:05	HQ
Max asset category priority	Last seen	Correlation rule
High	2022-08-23 17:27:05	R093_Изменение критичных веток реестра
Alert ID		
da25307c-ab94-4f86-9229-ed9f11a59f9d		

Related events

Download events

Find in events

Timestamp ↓	Event details	Tenant
> 2022-08-23 17:27:05	DestinationAccountID: e5d3bc3d-ec5b-4fed-a644-bae8d8bc80a8 , DestinationProcessName: C:\Windows\System32\reg.exe , DestinationUserID: 0xcfd554 , DestinationUserName: talankin , DeviceCustomString3: 0x28a4 , DeviceCustomString3Label: Process ID , DeviceCustomString4: C:\Users\talankin\Downloads\ChromeUpdate.bat , DeviceCustomString4Label: New Value , DeviceCustomString5: - , DeviceCustomString5Label: OldValue , DeviceCustomString6: ChromeUpdate , DeviceCustomString6Label: Object Value Name , FileName: \REGISTRY\USER\S-1-5-21-3912863674-961347404-1945235527-1117\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	HQ

Total: 1

Related endpoints

Download assets

Search for IP addresses or FQDN...

Count ↓	Endpoint	Categories
1	Name: WINDOWS-KEDR , IP: 192.168.1.172 , FQDN: windows-kedr.soc.env	Categorized assets/Business Impact/HIGH Categorized assets/Device type/Workstation

Total: 1

Related users

Download users

Search for users...

Count ↓	User	User principal name	Email	Domain
1	igor.talankin	talankin@soc.env		soc.env

Total: 1

Взятие в работу L1

Аналитик берет в работу алерт, назначая его на себя.

Анализ алерта

При анализе алерта аналитик обращает внимание на то какое правило сработало и соответствуют ли данные из событий с самим правилом. Как видно из названия правила алерт сработал на изменение какой-то критичной ветки реестра, в поле Related events в событии присутствуют путь до ключа реестра, есть старое и новое значение ключа реестра, отсюда можно сделать вывод, что правило соответствует произошедшему событию и аналитик обладает достаточной экспертизой, чтобы продолжить реагирование. Иначе же аналитик может перевести алерт на L2, назначив его на другого аналитика.

Проверка достаточности данных

На данном этапе аналитик должен определить каких данных ему будет достаточно для дальнейшего расследования. Чтобы продолжить расследование в рамках алерта по несанкционированному изменению ветки реестра, необходимо точно знать какой ключ был изменен и на каком хосте это было сделано. Дополнительными полезными данными будет информация о том, кто это сделал и новое значение ключа реестра. Раскрыв дерево событий от верхнеуровневого правила до самого события, можно увидеть детали, нажав на интересующее событие.

Event details



Timestamp	2022-08-23 17:27:03 :308
Name	A registry value was modified.
EndTime	2022-08-23 14:27:01 :308
DeviceAction	New Registry Value created
DeviceAssetID	4448427a-4a27-46a7-bb13-b8c62192fbd5
DeviceEventCategory	Microsoft-Windows-Security-Auditing
DeviceEventClassID	4657
DeviceHostName	windows-kedr.soc.env
DeviceNtDomain	SOCENV
DeviceProduct	Windows
DeviceReceiptTime	2022-08-23 17:27:03 :308
DeviceTimeZone	+03:00
DeviceVendor	Microsoft
SourceNtDomain	SOCENV
SourceUserID	S-1-5-21-3912863674-961347404-1945235527-1117
SourceUserName	talankin
DestinationAccountID	e5d3bc3d-ec5b-4fed-a644-bae8d8bc80a8
DestinationProcessName	C:\Windows\System32\reg.exe
DestinationUserID	0xcfd554
DestinationUserName	talankin
DeviceCustomString3	0x28a4
DeviceCustomString3Label	Process ID
DeviceCustomString4	C:\Users\talankin\Downloads\ChromeUpdate.bat
DeviceCustomString4Label	New Value
DeviceCustomString5	-
DeviceCustomString5Label	OldValue
DeviceCustomString6	ChromeUpdate
DeviceCustomString6Label	Object Value Name
Service	From Agent HTTP.Windows
ExternalID	25365043
FileID	0x164
FileName	\REGISTRY\USER\S-1-5-21-3912863674-961347404-1945235527-1117\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Проверка на False Positive

В рамках проверки на ложное срабатывание аналитик должен проверить верно ли сработало правило, может ли быть такая активность легитимной в связи с нормальной работой системы (например, обновление). Проанализировав детали события, видно, что персональная учетная запись talankin выполнила создание ключа реестра с помощью утилиты reg.exe, а также ключ реестра был создан в ветке \Microsoft\Windows\CurrentVersion\Run, отвечающей за автозапуск программ при входе пользователя в систему. Эти данные дают понять, что алерт скорее всего является True Positive и можно продолжить анализ дальше.

