

MONITORING DI SPLUNK

Traccia: Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora". Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

Svolgimento:

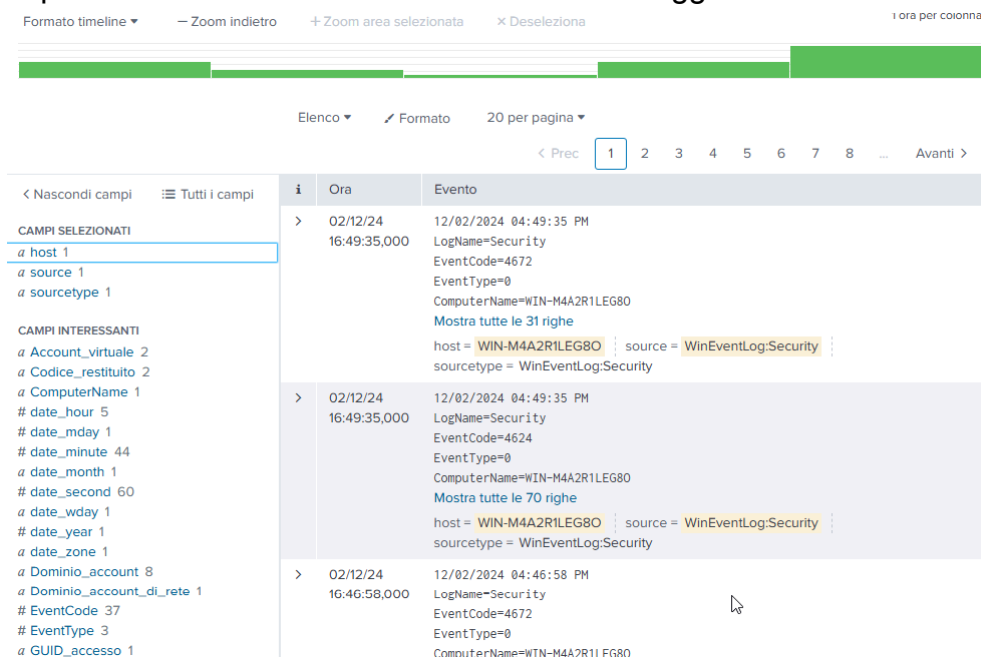
Nell'esercizio di oggi si chiede di eseguire il monitoraggio del dispositivo locale utilizzando Splunk per muovere i primi passi nella lettura e nella comprensione dei dati all'interno di un sistema Siem.

Splunk è una piattaforma software che aiuta a raccogliere, monitorare, analizzare e visualizzare grandi volumi di dati generati da macchine, come i log di sistema, applicazioni o dispositivi di rete. È particolarmente utile per attività come la gestione e l'analisi della sicurezza, il monitoraggio delle infrastrutture IT, la risoluzione dei problemi e l'ottimizzazione delle performance. Splunk serve a convertire i dati grezzi in informazioni utili attraverso dashboard, ricerche e alert, facilitando la comprensione e la gestione in tempo reale di sistemi complessi.

Monitoring

Per cominciare, si è installato Splunk Enterprise su Windows Server.

Per analizzare dei file di log, si va nella sezione apposita, utile a monitorare un sistema locale o altro. In questo caso abbiamo analizzato il local host, quindi lo stesso dispositivo da cui stiamo effettuando il monitoraggio.



The screenshot displays the Splunk Monitoring interface. At the top, there are navigation controls including 'Formato timeline', 'Zoom indietro', '+ Zoom area selezionata', 'X Deseleziona', and '1 ora per colonna'. Below these is a search bar with 'Elenco', 'Formato', and '20 per pagina' options. A table of events is shown with columns for 'Ora' and 'Evento'. The left sidebar contains a list of fields under 'CAMPI SELEZIONATI' and 'CAMPI INTERESSANTI'.

