S10L1

Conti Mirco

Data: 02/12/24

INFORMAZIONI PRINCIPALI

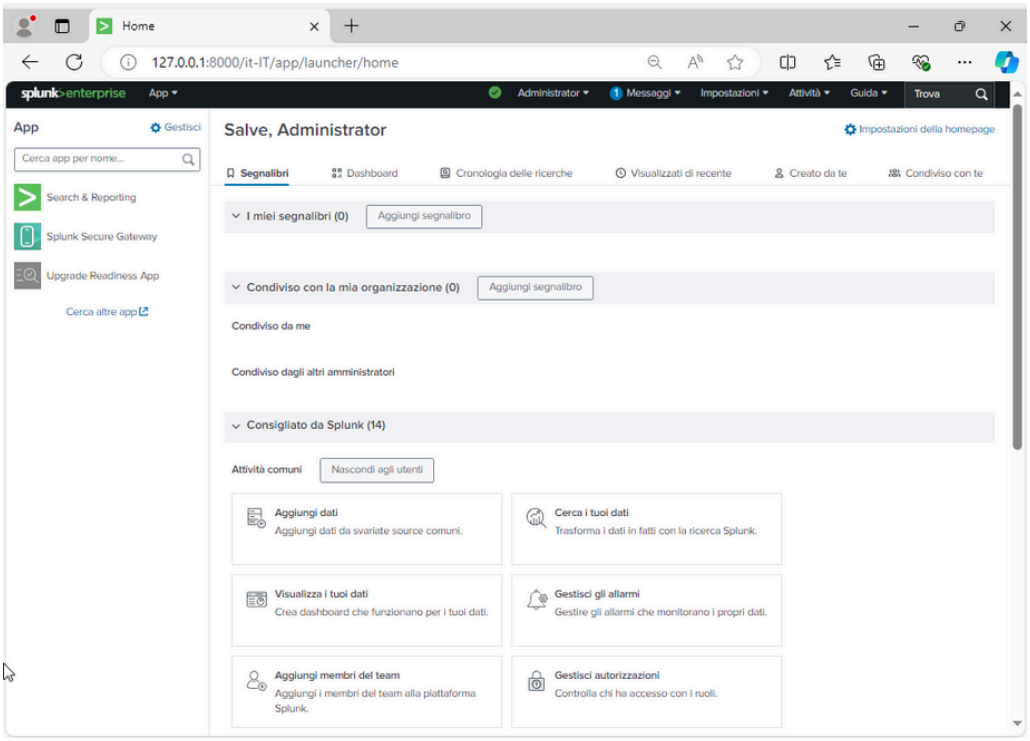
Esercizio di oggi: Configurazione della Modalità Monitora in Splunk Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora".

Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

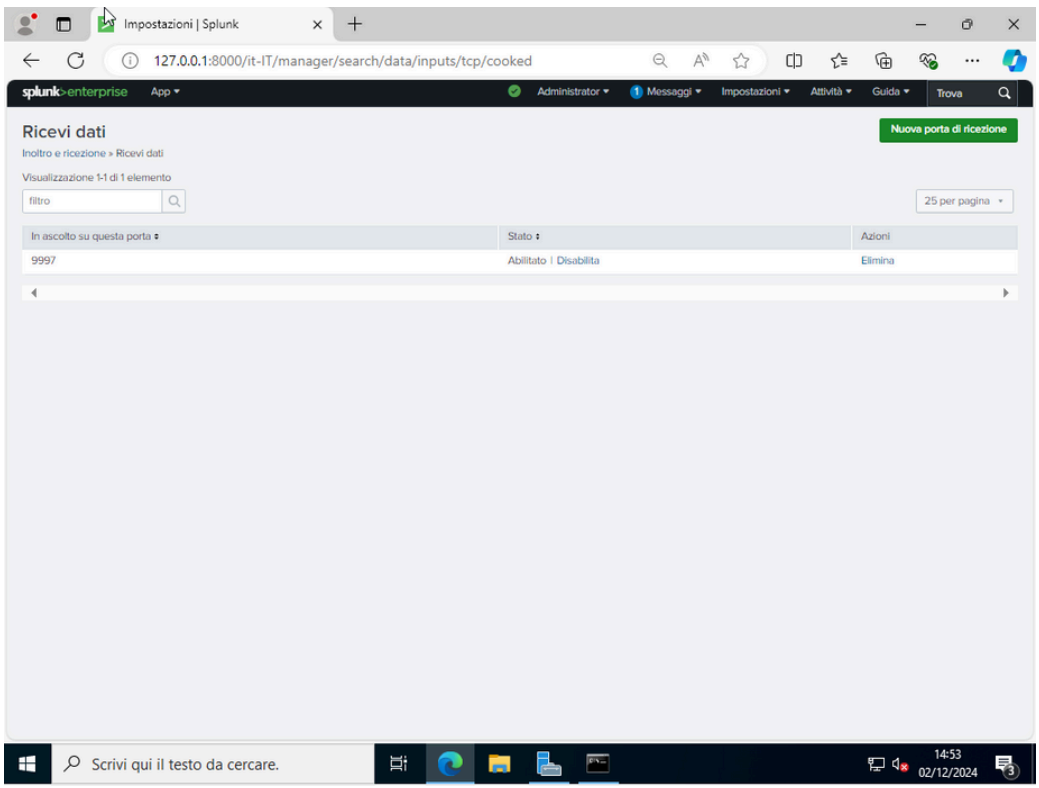
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

