

Day 22 - Create Alerts and Dashboards in Kibana - parte 4

CREARE ALERT E DASHBOARD BASATI SULLA TELEMETRIA GENERATA DA MYTHIC

Create Alerts and Dashboards

Creiamo un Alert per l'attività di **Mythic**, in particolare ci serve isolare quelli con **Event ID 1**, relativo alla creazione dei processi e vedere l'hash MD5 associato

The screenshot displays the Elastic SIEM interface. The search bar contains the query `svchost-johndoe.exe and event.code:1` with a filter for `agent.name: WIN-johndoe`. The search results show a single document for an event created on October 6, 2024, at 19:38:34.606. The document details are as follows:

Field	Value
elastic_agent.version	8.15.2
event.action	Process Create (rule: ProcessCreate)
event.agent_id_status	verified
event.code	1
event.created	Oct 6, 2024 @ 19:38:34.606
event.dataset	winlog.winlog
event.ingested	Oct 6, 2024 @ 19:38:42.000
event.kind	event
event.provider	Microsoft-Windows-Sysmon
host.architecture	x86_64

The document view also shows the following message: `Process Create: RuleName: technique_id=T1036, technique_name=Masqu...`

Create Alerts and Dashboards

Possiamo controllare l'hash su **Virus Total**, in questo caso non darà alcun risultato, un altro modo per verificare la pericolosità potenziale del file è quella di vedere l' *original file name*, possiamo quindi sfruttare più campi per trovare processi pericolosi appena creati.

```
k winlog.event_data. Hashes SHA1=4D4DD71069671D64CCD536873BB7C3419FCC  
DF1A,MD5=506C9AED4860F616573BAF6D367C1B3D,S  
HA256=B63410488B190E512926BB617A11A71E502B  
1EADF85EA11D4C5ED950EEC894A6,IMPHASH=F34D5F  
2D4577ED6D9CEEC516C1F5A744
```

```
k winlog.event_data. Apollo.exe  
OriginalFileName
```

Per cui costruiremo una query ad hoc:


```
Q |event.code:"1" and (winlog.event_data.Hashes : *B63410488B190E512926BB617A11A71E502B1EADF85EA11D4C5ED950EEC894A6* or winlog.event_data.OriginalFileName : "Apollo.exe" )
```

Create Alerts and Dashboards


Per creare l'alert andiamo sulla sezione 'Security'-'Rules'-'Detection Rules'-'Create New Rule' (in alto a dx), questa volta dato che non abbiamo delle threshold da superare la regola sarà basata sulla query appena elaborata:

1 Define rule


Rule type

**Custom query**
Use KQL or Lucene to detect issues across indices.

✓ Selected

**Machine Learning**
Access to ML requires a [Platinum subscription](#).

Unavailable

**Threshold**
Aggregate query results to detect when number of matches exceeds threshold.











Select

Da qui impostiamo il campo 'Custom query' con quella elaborata.

I 'Required Fields' saranno:

Required fields ?

Optional

@timestamp	date	
host.name	keyword	
message	text	
winlog.event_data.CommandLine	keyword	
winlog.event_data.Image	keyword	
winlog.event_data.ParentCommandLine	keyword	
winlog.event_data.ParentImage	keyword	
winlog.event_data.ProcessGuid	keyword	
winlog.event_data.User	keyword	
winlog.event_data.CurrentDirectory	keyword	

+ Add required field

Create Alerts and Dashboards

Impostiamo le altre due sezioni come segue e clicchiamo infine su 'Create Rule':

2 About rule

Name

Mythic-C2-Apollo-Agent-Detected

Description

Detects potential c2 apollo agent

Default severity

Select a severity level for all alerts generated by this rule.

● Critical

3 Schedule rule

Runs every

5

Minut... ▼

Rules run periodically and detect alerts within the specified time frame.

Additional look-back time

5

Minut... ▼

Adds time to the look-back period to prevent missed alerts.

