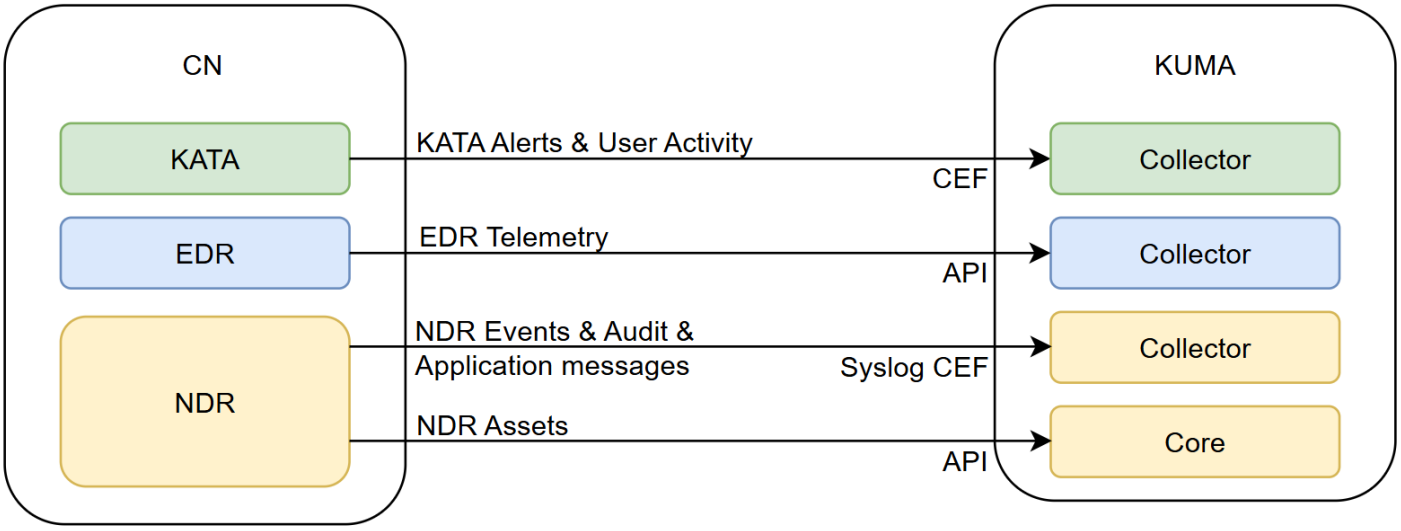
Cheat Sheet по интеграциям KATA с KUMA

Введение

В KATA версии 7.0 появились новые возможности и интеграции с KUMA. Данная статья направлена на упрощение восприятия данных интеграций, а также агрегации на одной странице всех инструкций по взаимодействию данных систем.

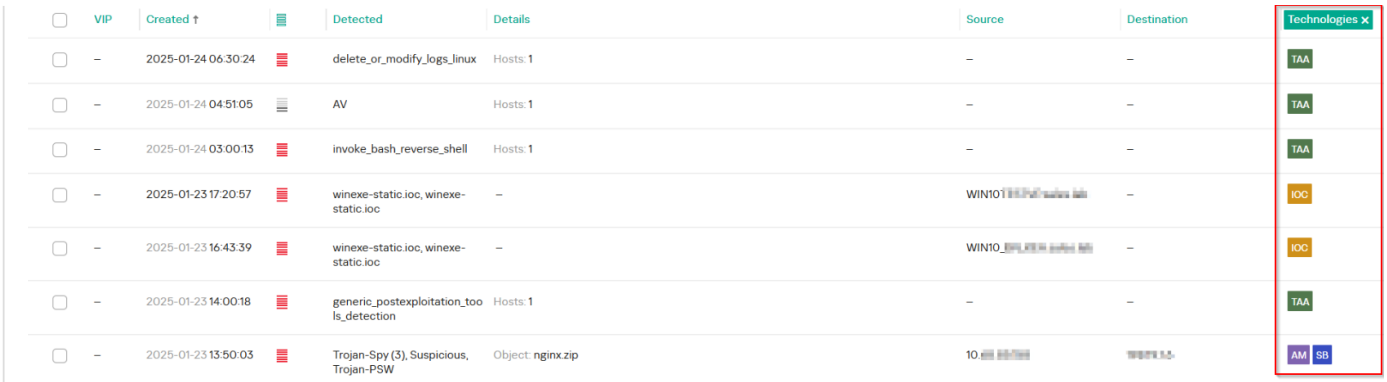
Схема взаимодействия



Подробнее

Что такое KATA Alerts?

