

ESERCIZIO S10 L1



Pratica S10/L1 PDF

Cyber Security & Ethical Hacking
Esercizio

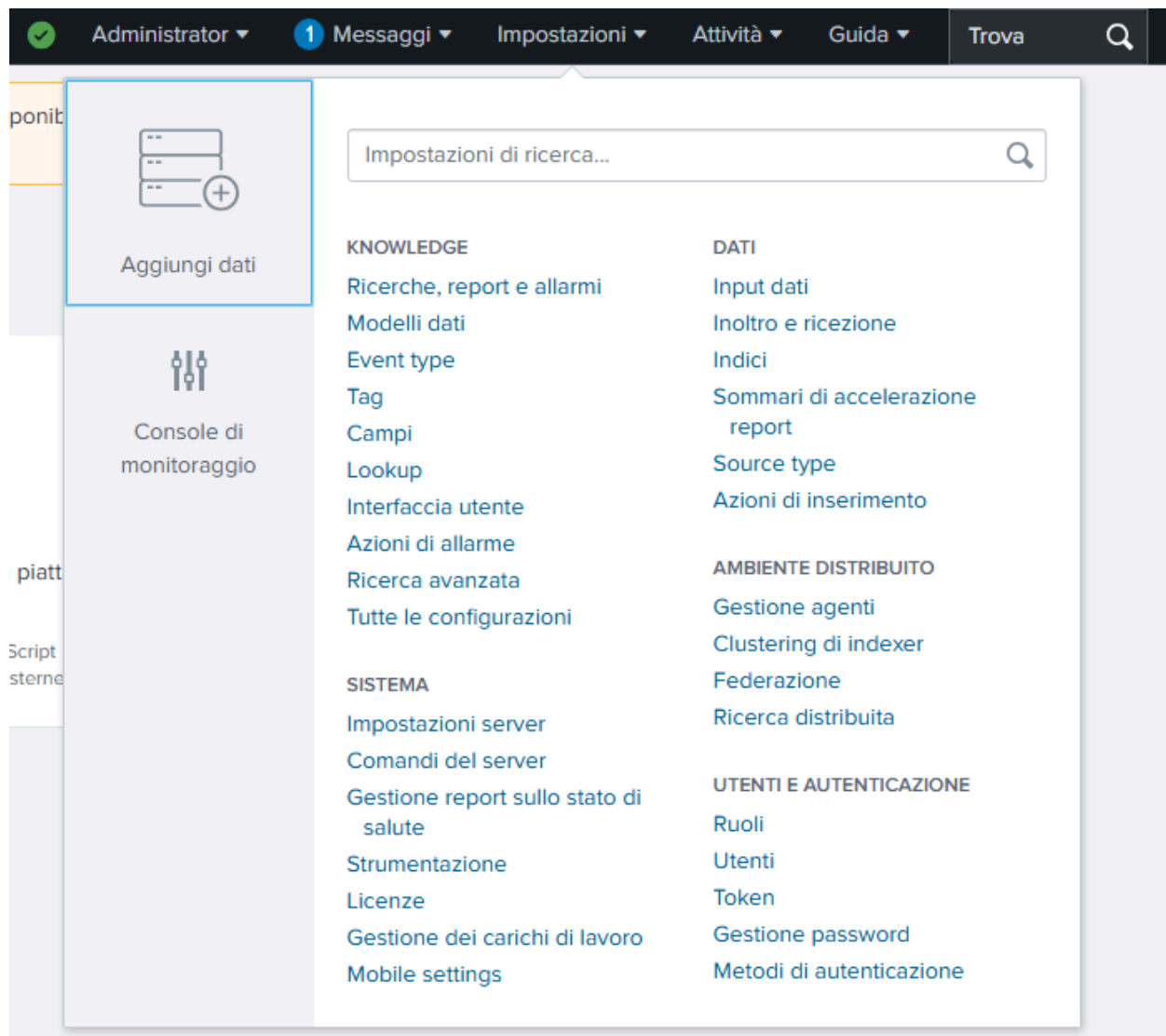
Esercizio di oggi: Configurazione della Modalità Monitora in Splunk