Определение критичности

На стадии определения критичности нужно валидировать критичность, которая была проставлена автоматически либо скорректировать её. Исходя из данных алерта имеет смысл выставить высокую критичность для данного алерта:

[Alerts](#) >

R093_Изменение критичных веток реестра Assigned

Priority: Medium ^ Assign to: Igor Talankin ▼ Close alert Create incident Link

Details

Correlation rule: High

Max asset category priority: High

Alert ID: da25307c-ab94-4f86-9229-ed9f11a59f9d

First seen: 2022-08-23 17:27:05

Last seen: 2022-08-23 17:27:05

Tenant: HQ

Correlation rule: [R093_Изменение критичных веток реестра](#)

Priority dropdown menu:

- Critical
- High
- Medium
- Low

Создание инцидента

Проведя действия в рамках триажа, аналитик может эскалировать алерт до инцидента, чтобы начать расследование. Для этого в карточке инцидента необходимо нажать Create incident, в появившемся окне заполнить необходимые поля и нажать Save:

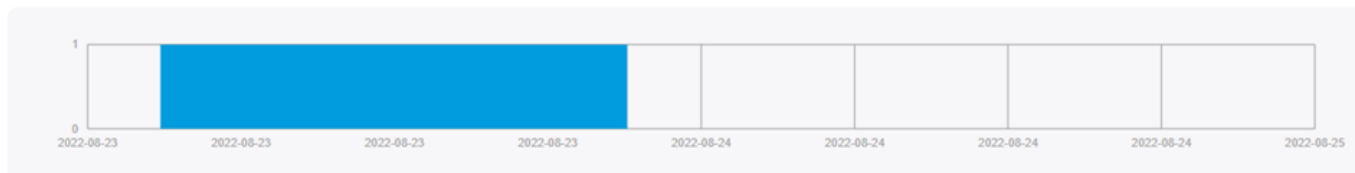
Summary

Created 2022-08-23 19:33:24

*Name R093_Изменение критичных веток реестра ?

*Tenant HQ

Status Opened



*Priority High

Affected asset categories HQ/Categorized assets/Business impact/HIGH ?

HQ/Categorized assets/Device type/Workstation

First event time 2022-08-23 17:27:05 ?

Last event time 2022-08-23 17:27:05 ?

Category

Type

RuCERT export Not exported

Description R093_Изменение критичных веток реестра

Related tenants HQ ?

Available tenants HQ ?

Расследование

Сбор информации о затронутых активах

Информация о затронутых активах автоматически выделяется в поля инцидента Related endpoints и Related users в том случае, если данные об этих активах загружены в KUMA с помощью интеграции с KSC, AD или внесены вручную. В изображении ниже видно, что в рамках инцидента были затронуты хост windows-kedr и учетная запись пользователя igor talankin.

Сразу можно отметить, что хост находится в категориях Business impact/HIGH и Device type/Workstation, то есть мы имеем дело с рабочей станцией, которая является критичной для нашей инфраструктуры (по легенде рабочая станция принадлежит администратору).

[Incidents](#) >

R093_Изменение критичных веток
реестра

Assign
to

Unassigned ▼

Close

Merge

Export to RuCERT

Save

Cancel

Related endpoints


Link	Search...				
<input type="checkbox"/>	Name	Tenant	Category	Count	⚙
<input type="checkbox"/>	WINDOWS-KEDR	HQ	HQ/Categorized assets/Business impact/HIGH HQ/Categorized assets/Device type/Workstation	1	

Total 1

Related users

Link

Search...

