



S10-E1

Umberto Valentini

Page 01

Monitorazione Splunk

S10-E1



Table of content

- 02. Indice**
- 03. Obiettivo**
- 04. Cos'è Splunk**
- 05. Setting monitoraggio**
- 06. Interfaccia di analisi**
- 07. Dettagli evento**

Obiettivo

L'esercizio prevede la configurazione della modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.



Cosa è Splunk



Un SIEM (Security Information and Event Management) è una soluzione che centralizza la raccolta e l'analisi dei log di sistema, combinandoli con il monitoraggio degli eventi di sicurezza per rilevare e rispondere alle minacce. Grazie alla correlazione degli eventi e al monitoraggio in tempo reale, il SIEM identifica comportamenti anomali e supporta l'automazione delle risposte. È uno strumento essenziale per migliorare la sicurezza e garantire la compliance normativa.

In questo ambito, Splunk si distingue come una piattaforma versatile e potente, in grado di raccogliere, indicizzare e analizzare enormi volumi di dati da qualsiasi sorgente. Offre analisi avanzate, alerting in tempo reale e visualizzazioni interattive. Grazie alla scalabilità e al supporto per il machine learning, Splunk aiuta le organizzazioni a ottimizzare la sicurezza e a trasformare i dati in insight strategici.

Splunk è una scelta eccellente come SIEM per diverse ragioni, che vanno dalla sua flessibilità alla sua capacità di scalare in ambienti complessi. Fondamentale la sua scalabilità, ovvero la sua capacità di essere adattabile alla grandezza dell'azienda.

The screenshot shows the 'Aggiungi dati' (Add Data) wizard in the Splunk interface. The top navigation bar includes options for 'Carica' (Upload), 'Monitora' (Monitoring), and 'Inoltra' (Forward). The 'Monitora' option is highlighted with a green icon and a cursor. Below the navigation are three tabs: 'Log di eventi locali' (Local Log Events), 'Log di eventi remoti' (Remote Log Events), and 'File e directory' (Files and Directories). The 'Log di eventi locali' tab is selected. A progress bar at the top indicates the steps: 'Selezione source' (Select Source) (green dot), 'Impostazioni di input' (Input Settings) (white dot), 'Verifica' (Review) (white dot), and 'Fine' (Finish) (white dot). The main content area for 'Log di eventi locali' contains the text: 'Configure this instance to monitor local Windows Event Log channels, services, and system processes send data. This monitor runs once you define.' followed by a link 'Ulteriori informazioni'. Below this is a dropdown menu labeled 'Selezione log eventi' (Select log events) with options 'Disponibilelemento/i' (Available elements) and 'Application' (selected). The bottom section, titled 'Impostazioni di input' (Input Settings), provides instructions for setting up input parameters and includes a 'Host' configuration example where the 'Valore campo' (Field value) 'Host' is set to '9K104BT'.

Setting del monitoraggio

Splunk ha un'interfaccia intuitiva, seguendo la voce “Cerca dati”, presente nella home del software, abbiamo la possibilità di trovare la scelta “Monitora”.

I passi sono pochi e semplici, settiamo:

- Provenienza dati da analizzare.
- Log da mettere in evidenza nella ricerca dati.
- L'host preso in esame, quindi il nome della sua macchina.

Semplice e conciso, con poche impostazioni possiamo avviare l'analisi dati.

Interfaccia di analisi

windows host="DESKTOP-9K104BT" source="WinEventLog:*

✓ 135.073 eventi (01/12/24 17:00:00,000 - 02/12/24 17:45:12,000) Nessun campionamento degli eventi ▾ Processo ▾ Modalità intelligente ▾

Eventi (135.073) Pattern Statistiche Visualizzazione

Formato timeline ▾ - Zoom indietro + Zoom area selezionata × Deseleziona 1 ora per colonna

	Ora	Evento
>	02/12/24 17:45:11,000	... 4 lines omitted ... ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni ... 18 lines omitted ... ID processo: 0xc7c Nome processo: C:\Windows\System32\wbem\WmiPrvSE.exe Mostra tutte le 27 righe host = DESKTOP-9K104BT source = WinEventLog:Security sourcetype = WinEventLog:Security
>	02/12/24 17:45:11,000	... 4 lines omitted ... ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni ... 18 lines omitted ... ID processo: 0xc7c Nome processo: C:\Windows\System32\wbem\WmiPrvSE.exe Mostra tutte le 27 righe host = DESKTOP-9K104BT source = WinEventLog:Security sourcetype = WinEventLog:Security
>	02/12/24 17:45:11,000	... 4 lines omitted ... ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni ... 18 lines omitted ...

