# Consegna S10-L1

## Consegna: Configurazione della Modalità Monitora in Splunk

⚜️ **Tag:** #splunk #monitoraggio #configurazione #cybersecurity

### Traccia

Abbiamo esplorato diverse funzionalità offerte da **Splunk**. Oggi ci concentreremo sulla modalità **"Monitora"**.

### Obiettivo

Configurare la modalità "Monitora" in Splunk e realizzare screenshot che confermino l’avvenuta configurazione.

---

### Istruzioni

1. **Accesso a Splunk:**
    - Aprire il browser e accedere all’istanza di Splunk all'indirizzo configurato.
    - Effettuare il login con le credenziali fornite (es. admin / password).
2. **Navigare nella Modalità Monitora:**
    - Dal pannello principale, cliccare su **Settings**.
    - Selezionare **Data Inputs**.
    - Cliccare su **Monitor**.
3. **Aggiungere una Sorgente da Monitorare:**
    - Scegliere il tipo di sorgente dati (es. file o directory).

- Specificare il percorso assoluto della sorgente (es. `/var/log/syslog`).
- Configurare eventuali filtri o escludere percorsi specifici.

4. **Configurare le Opzioni di Monitoraggio:**
   - Assegnare un **sourcetype** appropriato alla sorgente.
   - Specificare l'**indice** in cui salvare i dati monitorati.
   - Verificare le opzioni avanzate per personalizzare la configurazione.
5. **Salvare e Verificare la Configurazione:**
   - Salvare le impostazioni e attendere che Splunk inizi a raccogliere i dati.
   - Navigare nella sezione **Search & Reporting** per verificare i log acquisiti.
6. **Screenshot della Configurazione:**
   - Documentare i passaggi effettuati con screenshot:
     - Pannello di configurazione della modalità Monitora.
     - Visualizzazione dei dati monitorati nella sezione di ricerca.

---

## Conclusione

Questo esercizio consente di comprendere l'importanza della configurazione del monitoraggio in Splunk, fornendo competenze pratiche per l'osservazione e l'analisi dei dati in tempo reale.

---

🔑 **Chiavi:**
[splunk, monitoraggio, configurazione, cybersecurity]