<input type="checkbox"/>	User	Tenant	User principal name	Email	Count	
<input type="checkbox"/>	Igor talankin	HQ	talankin@soc.env		1	

Если нажать на хост, то появятся детали актива. Детали содержат довольно подробную информацию, куда входит:

- FQDN, IP адрес, MAC адрес, время создания и обновления информации
- Количество алертов с разделением по критичности, с которыми этот актив связан. Также есть возможность сразу перейти к этим алертам, для поиска дополнительной информации в рамках инцидента.
- Категории, к которым относится актив
- Уязвимости на хосте
- Информация об установленном ПО
- Информация о hardware
- Другая дополнительная информация

Asset details

[Delete](#)[Edit](#)[Move to KSC group](#)[KSC response](#)

Name

WINDOWS-KEDR

Tenant

HQ

Asset source

Kaspersky Security Center, Created manually

ID

44484278-4a27-46a7-bb13-b8c62192fbd5

Created

2022-08-19 11:25:30

Updated

2022-08-23 18:15:19

IP address

192.168.1.172

FQDN

windows-kedr.soc.env

MAC address

00:50:56:AC:73:B1

Related alerts

[Find in Alerts](#)

Critical: 1

Closed: 1



High: 2

Closed: 1, Escalated: 1



Medium: 18

New: 3, Closed: 15



Low: 12

New: 1, Closed: 11

> Categories

> Kaspersky Security Center vulnerabilities

▼ Software info

1. Software
Microsoft Windows OSE

Installation type
Executable file

2. Software
Notepad++ (64-bit x64) 8.0 Notepad++ Team

Install date
2021-06-23

Installation type
Executable file

3. Software
Kaspersky Endpoint Security for Windows 11.6.0.394 AO Kaspersky Lab

Install date
2021-06-11

Installation type
MSI

4. Software
WinRAR 6.02 (64-bit) 6.02.0 win.rar GmbH

Install date
2021-06-23

Operating system
Microsoft Windows 10 19042

> Categories

▼ Kaspersky Security Center vulnerabilities [Update](#)

☐ ● KLA12500 in Google Chrome

CVE 10 : CVE-2022-1305,CVE-2022-1306,CVE-2022-1307,CVE-2022-1308,CVE-2022-1309,CVE-2022-1310,CVE-2022-1311,CVE-2022-1312,CVE-2022-1313,CVE-2022-1314

☐ ● KLA12571 in Google Chrome

CVE 9 : CVE-2022-2156,CVE-2022-2157,CVE-2022-2158,CVE-2022-2160,CVE-2022-2161,CVE-2022-2162,CVE-2022-2163,CVE-2022-2164,CVE-2022-2165

☐ ● KLA12332 in Google Chrome

CVE 7 : CVE-2021-37997,CVE-2021-37998,CVE-2021-37999,CVE-2021-38000,CVE-2021-38001,CVE-2021-38002,CVE-2021-38003

☐ ● KLA12377 in Google Chrome

CVE 5 : CVE-2021-4098,CVE-2021-4099,CVE-2021-4100,CVE-2021-4101,CVE-2021-4102

Если нажать на связанную учетную запись, то можно изучить данные о ней по информации из Active Directory:

- Имя пользователя
- Имя учетной записи
- Email
- Группы, в которых состоит учетная запись
- Дата истечения пароля, дата создания и время последнего неверного ввода пароля
- Другая информация из AD

Как видно из списка групп, учетная запись состоит в группе доменных администраторов, что подтверждает высокую критичность инцидента.

Account details



Display name

igor talankin

Common Name

igor2 talankin

Distinguished name

cn=igor2 talankin,cn=users,dc=soc,dc=env

User logon name

talankin

User principal name

talankin@soc.env

Member Of

{ cn=domain admins,cn=users,dc=soc,dc=env }

User account control

66048

▼ Additional info

Created

2021-07-06 12:17:02

Account expires

30828-09-14 05:48:05

Bad password time

2022-08-23 14:43:10

Определение скоупа






Для определения скоупа инцидента необходимо произвести расследование и выявить по возможности другие события и алерты, которые относятся к этой злонамеренной активности.

Привязка события к инциденту возможна только через алерт (при этом алерт перед изменениями в т.ч. добавления новых событий в него, необходимо отвязать от инцидента).







Поиск связанных алертов

Первым делом имеет смысл проверить другие алерты, которые происходили с затронутыми активами.