Elenco ▾ Formato 20 per pagina ▾ 1 2 3 4 5 6 7 8 ... Avanti >

< Nascondi campi CAMPI SELEZIONATI ▾ Tutti i campi ▾ host 1 source 3 sourcetype 3 CAMPI INTERESSANTI ComputerName 1 Dominio_account 6 EventCode 71 EventType 5 ID_accesso 19 ID_processo 34 ID_sicurezza 17 index 1 Keywords 4 linecount 17 LogName 3 Message 100+ Nome_account 15 Nome_processo 10 OpCode 5 punct 89 RecordNumber 100+ SourceName 32

Ultime 24 ore ▾ Q

C:\Windows\system32\cmd.exe

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::1:1%1
Indirizzo IPv4. : 192.168.1.83
Subnet mask : 255.255.255.0
Gateway predefinito : 192.168.1.254

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}

Stato supporto. : Supporto discorso
Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 : 2001:192.168.1.83
Indirizzo IPv6 locale rispetto al collegamento . : fe80::1:1%1
Gateway predefinito :

C:\Users\user>hostname
DESKTOP-9K104BT

C:\Users\user>

Dettagli evento

Ora	Evento
02/12/24 17:45:11,000	12/02/2024 05:45:11 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni RecordNumber=1673963 Keywords=Controllo riuscito TaskCategory=Gestione account utente OpCode=Informazioni Message=È stata enumerata l'appartenenza a un gruppo locale di un utente.
Soggetto:	
ID sicurezza:	S-1-5-18
Nome account:	DESKTOP-9K104BT\$
Dominio account:	WORKGROUP
ID accesso:	0x3E7
Utente:	
ID sicurezza:	S-1-5-21-1859916961-34304393-1824526448-1003
Nome account:	WmsControl
Dominio account:	DESKTOP-9K104BT
Informazioni sul processo:	
ID processo:	0xc7c
Nome processo:	C:\Windows\System32\wbem\WmiPrvSE.exe
Comprimi	

Ora	Evento
02/12/24 17:45:11,000	... 4 lines omitted ... ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni ... 18 lines omitted ... ID processo: 0xc7c Nome processo: C:\Windows\System32\wbem\WmiPrvSE.exe Mostra tutte le 27 righe
	Azioni evento ▾
	Tipo ✓ Campo Valore
Selezionato	<input checked="" type="checkbox"/> host DESKTOP-9K104BT <input checked="" type="checkbox"/> source WinEventLog:Security <input checked="" type="checkbox"/> sourcetype WinEventLog:Security
Evento	<input type="checkbox"/> ComputerName DESKTOP-9K104BT <input type="checkbox"/> Dominio_account WORKGROUP DESKTOP-9K104BT <input type="checkbox"/> EventCode 4798 <input type="checkbox"/> EventType 0 <input type="checkbox"/> ID_accesso 0x3E7 <input type="checkbox"/> ID_processo 0xc7c <input type="checkbox"/> ID_sicurezza S-1-5-18 S-1-5-21-1859916961-34304393-1824526448-1003 <input type="checkbox"/> Keywords Controllo riuscito <input type="checkbox"/> LogName Security <input type="checkbox"/> Message È stata enumerata l'appartenenza a un gruppo locale di un utente. Soggetto: ID sicurezza: S-1-5-18 Nome account: DESKTOP-9K104BT\$ Dominio account: WORKGROUP ID accesso: 0x3E7 Utente: ID sicurezza: S-1-5-21-1859916961-34304393-1824526448-1003 Nome account: WmsControl Dominio account: DESKTOP-9K104BT Informazioni sul processo: ID processo: 0xc7c Nome processo: C:\Windows\System32\wbem\WmiPrvSE.exe

L'analisi del file, mette in evidenza la traccia di un Ping Of Death, potremmo quasi dire “Firmato”.

Si del file, mette in
nza la traccia di un
f Death, potremmo
dire "Firmato".

Eventi (62) Pattern Statistiche Visualizzazione

Formato timeline ▾ – Zoom indietro + Zoom area selezionata × Deselezione 1 ora per colonna

Elenco ▾ Formato 20 per pagina ▾ < Prec 1 2 3 4 Avanti >

< Nascondi campi CAMPI SELEZIONATI ▾ Tutti i campi a description 6

i	Ora	Evento
>	02/06/24 00:30:00,000	2024-06-02 00:30:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	02/06/24 00:00:00,000	2024-06-02 00:00:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 23:30:00,000	2024-06-01 23:30:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 23:00:00,000	2024-06-01 23:00:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 22:30:00,000	2024-06-01 22:30:00,Ping of Death Attack,192.168.1.22,10.0.0.1,Ping of Death attack detected on Epicode.com by Elliot,Large ICMP packet causing disruption description = Ping of Death attack detected on Epicode.com by Elliot host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 22:00:00,000	2024-06-01 22:00:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 21:30:00,000	2024-06-01 21:30:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 21:00:00,000	2024-06-01 21:00:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 20:30:00,000	2024-06-01 20:30:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv
>	01/06/24 20:00:00,000	2024-06-01 20:00:00,Normal Access,,,Normal access log, description = Normal access log host = Windows source = Shadow (1).zip:\Shadow.csv sourcetype = csv

additional_info 13 Valori, 20,968% di eventi Selezionato Si No >

Report Primi valori Primi valori nel tempo Valori rari

Eventi con questo campo

Primi 10 valori Conteggio %

Brute force password attack detected	1	7,692%
Email spoofing attempt detected	1	7,692%
Encoded URL contains suspicious patterns	1	7,692%
Excessive traffic causing slowdown	1	7,692%
High number of SYN packets	1	7,692%
JavaScript alert function found	1	7,692%
Large ICMP packet causing disruption	1	7,692%
Multiple failed login attempts	1	7,692%
Multiple requests from same IP	1	7,692%
Phishing email with malicious link	1	7,692%

