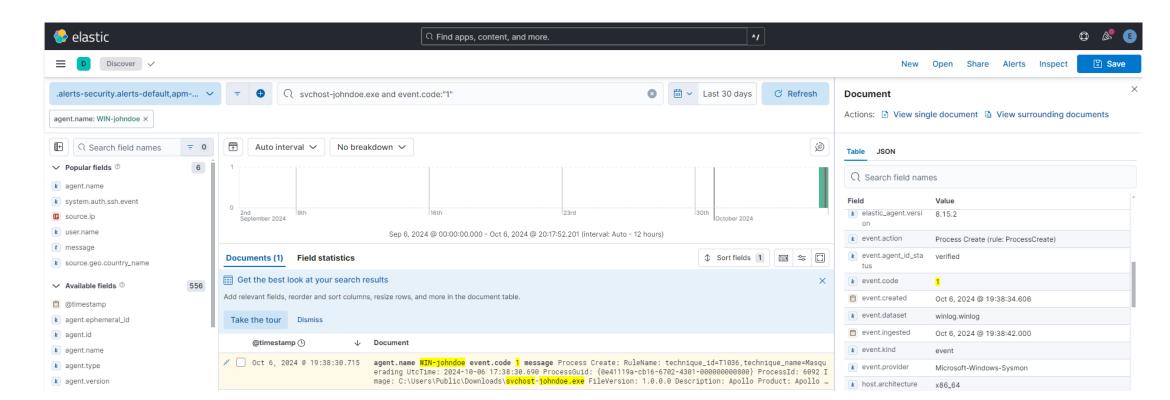
Day 22 - Create Alerts and Dashboards in Kibana - parte 4

CREARE ALERT E DASHBOARD BASATI SULLA TELEMETRIA GENERATA DA MYTHIC

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



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

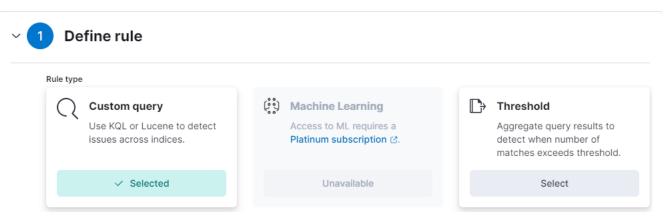
SHA1=4D4DD71069671D64CCD536873BB7C3419FCC DF1A,MD5=506C9AED4860F616573BAF6D367C1B3D,S HA256=B63410488B190E512926BB617A11A71E502B 1EADF85EA11D4C5ED950EEC894A6,IMPHASH=F34D5F 2D4577ED6D9CEEC516C1F5A744

winlog.event_data. Apollo.exe OriginalFileName

Per cui costruiremo una query ad hoc:

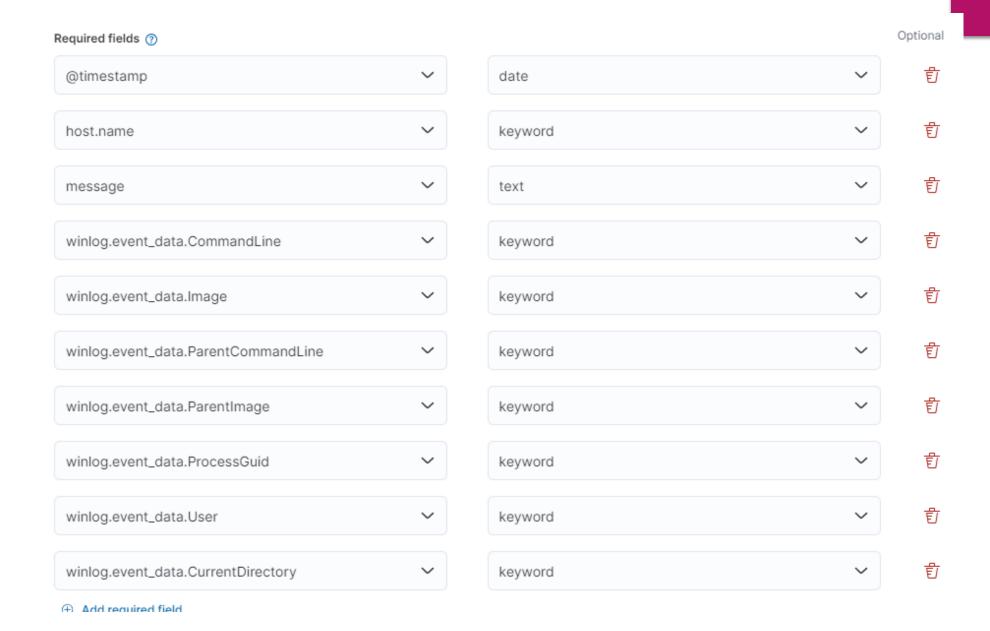
event.code:"1" and (winlog.event_data.Hashes: *B63410488B190E512926BB617A11A71E502B1EADF85EA11D4C5ED950EEC894A6* or winlog.event_data.OriginalFileName: "Apollo.exe")

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:

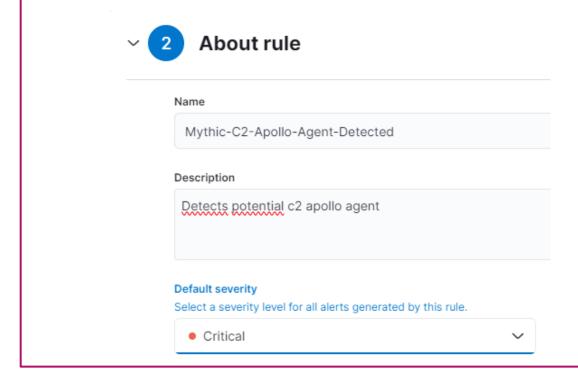


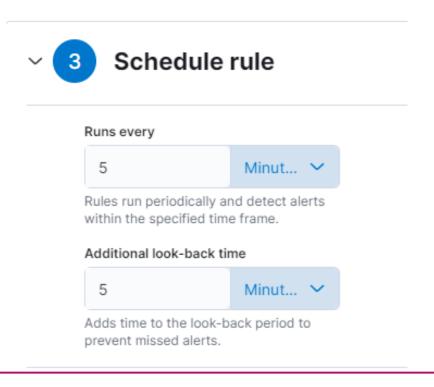
Da qui impostiamo il campo 'Custom query' con quella elaborata.

I 'Required Fields' saranno:



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

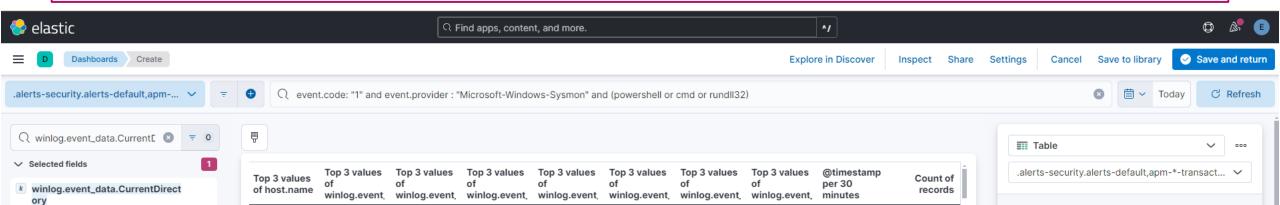




Prima di testarli creiamo una nuova Dashboard, per prima cosa cercheremo eventi di network (quindi come visto in precedenza avranno come **Event ID 3** (processi che avviano connessioni verso l'esterno), **Event ID 1** (creazione nuovi processi che usano powershell, cmd, rundll32) e **Event ID 5001**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



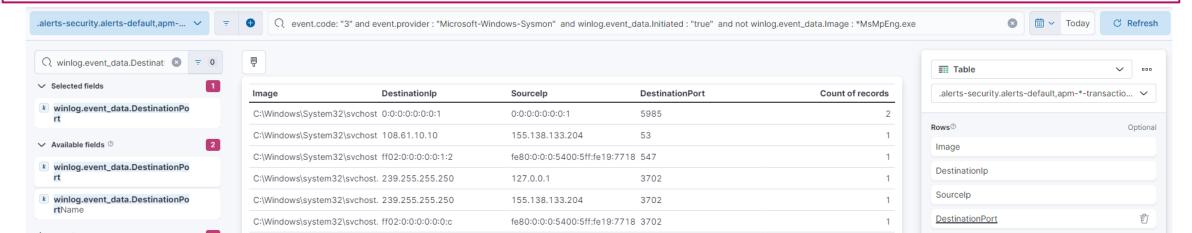
Specifichiamo che con la query oltre all'**Event Id** cerchiamo eventi generati da **Sysmon** e che creino i processi indicati tra parentesi nella query indicata prima.

Detto ciò riformattiamo la tabella aggiungendo '999' come numero di valori, rinominando i campi e deselezionando 'Group remaining values as "Other".

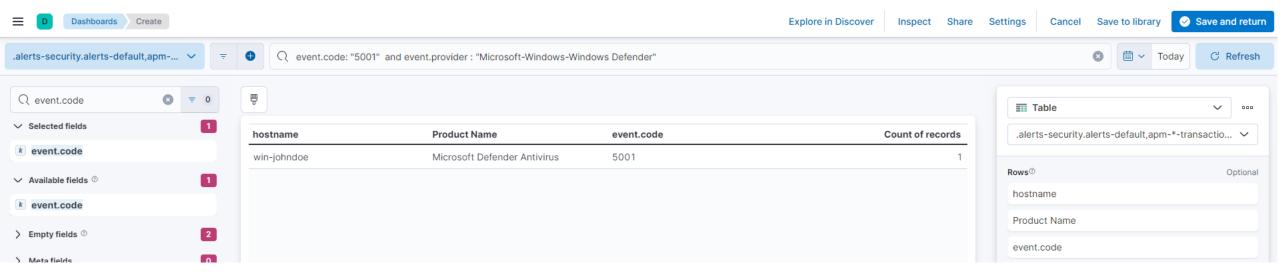
Alla fine rimuoveremo alcuni campi per migliorare la visualizzazione dei dati, il risultato sarà questo:

[No Title]					
Parentlmage	ParentCommandLine	Image	CommandLine	CurrentDirectory	Count of records
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe	-k n C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32	e.exe"/c C:\Windows\system32\	1
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe	-k n C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32	2.exe" C C:\Windows\system32\	1
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe	-k n C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32	2.exe" C C:\Windows\system32\	1
C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe	-k n C:\Windows\System32\rundll32.exe	"C:\Windows\system32\rundll32	2.exe" St C:\Windows\system32\	1
	C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe

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.



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



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