Create Alerts and Dashboards

Prima di testarli creiamo una nuova Dashboard, per prima cosa cercheremo eventi di network (quindi come visto in precedenza avranno come **Event ID 3** (processi che avviano connessioni verso l'esterno) , **Event ID 1** (creazione nuovi processi che usano powershell, cmd, rundll32) e **Event ID 5001** (disabilitazione **Windows Defender**).

Per cui andiamo nella sezione 'Discover' per creare le relative queries, testarle e creare poi le dashboard.

Per creare le dashboard andremo sulla relativa sezione, 'Create new dashboard' -> 'Create Visualization', come tipo sceglieremo 'Table' come in figura, e i campi quelli indicati nella regola dell>alert, qui di seguito quella relativa alla prima query con **Event ID 1**.

elastic

Find apps, content, and more.

Dashboards Create

Explore in Discover Inspect Share Settings Cancel Save to library Save and return

.alerts-security.alerts-default,apm-... event.code: "1" and event.provider : "Microsoft-Windows-Sysmon" and (powershell or cmd or rundll32)

winlog.event_data.CurrentDirect ory

Selected fields

Top 3 values of host.name Top 3 values of winlog.event Top 3 values of winlog.event Top 3 values of winlog.event Top 3 values of winlog.event Top 3 values of winlog.event Top 3 values of winlog.event Top 3 values of winlog.event @timestamp per 30 minutes Count of records

Table

.alerts-security.alerts-default,apm-*--transact...

Create Alerts and Dashboards

Specifichiamo che con la query oltre all'**Event Id** cerchiamo eventi generati da **Sysmon** e che creino i processi indicati tra parentesi nella query indicata prima.

Detto ciò riformattiamo la tabella aggiungendo '999' come numero di valori, rinominando i campi e deselezionando 'Group remaining values as "Other"'.
Alla fine rimuoveremo alcuni campi per migliorare la visualizzazione dei dati, il risultato sarà questo:

[No Title]						
User	ParentImage	ParentCommandLine	Image	CommandLine	CurrentDirectory	Count of records
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k n	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" /c	C:\Windows\system32\	1
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k n	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" C	C:\Windows\system32\	1
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k n	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" C	C:\Windows\system32\	1
WIN-JOHNDOE\Administrator	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k n	C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32.exe" S	C:\Windows\system32\	1

Create Alerts and Dashboards

Per proseguire con la creazione della seconda tabella, il processo sarà analogo a quello utilizzato per la prima. La principale differenza riguarda la query e i campi da visualizzare. In particolare, è importante notare che se il campo **winlog.event_data.Initiated** risulta essere true, questo significa che il nostro server sta iniziando una connessione. Questo è un aspetto cruciale per l'analisi della sicurezza, poiché potrebbe indicare attività sospette in uscita dal sistema. Le tab sono state riformattate nello stesso modo della precedente, garantendo una visualizzazione coerente e chiara dei dati. Di seguito, potremo vedere il risultato finale che dovrebbe riflettere la struttura e i campi corretti per questa seconda query.

The screenshot displays a Splunk dashboard interface. At the top, a search bar contains the query: `event.code: "3" and event.provider: "Microsoft-Windows-Sysmon" and winlog.event_data.Initiated: "true" and not winlog.event_data.Image: *MsMpEng.exe`. Below the search bar, the dashboard is divided into three main sections:

- Left Panel:** Contains a search input field with the text `winlog.event_data.DestinationPort`. Below it, there are two sections: "Selected fields" with one item, `winlog.event_data.DestinationPort`, and "Available fields" with two items, `winlog.event_data.DestinationPort` and `winlog.event_data.DestinationPortName`.
- Center Panel:** Displays a table with the following data:
- Right Panel:** Shows a table view configuration for the selected fields, including `Image`, `DestinationIp`, `SourceIp`, and `DestinationPort`.