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

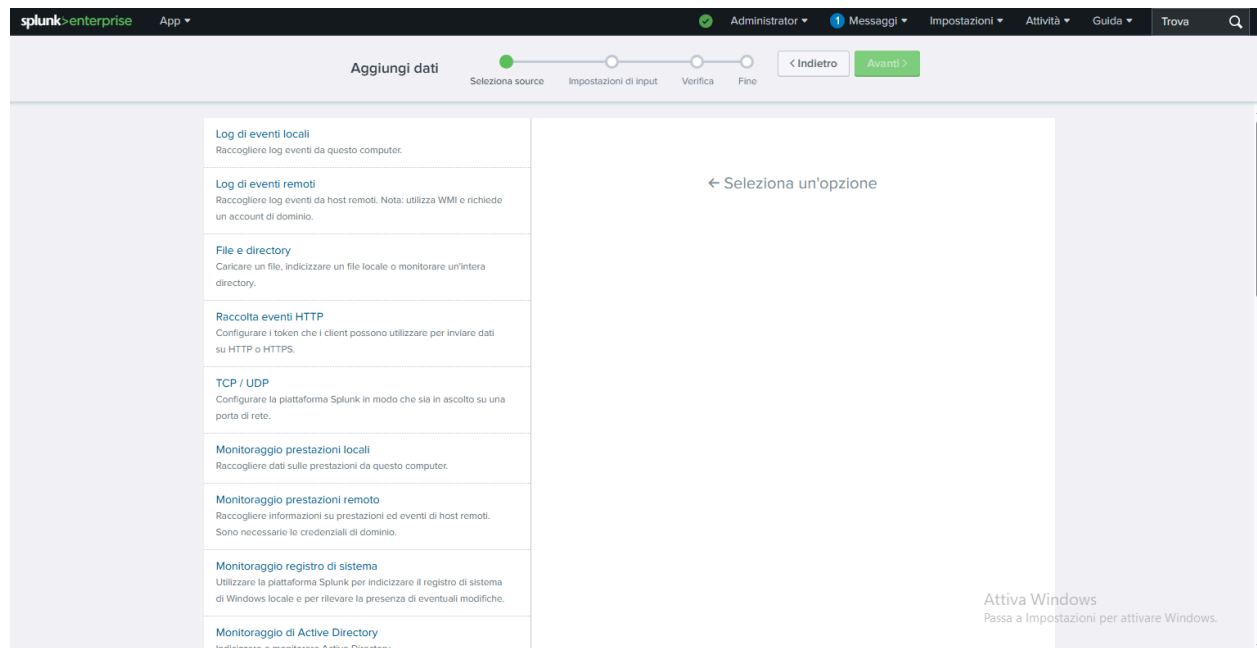
Navigo innanzitutto nella sezione **Impostazioni**, poi clicco su **Aggiungi dati**



Come richiesto dalla traccia questa volta selezioniamo l'azione **Monitora** :



Seleziono a questo punto la prima sezione : **Log di eventi locali**



Ora, scelgo le impostazioni desiderate, in questo caso seleziono **Security**

Aggiungi dati

< Indietro

Avanti >

Log di eventi locali

Raccogliere log eventi da questo computer.

Log di eventi remoti

Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.

File e directory

Caricare un file, indicizzare un file locale o monitorare un'intera directory.

Raccolta eventi HTTP

Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.

TCP / UDP

Configurare la piattaforma Splunk in modo che sia in ascolto su una

Configura questa istanza per monitorare canali Log Windows dove applicazioni, servizi, e processi di sistema inviano dati. Questo monitor si esegue una volta per ogni input di Log eventi che definisci. [Ulteriori informazioni](#)

Seleziona log eventi

Disponibile elemento/i

aggiungi tutto »

Application

Security

Setup

System

ForwardedEvents

DirectShowPluginControl

Els_Hyphenation/Analytic

EndpointMapper

FirstUXPerf-Analytic

Seleziona toe

Security

Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.