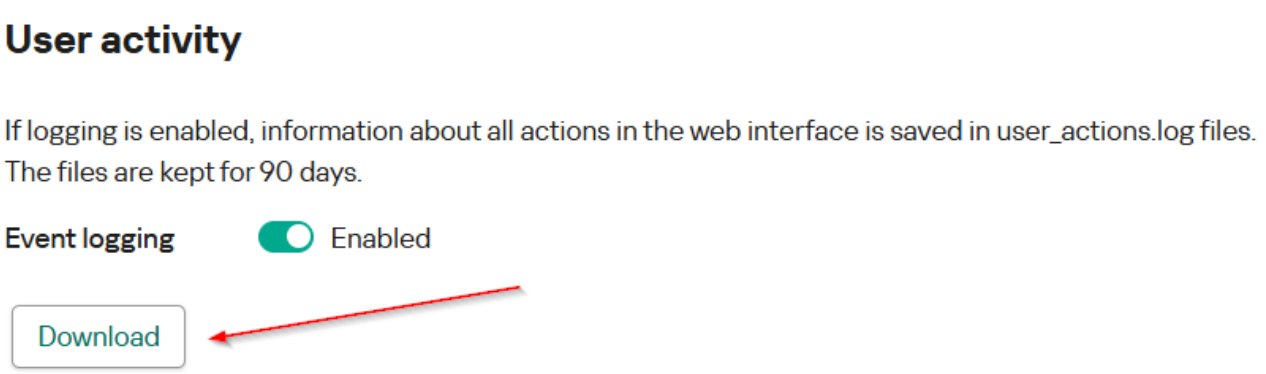
Вкладка Alerts в веб-интерфейсе KATA



VIP	Created	Detected	Details	Source	Destination	Technologies
–	2025-01-24 06:30:24	delete_or_modify_logs_linux	Hosts: 1	–	–	TAA
–	2025-01-24 04:51:05	AV	Hosts: 1	–	–	TAA
–	2025-01-24 03:00:13	invoke_bash_reverse_shell	Hosts: 1	–	–	TAA
–	2025-01-23 17:20:57	winexe-static.ioc, winexe-static.ioc	–	WIN10	–	IOC
–	2025-01-23 16:43:39	winexe-static.ioc, winexe-static.ioc	–	WIN10_	–	IOC
–	2025-01-23 14:00:18	generic_postexploitation_tools_detection	Hosts: 1	–	–	TAA
–	2025-01-23 13:50:03	Trojan-Spy (3), Suspicious, Trojan-PSW	Object: nginx.zip	10.		AM SB

Что такое User activity?

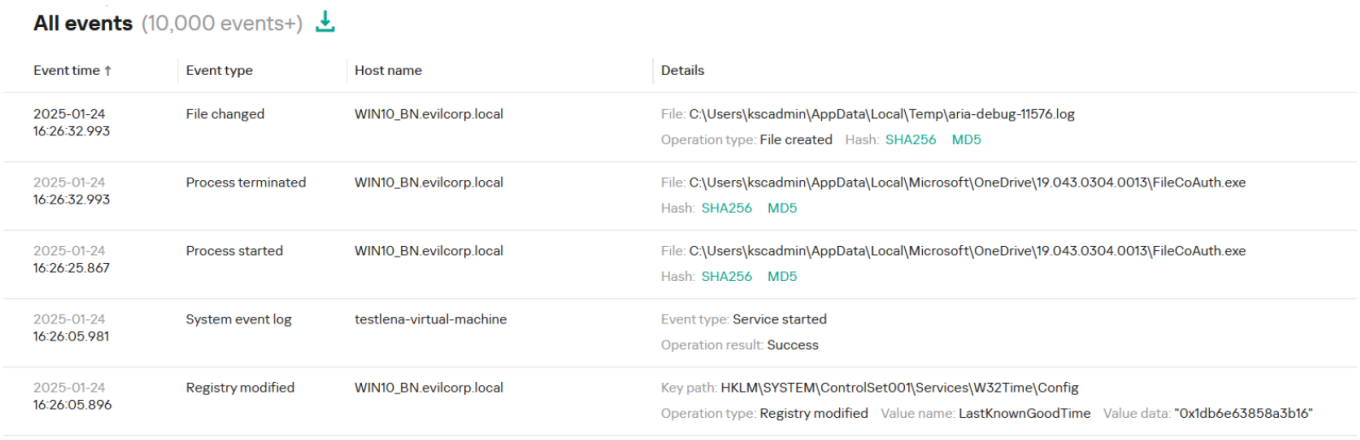
Вкладка Logs - User activity в интерфейсе KATA