Image	DestinationIp	SourceIp	DestinationPort	Count of records
C:\Windows\System32\svchost	0:0:0:0:0:0:1	0:0:0:0:0:0:1	5985	2
C:\Windows\System32\svchost	108.61.10.10	155.138.133.204	53	1
C:\Windows\System32\svchost	ff02:0:0:0:0:1:2	fe80:0:0:0:5400:5ff:fe19:7718	547	1
C:\Windows\system32\svchost.	239.255.255.250	127.0.0.1	3702	1
C:\Windows\system32\svchost.	239.255.255.250	155.138.133.204	3702	1
C:\Windows\system32\svchost.	ff02:0:0:0:0:0:c	fe80:0:0:0:5400:5ff:fe19:7718	3702	1

Create Alerts and Dashboards

Infine c'è la terza query destinata alla rilevazione di eventi legati alla disabilitazione di Windows Defender:

The screenshot displays the Splunk dashboard interface. At the top, there's a navigation bar with a menu icon, a 'D' icon, and tabs for 'Dashboards' and 'Create'. On the right, there are links for 'Explore in Discover', 'Inspect', 'Share', 'Settings', 'Cancel', 'Save to library', and a 'Save and return' button. Below the navigation bar, a search bar contains the query: 'event.code: "5001" and event.provider : "Microsoft-Windows-Windows Defender"'. To the right of the search bar are icons for a calendar, 'Today', and a 'Refresh' button. On the left side, there's a sidebar with a search input 'event.code', a 'Selected fields' section with 'event.code', and an 'Available fields' section with 'event.code'. Below these are 'Empty fields' and 'Meta fields' sections. The main area shows a table with the following data:

hostname	Product Name	event.code	Count of records
win-johndoe	Microsoft Defender Antivirus	5001	1

On the right side, there's a 'Table' view selector and a 'Rows' section with input fields for 'hostname', 'Product Name', and 'event.code'.

La dashboard finale sarà questa, la salviamo come 'Suspicious Activity'.

Find apps, content, and more.

Dashboards

Editing New Dashboard

Unsaved changes Settings Share Switch to view mode Save

Filter your data using KQL syntax

Today Refresh

Create visualization Add panel Add from library Controls

Process creation (powershell, cmd , rundll32)

User	ParentImage	ParentCommandLine	Image	CommandLine	CurrentDirectory	Count of records
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r C:\Windows\System32\rundll32.exe		"C:\Windows\system32\rundll32.exe" /c C:\Windows\system32\		1
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r C:\Windows\System32\rundll32.exe		"C:\Windows\system32\rundll32.exe" C C:\Windows\system32\		1
NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r C:\Windows\System32\rundll32.exe		"C:\Windows\system32\rundll32.exe" C C:\Windows\system32\		1
WIN-JOHNDOE\Administrator	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k r C:\Windows\System32\rundll32.exe		"C:\Windows\system32\rundll32.exe" S C:\Windows\system32\		1

Process Initiated Network Connection

Image	DestinationIp	SourceIp	DestinationPort	Count of records
C:\Windows\System32\svchost.exe	0:0:0:0:0:0:1	0:0:0:0:0:0:1	5985	2
C:\Windows\System32\svchost.exe	108.61.10.10	155.138.133.204	53	1
C:\Windows\System32\svchost.exe	ff02:0:0:0:0:0:1:2	fe80:0:0:0:5400:5ff:fe19:7718	547	1
C:\Windows\system32\svchost.exe	239.255.255.250	127.0.0.1	3702	1
C:\Windows\system32\svchost.exe	239.255.255.250	155.138.133.204	3702	1
C:\Windows\system32\svchost.exe	ff02:0:0:0:0:0:0:c	fe80:0:0:0:5400:5ff:fe19:7718	3702	1

Microsoft Defender Disabled

hostname	Product Name	event.code	Count of records
win-johndoe	Microsoft Defender Antivirus	5001	1