i	Ora	Evento
>	02/12/24 16:49:35,000	12/02/2024 04:49:35 PM LogName=Security EventCode=4672 EventType=0 ComputerName=WIN-M4A2R1LEG80 Mostra tutte le 31 righe host = WIN-M4A2R1LEG80 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	02/12/24 16:49:35,000	12/02/2024 04:49:35 PM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-M4A2R1LEG80 Mostra tutte le 70 righe host = WIN-M4A2R1LEG80 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	02/12/24 16:46:58,000	12/02/2024 04:46:58 PM LogName=Security EventCode=4672 EventType=0 ComputerName=WIN-M4A2R1LEG80

Come possiamo vedere, l'output che otterremo sarà l'elenco degli eventi locali, che specificano l'host da cui i dati sono stati prelevati.

Nella colonna a sinistra, potremo visualizzare l'elenco dei campi selezionati ed interessanti, che servono ad ottimizzare la ricerca in base a criteri precisi. C'è anche la possibilità di creare e personalizzare un campo allo scopo di migliorare la ricerca.

```
CAMPI SELEZIONATI
a host 1
a source 1
a sourcetype 1

CAMPI INTERESSANTI
a Account_virtuale 2
a Codice_restituito 2
a ComputerName 1
# date_hour 5
# date_mday 1
# date_minute 44
a date_month 1
# date_second 60
a date_wday 1
# date_year 1
a date_zone 1
a Dominio_account 8
a Dominio_account_di_rete 1
# EventCode 37
# EventType 3
a GUID_accesso 1
a ID_accesso 53
a ID_accesso_collegato 21
a ID_processo 100+
```

Ora andremo a vedere l'esempio di un evento aperto, che ci mostrerà tutti i campi selezionati e selezionabili. Ci darà tutte le informazioni in un formato più comprensibile in quanto, come detto prima, Splunk riesce a trasformarli in dati non grezzi.

16:49:35,000 LogName=Security
EventCode=4624
EventType=0
ComputerName=WIN-M4A2R1LEG80
[Mostra tutte le 70 righe](#)

Azioni evento ▼

Tipo	<input checked="" type="checkbox"/>	Campo	Valore	Azioni
Selezionato	<input checked="" type="checkbox"/>	host ▼	WIN-M4A2R1LEG80	▼
	<input checked="" type="checkbox"/>	source ▼	WinEventLog:Security	▼
	<input checked="" type="checkbox"/>	sourcetype ▼	WinEventLog:Security	▼
Evento	<input type="checkbox"/>	Account_virtuale ▼	No	▼
	<input type="checkbox"/>	ComputerName ▼	WIN-M4A2R1LEG80	▼
	<input type="checkbox"/>	Dominio_account ▼	WORKGROUP	▼
	<input type="checkbox"/>	Dominio_account_di_rete ▼	NT AUTHORITY	▼
	<input type="checkbox"/>	Dominio_account_di_rete ▼	-	▼
	<input type="checkbox"/>	EventCode ▼	4624	▼
	<input type="checkbox"/>	EventType ▼	0	▼
	<input type="checkbox"/>	GUID_accesso ▼	{00000000-0000-0000-0000-000000000000}	▼
	<input type="checkbox"/>	ID_accesso ▼	0x3E7	▼
	<input type="checkbox"/>	ID_accesso_collegato ▼	0x0	▼

Conclusioni

In questa esercitazione abbiamo approfondito l'uso della modalità "Monitora" offerta da Splunk.

Attraverso la configurazione di questa funzionalità, abbiamo appreso come Splunk possa essere utilizzato per monitorare in tempo reale i dati provenienti da diverse fonti, consentendo una gestione efficace delle informazioni e una rapida individuazione di eventuali anomalie.

Gli screenshot allegati documentano l'avvenuta configurazione e dimostrano la corretta esecuzione del compito. Questa attività ha fornito una comprensione pratica dell'uso di Splunk per il monitoraggio continuo, sottolineando l'importanza della piattaforma per il controllo dei dati in ambienti complessi.

*Progetto a cura di
Sonia Laterza*