Как настроить отправку алертов и действий пользователей KATA в KUMA - ссылка

Что такое EDR telemetry?

Вкладка Threat hunting в веб-интерфейсе KATA



All events (10,000 events+)

Event time	Event type	Host name	Details
2025-01-24 16:26:32.993	File changed	WIN10_BN.evilcorp.local	File: C:\Users\kscadmin\AppData\Local\Temp\aria-debug-11576.log Operation type: File created Hash: SHA256 MD5
2025-01-24 16:26:32.993	Process terminated	WIN10_BN.evilcorp.local	File: C:\Users\kscadmin\AppData\Local\Microsoft\OneDrive\19.043.0304.0013\FileCoAuth.exe Hash: SHA256 MD5
2025-01-24 16:26:25.867	Process started	WIN10_BN.evilcorp.local	File: C:\Users\kscadmin\AppData\Local\Microsoft\OneDrive\19.043.0304.0013\FileCoAuth.exe Hash: SHA256 MD5
2025-01-24 16:26:05.981	System event log	testlena-virtual-machine	Event type: Service started Operation result: Success
2025-01-24 16:26:05.896	Registry modified	WIN10_BN.evilcorp.local	Key path: HKLM\SYSTEM\ControlSet001\Services\W32Time\Config Operation type: Registry modified Value name: LastKnownGoodTime Value data: "0x1db6e63858a3b16"

Как настроить отправку телеметрии EDR в KUMA - ссылка

Что такое NDR events?

Вкладка Network traffic events в веб-интерфейсе KATA

Last seen	Title	Sco...	Source	Destination	Prot...	Techn...	Total a...	ID	Stat...
2025-02-11 14:44:50...	Сработало правило из набора ndr (системный набор прави...	9.6			UDP	IDS	18	20776	
2025-02-11 14:42:39...	Сработало правило из набора ndr (системный набор прави...	9.6			UDP	IDS	28	20769	
2025-02-11 14:36:31...	Сработало правило из набора ndr (системный набор прави...	9.6			UDP	IDS	5	20775	
2025-02-11 14:22:30...	Сработало правило из набора ndr (системный набор прави...	9.6			UDP	IDS	5	20772	
2025-02-11 14:16:14...	Обнаружены признаки ARP-спуфинга в ARP-ответах	9			ARP	IDS	2	20788	
2025-02-11 14:16:14...	Обнаружены признаки ARP-спуфинга в ARP-ответах	9			ARP	IDS	13	20782	
2025-02-11 14:10:14...	Обнаружены признаки ARP-спуфинга в ARP-ответах	9.6			ARP	IDS	58	20786	
2025-02-11 14:09:50...	Обнаружены признаки ARP-спуфинга в ARP-ответах	9.6			ARP	IDS	38	20787	
2025-02-11 13:45:36...	Обнаружены признаки ARP-спуфинга в ARP-ответах	9			ARP	IDS	145	20771	

Что такое NDR Audit?