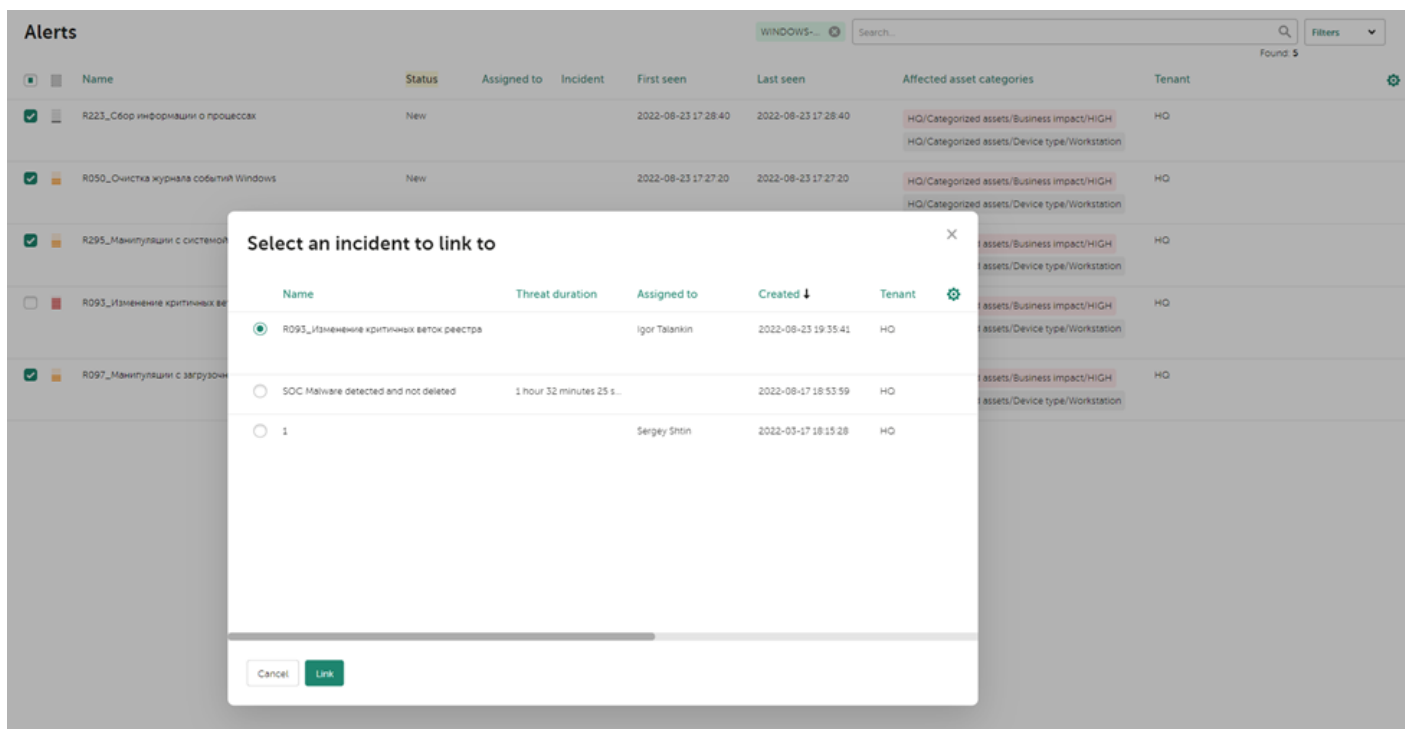
Для этого достаточно выбрать актив и в разделе со связанными алертами нажать Find in alerts.

Related alerts		Find in Alerts
	Critical: 1 Closed: 1	
	High: 3 New: 1, Closed: 1, Escalated: 1	
	Medium: 18 New: 3, Closed: 15	
	Low: 12 New: 1, Closed: 11	

В окне с алертами можно сделать фильтрацию по времени или статусу, чтобы исключить уже обработанные алерты или устаревшие:

Alerts		WINDOWS-...	Search...				Found: 5
<input type="checkbox"/>		Name	Status	Assigned to	Incident	First seen	Last seen
<input type="checkbox"/>		R223_Сбор информации о процессах	New			2022-08-23 17:28:40	2022-08-23 17:28:40
<input type="checkbox"/>		R050_Очистка журнала событий Windows	New			2022-08-23 17:27:20	2022-08-23 17:27:20
<input type="checkbox"/>		R295_Манипуляции с системой непривилегированным процессом	New			2022-08-23 17:27:05	2022-08-23 17:27:05
<input type="checkbox"/>		R093_Изменение критичных веток реестра	Escalated		R093_Изменен критичных веток реестра	2022-08-23 17:27:05	2022-08-23 17:27:05
<input type="checkbox"/>		R097_Манипуляции с загрузочным скриптом	New			2022-08-23 17:27:05	2022-08-23 17:27:05