Clicco su **Avanti**

Aggiungi dati

< Indietro

Verifica >

Impostazioni di input

In alternativa, impostare ulteriori parametri di input per questo input di dati come segue:

Host

Quando la piattaforma Splunk indicizza i dati, ciascun evento riceve un valore "host". Il valore host deve essere il nome della macchina da cui ha origine l'evento. Il tipo di input scelto determina le opzioni di configurazione disponibili. [Ulteriori informazioni](#)

Valore campo

Host

SplunkServer

Indice

La piattaforma Splunk archivia i dati in entrata come eventi nell'indice selezionato. Valutare l'uso di un indice "sandbox" come destinazione se si hanno problemi a determinare un corso tipo per i propri dati. Un indice sandbox consente di

Indice

Default ▾

[Crea un nuovo indice](#)

Seleziono **Verifica**

Aggiungi dati

< Indietro

Invia >

Verifica

Tipo di input

Log eventi di Windows

Log eventi

Security

Contesto app

search

Host

SplunkServer

Indice

default

Seleziono Invio e successivamente **Avvia Ricerca**

Aggiungi dati

Seleziona source Impostazioni di input Verifica Fine

< Indietro Avanti >

✓ Log eventi locali (input) è stato creato correttamente.
Configurare gli input da Impostazioni > [Input dati](#)

Avvia ricerca Eseguire una ricerca tra i dati ora oppure visualizzare [esempi ed esercitazioni](#). [🔗](#)

Aggiungi altri dati Aggiungere altri input di dati ora oppure visualizzare [esempi ed esercitazioni](#). [🔗](#)

Scarica app Le app consentono di fare di più con i propri dati. [Ulteriori informazioni](#). [🔗](#)

Crea dashboard Visualizza le ricerche. [Ulteriori informazioni](#). [🔗](#)

Ecco la schermata di risultato :

Nuova ricerca

Salva come Crea vista tabella Chiudi

source="WinEventLog:*" host="SplunkServer"

Intervallo temporale: Sempre 🔍

✓ 4.768 eventi (prima di 15/09/25 13:51:39,000) Nessun campionamento degli eventi

Processo

Eventi (4.768) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro Zoom area selezionata Deseleziona 1 mese per colonna

Formato Mostra: 20 per pagina Visualizza: Elenco

i	Ora	Evento
>	15/09/25 13:40:23,000	09/15/2025 01:40:23 PM LogName=Security EventCode=5061 EventType=0 ComputerName=SplunkServer Mostra tutte le 28 righe
>	15/09/25 13:40:23,000	09/15/2025 01:40:23 PM LogName=Security EventCode=5058 EventType=0 ComputerName=SplunkServer Mostra tutte le 33 righe
>	15/09/25 13:38:57,000	09/15/2025 01:38:57 PM LogName=Security EventCode=4672 EventType=0 ComputerName=SplunkServer Mostra tutte le 31 righe

Attiva Windows
Passa a Impostazioni per attivare Windows.

La presenza degli eventi log dimostrano il corretto funzionamento del procedimento con Splunk della sezione **Monitora**. Sono presenti di fatto **4.768 eventi**.

source="WinEventLog:*" host="SplunkServer"

✓ 4.768 eventi (prima di 15/09/25 13:51:39,000)

Questo è un esempio di evento dove viene mostrata data, ora e caratteristiche.
Host >>> Source >>> Sourcetype

i	Ora	Evento
>	15/09/25 13:40:23,000	09/15/2025 01:40:23 PM LogName=Security EventCode=5061 EventType=0 ComputerName=SplunkServer Mostra tutte le 28 righe host = SplunkServer source = WinEventLog:Security sourcetype = WinEventLog:Security

Possiamo cliccare su **Mostra tutte le 28 righe** dove è possibile visualizzare più dettagli dell'evento.

```
> 15/09/25      09/15/2025 01:40:23 PM
13:40:23,000    LogName=Security
                EventCode=5061
                EventType=0
                ComputerName=SplunkServer
                SourceName=Microsoft Windows security auditing.
                Type=Informazioni
                RecordNumber=4768
                Keywords=Controllo riuscito
                TaskCategory=System Integrity
                OpCode=Informazioni
                Message=Operazione di crittografia.

Soggetto:
  ID sicurezza:      S-1-5-18
  Nome account:      SPLUNKSERVER$
  Dominio account:   WORKGROUP
  ID accesso:        0x3E7

Parametri di crittografia:
  Nome provider:     Microsoft Software Key Storage Provider
  Nome algoritmo:     RSA
  Nome chiave:        C:\Program Files\Splunk\etc\auth\server.pem.pfx
  Tipo di chiave:     Chiave computer.

Operazione di crittografia:
  Operazione:        Apri una chiave.
  Codice restituito:   0x0

Comprimi
host = SplunkServer | source = WinEventLog:Security | sourcetype = WinEventLog:Security
```

Attiva Windows

Per informazioni sui problemi di attivazione, visitate il sito di supporto di Windows.