Вкладка Logs - Audit в веб-интерфейсе KATA

Date and time	Action	Result	User	User node	Description
2025-02-11 15:22:17	Открытие списка записей аудита	Success			**(900003)** Открыт список записей аудита. Количество записей в списке: 1699.
2025-02-11 15:16:07	Подключение через веб-интерфейс	Success			**(2000001)** Пользователь NDR/dronov_adm успешно подключился через веб-интерфейс.
2025-02-11 15:16:07	Подключение через веб-интерфейс	Success			**(2000001)** Пользователь NDR/dronov_adm успешно подключился через веб-интерфейс.
2025-02-11 15:14:44	Открытие списка записей аудита	Success			**(900003)** Открыт список записей аудита. Количество записей в списке: 1696.
2025-02-11 15:09:32	Подключение через веб-интерфейс	Success			**(2000001)** Пользователь NDR/dronov_adm успешно подключился через веб-интерфейс.
2025-02-11 15:08:11	Подключение через веб-интерфейс	Success			**(2000001)** Пользователь NDR/dronov_sso успешно подключился через веб-интерфейс.
2025-02-11 15:06:49	Подключение через веб-интерфейс	Success			**(2000001)** Пользователь NDR/sso успешно подключился через веб-интерфейс.
2025-02-11 15:06:32	Изменение статуса события	Success			**(1900001)** Событию присвоен статус Обработано. ID события: 20745.
2025-02-11 15:06:32	Изменение статуса события	Success			**(1900001)** Событию присвоен статус Обработано. ID события: 20744.

Что такое NDR Application messages?

Вкладка Logs - Application messages в веб-интерфейсе KATA

Date and time	Status	Node	System process	Message
2025-02-11 14:35:30	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000004)** Установка обновлений не выполнена, так как базы программы актуальны.
2025-02-11 14:35:29	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000001)** Установка обновлений запущена автоматически (по расписанию).
2025-02-11 13:35:30	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000004)** Установка обновлений не выполнена, так как базы программы актуальны.
2025-02-11 13:35:29	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000001)** Установка обновлений запущена автоматически (по расписанию).
2025-02-11 12:35:30	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000004)** Установка обновлений не выполнена, так как базы программы актуальны.
2025-02-11 12:35:29	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000001)** Установка обновлений запущена автоматически (по расписанию).
2025-02-11 11:35:30	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000004)** Установка обновлений не выполнена, так как базы программы актуальны.
2025-02-11 11:35:29	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000001)** Установка обновлений запущена автоматически (по расписанию).
2025-02-11 10:35:30	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000004)** Установка обновлений не выполнена, так как базы программы актуальны.
2025-02-11 10:35:29	Normal operation	cd9d3244-3a04-4bae-86a1-08166196c...	ProductServer	**(2000001)** Установка обновлений запущена автоматически (по расписанию).

Как настроить отправку событий, аудита и сообщений NDR в KUMA - ссылка

Что такое NDR Assets?

Вкладка Assets в веб-интерфейсе KATA

Name	Sta...	Address inform...	Category	Security state	Importance	Last seen
KSCDK.sales.lab	Authorized	00:50:56:a8:da:33; 1...	Workstation	Critical	Medium	2025-02-11 15:27:...
dc.evilcorp.local	Authorized	00:50:56:a8:53:b1; 1...	Server	Critical	High	2025-02-11 15:28:...
KSCM-14.evilcorp.local	Authorized	00:50:56:a8:dc:19; 1...	Workstation	Critical	Medium	2025-02-11 15:28:...
AdminTrokhin	Authorized	00:50:56:89:f2:00; 10...	Workstation	Critical	Medium	2025-02-11 15:28:...
WIN10_BN_KEA.sales...	Authorized	00:50:56:89:73:73; 1...	Workstation	OK	Medium	2025-02-11 15:28:...
testlena-virtual-mac...	Authorized	00:50:56:a8:52:3d; 1...	Workstation	OK	Medium	2025-02-11 15:28:...
WIN10_BN.evilcorp.l...	Authorized	Several values	Server	Critical	High	2025-02-11 15:28:...
WIN10_KES_EDR_BN....	Authorized	00:50:56:a8:f5:b7; 10...	Server	Critical	High	2025-02-11 15:28:...
kali	Unauthor...	00:50:56:a8:11:21; 1...	Laptop	OK	Low	2025-02-11 15:27:...

Как настроить передачу активов, обнаруженных NDR в KUMA - ссылка

Revision #7
Created 3 February 2025 07:29:26 by Koala
Updated 11 February 2025 12:28:59 by Koala