Как видно, с данным активом связаны и другие алерты. Судя по времени, в которое сработали алерты, мы можем сделать вывод, что все они так или иначе связаны друг с другом. Чтобы связать алерты с инцидентом, отмечаем интересующие алерты и нажимаем в нижней части панели Link, в появившемся окне отмечаем инцидент, с которым мы хотим связать алерты и снова нажимаем Link:



Перейдя обратно в карточку инцидента, мы можем убедиться, что все отмеченные алерты привязаны:

Related alerts

[Link](#)

<input type="checkbox"/>	Name	Tenant	First seen ↑	Priority
<input type="checkbox"/>	R097_Манипуляции с загрузочным скриптом	HQ	2022-08-23 17:27:05	Medium
<input type="checkbox"/>	R093_Изменение критичных веток реестра	HQ	2022-08-23 17:27:05	High
<input type="checkbox"/>	R295_Манипуляции с системой непривилегированным процессом	HQ	2022-08-23 17:27:05	Medium
<input type="checkbox"/>	R050_Очистка журнала событий Windows	HQ	2022-08-23 17:27:20	Medium
<input type="checkbox"/>	R223_Сбор информации о процессах	HQ	2022-08-23 17:28:40	Low

Ту же самую операцию мы можем провести с учетной записью и найти связанные алерты. В случае, если в новом алерте будут новые связанные активы, то мы можем продолжать поиск связанных алертов и по ним, тем самым расширяя скоуп расследования.

В случае, если мы обнаружили, что уже есть инцидент в работе, с которым мы можем объединить текущий инцидент, чтобы вести процесс реагирования в рамках одного инцидента, мы можем склеить их с помощью функции Merge. Для этого в карточке инцидента нужно нажать в верхней части на Merge, а затем выбрать инцидент, с которым мы хотим выполнить склеивание.

Threat hunting

После поиска связанных активов и алертов, можно приступить к более детальному расследованию и углубиться в поиск связанных с инцидентом IOC по всей инфраструктуре.

Для поиска связанных событий можно воспользоваться вкладкой Events и произвести поиск вручную или выбрать любой из связанных алертов и в его карточке нажать Find in events. Данный функционал называется Drilldown analysis:

[Alerts](#) >
R093_Изменение критичных веток реестра Escalated

Priority: High

Assign to: Igor Talankin

Unlink

Details on alert

Correlation rule priority	First seen	Tenant
High	2022-08-23 17:27:05	HQ
Max asset category priority	Last seen	Correlation rule
High	2022-08-23 17:27:05	R093_Изменение критичных веток реестра
Linked to incident	Alert ID	
R093_Изменение критичных веток реестра	da25307c-ab94-4f86-9229-ed9f11a59f9d	

Assigned

Related events

Download events

Find in events

Timestamp ↓	Event details
2022-08-23 17:27:05	DestinationAccountID: e5d3bc3d-ec5b-4fed-a644-bae8d8bc80a8 , DestinationProcessName: C:\Windows\System32\reg.exe , DestinationUserID: 0xcfd554 , DestinationUserName: talankin , DeviceCustomString3: 0x28a4 , DeviceCustomString3Label: Process ID , DeviceCustomString4: C:\Users\talankin\Downloads\ChromeUpdate.bat , DeviceCustomString4Label: New Value , DeviceCustomString5: - , DeviceCustomString5Label: OldValue , DeviceCustomString6: ChromeUp , DeviceCustomString6Label: Object Value Name , FileName: \REGISTRY\USER\S-1-5-21-391286367-961347404-1945235527-1117\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2022-08-23 17:27:05	TenantID: HQ , StartTime: 2022-08-23 17:27:03 , EndTime: 2022-08-23 17:27:03 , DeviceProduct: , DeviceTimeZone: +03:00 , DeviceVendor: Kaspersky , DestinationAccountID: e5d3bc3d-ec5b-4fed-a644-bae8d8bc80a8 , DestinationProcessName: C:\Windows\System32\reg.exe , DestinationUserID: 0xcfd554 , DestinationUserName: talankin
2022-08-23 17:27:03	TenantID: HQ , EndTime: 2022-08-23 14:27:01 , DeviceAction: New Registry Value created , DeviceAssetID: 4448427a-4a27-46a7-bb13-b8c62192fbd5 , DeviceEventCategory: Microsoft-Win Security-Auditing , DeviceEventClassID: 4657 , DeviceHostName: windows-kedr.soc.env , DeviceNtDomain: SOCENV , DeviceProduct: Windows , DeviceReceiptTime: 2022-08-23 17:27:03
Find in events: 1	
Find in events: 1	

В появившемся окне с событиями мы можем искать события и сразу же связывать их с выбранным алертом (для привязки алерта он должен быть отвязан от инцидента). Для этого необходимо в верхней части выбрать Search events -> All events:

Events > Alert investigation: R093...

Related to alert No refresh 15 2022-08-23 17:27:05 - 2022-...

SELECT * FROM 'events'

Use of SQL functions is limited

Link to alert Timestamp

Search events
Related to alert ✓
R093_Изменение критичных веток р...
Storage
All events

DestinationHostName... Destination... Des

Linked	2022-08-23 17:27:05	R093_Изменение критичных веток реестра	talankin	C:\Window:
Linked	2022-08-23 17:27:05	R093_02_Изменение критичных веток реестра	talankin	C:\Window:

В результате поиска, нам удалось найти команду, которую выполнил злоумышленник, чтобы создать новый ключ реестра. Исходя из данных события, мы можем найти какой процесс был родительским для reg.exe, им окажется cmd.exe, то есть злоумышленник запустил командную строку и выполнил команду в ней.

Events > Alert investigation: R093_Изменение критичных веток ре...

All events

SELECT * FROM 'events' WHERE DeviceEventClassID = '4688' AND DeviceVendor =

Link to alert	Timestamp	Name	DeviceHostName
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:34	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:24	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:23	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:20	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:16	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:27:03	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:26:49	A new process has been created.	windows-kedr.soc.env
Not linked	2022-08-23 17:26:47	A new process has been created.	windows-kedr.soc.env

Event details

DeviceProduct	Windows
DeviceReceiptTime	2022-08-23 17:27:03.308
DeviceTimeZone	+03:00
DeviceVendor	Microsoft
SourceNtDomain	SOCENV
SourceUserID	S-1-5-21-3912863674-961347404-1945235527-1117
SourceUserName	talankin
DestinationNtDomain	-
DestinationProcessName	C:\Windows\System32\reg.exe
DestinationUserID	S-1-0-0
DestinationUserName	-
DeviceCustomString1	S-1-16-8192
DeviceCustomString1Label	Mandatory Label
DeviceCustomString3	0x28a4
DeviceCustomString3Label	New Process Id
DeviceCustomString4	REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "ChromeUpdate" /t REG_SZ /F /D "C:\Users\talankin\Downloads\ChromeUpdate.bat"
DeviceCustomString4Label	Command Line

Link to alert

Из этого события появляется информация о некотором файле ChromeUpdate.bat. Чтобы узнать происхождение этого файла, мы можем продолжить процесс поиска, выполнив поиск по FileName = 'C:\\Users\\talankin\\Downloads\\ChromeUpdate.bat' и по маске доступа %%4417 (тип доступа WriteData (or AddFile)). В результате поиска мы найдем, что файл был создан процессом msedge.exe, чтобы говорит о том, что файл был скачен из внешнего источника, для дальнейшего анализа уже потребуются события с проху сервера или NGFW. Это событие мы также привязываем к нашему алерту.

Events >

Alert investigation: R093_Изменение критичных веток реестра

All events

No refresh

15m 15 minutes

Storage: Main-stor...

...

SELECT * FROM 'events' WHERE DeviceCustomString1 like '%4417%' AND FileName like 'C:\\Users\\talankin\\Downloads\\ChromeUpdate.bat' AND DeviceVendor = 'Microsoft'

ORDER BY Timestamp DESC LIMIT 250

Link to alert	Name	DeviceHostName	SourceUserName	DestinationProcessName	DeviceCustomString4
Not linked	A handle to an object was requested.	windows-kedr-soc-env	talankin	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe	

В ходе расследования мы можем выявить новые индикаторы компрометации такие как имя файла, URL, IP адрес и т.д., по этим данным также стоит выполнить поиск ретроспективный анализ, в результате которого можно выявить новые затронутые активы и обнаружить новые следы присутствия злоумышленника. В данном инциденте имеет смысл выполнить поиск файла ChromeUpdate.bat в событиях за последние пару недель.

Произведя Threat hunting для каждого алерта, мы должны выявить всю цепочку атаки.

Определение причин инцидента

По результатам поиска связанных событий мы выявили причины инцидента и можем записать результаты нашего анализа в журнал в карточке инцидента, чтобы передать информацию другим аналитикам или для полноты описания всего процесса реагирования. В разделе Change log мы можем указать важную информацию:

Change log

Comment

Add

Timestamp ↓	User	Action
2022-08-24 12:08:45	Igor Talankin	По результатам расследования выявлено, что учтеная запись talankin скачала вредоносный файл ChromeUpdate.bat с помощью браузера msedge.exe на хост windows-kedr. Выполнила команду для создания ключа реестра в ветке CurrentVersion\Run для автоматического выполнения файла при каждом входе пользователя talankin в систему. В результате выполнения файла ChromeUpdate.bat выполняется команда tasklist.

Реагирование

После расследования, у нас есть информация о затронутых активах, а также об индикаторах компрометации, которая поможет в сдерживании. Исходя из типа инцидента требуется определить список действий, которые нужно выполнить, чтобы остановить ход атаки. В данном случае имеет смысл:

- Запустить внеплановое антивирусное сканирование затронутых систем
- Изолировать хост от сети до момента, пока мы не убедимся в безопасности данного хоста
- Добавить файл ChromeUpdate.bat в карантин и создать правила предотвращающее его запуск на других хостах в инфраструктуре

Антивирусной сканирование

Для запуска сканирования в рамках этого инцидента необходимо перейти в карточку инцидента, выбрать затронутый хост и в верхней части информации об активе выбрать KSC Response и отметить заранее пред настроенную задачу по сканированию, а затем нажать Start.

Asset details

Delete

Edit

Move to

Name

WINDOWS-KEDR

Tenant

Select task

×

KUMA EPP Update

KUMA Virus scan Full

✓ KUMA Virus Scan Win

Сетевая изоляция хоста

Для изоляции хоста, необходимо повторить действия для выбранного хоста, но выбрать KEDR Response, затем в Task type выбрать Enable network isolation и заполнить дополнительные параметры при необходимости, например, уточнить время изоляции или исключения в случае необходимости иметь доступ к хосту во время изоляции.

Select task

×

*Task type

Enable network isolation

▼

* Isolation timeout

2

The number of hours during which network isolation will be active

⋮ Exclusion #1

*Traffic direction

Inbound

▼

*Asset IP

192.168.1.10

Local ports

3389

-

3389

🗑 Delete exclusion

+ Add exclusion

Предотвращение запуска вредоносного файла

Для добавления файла в карантин и создания превентивного правила с запретом запуска данного файла (в случае, если файл исполняемый) нужно повторить действия и выбрать KEDR Response -> Task type: Add preventive rule, в поле File hash указать хэш файла. В поле Asset имеет смысл указать All assets, так как нам необходимо застраховаться от дальнейшего распространения вредоносного файла.

Select task ×

*Task type

Add prevention rule ▼

*Asset

All assets ▼

*File hash #1

MD5 or SHA256 file hash

+ Add

Восстановление

После выполнения всех действий по расследованию и сдерживанию инцидента, а также после очистки инфраструктуры от следов злоумышленника, можно приступить к восстановлению нормальной работоспособности всех систем. Для это может понадобится отключить какие превентивные правила на EDR или убрать сетевую изоляцию, если она не отключится автоматически. Чтобы выполнить эти действия, необходимо повторить действия подобные тем, что были произведены на предыдущем этапе, только выбрать задачи Disable network isolation и Delete prevention rule.

Закрытие инцидента

В конце процесса реагирования мы можем закрыть инцидент, выбрав один из вариантов заключения: approved или not approved. Чтобы закрыть инцидент, необходимо в верхней части карточки инцидента выбрать Close incident, в появившемся окне отметить нужный вариант и выбрать Close:

Close incidents ×

Resolution:

☒ approved

☐ not approved

Cancel

Close

Закрытый инцидент нельзя «пере»-открыть.

Пошаговое руководство по разработке сценариев реагирования

<https://www.youtube.com/embed/jomLRu4UAjs>

Пример работы KUMA в тандеме с другими решениями на кейсе

https://www.youtube.com/embed/osNjaRVrveQ?si=2Ow1ndNg_paaupfL

Revision #9

Created 5 September 2023 15:10:05 by Boris RZR

Updated 11 November 2024 13:29:43 by Boris RZR