INIZIO ESERCIZIO

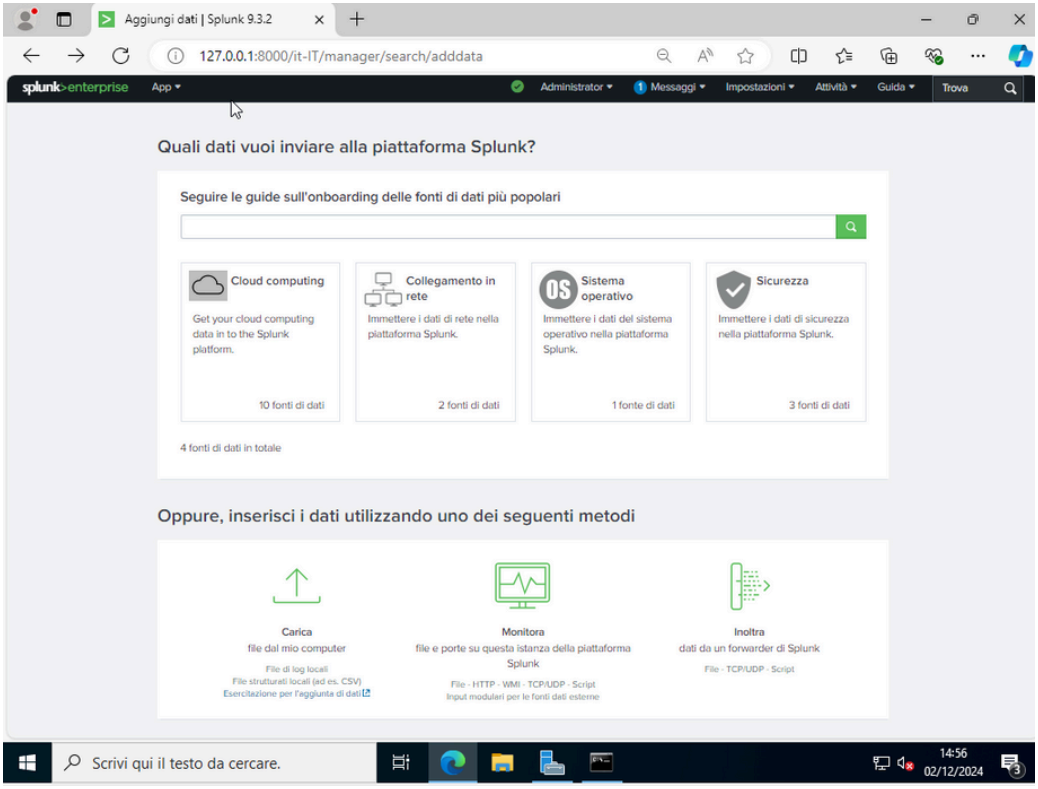
Dopo aver installato splunk forwarder su Windows 10 e Splunk enterprise su Windows server 2022, ho impostato la porta di ascolto (listening port) per abilitare la recezione dei log dalla macchina configurata (Desktop-9K104BT)



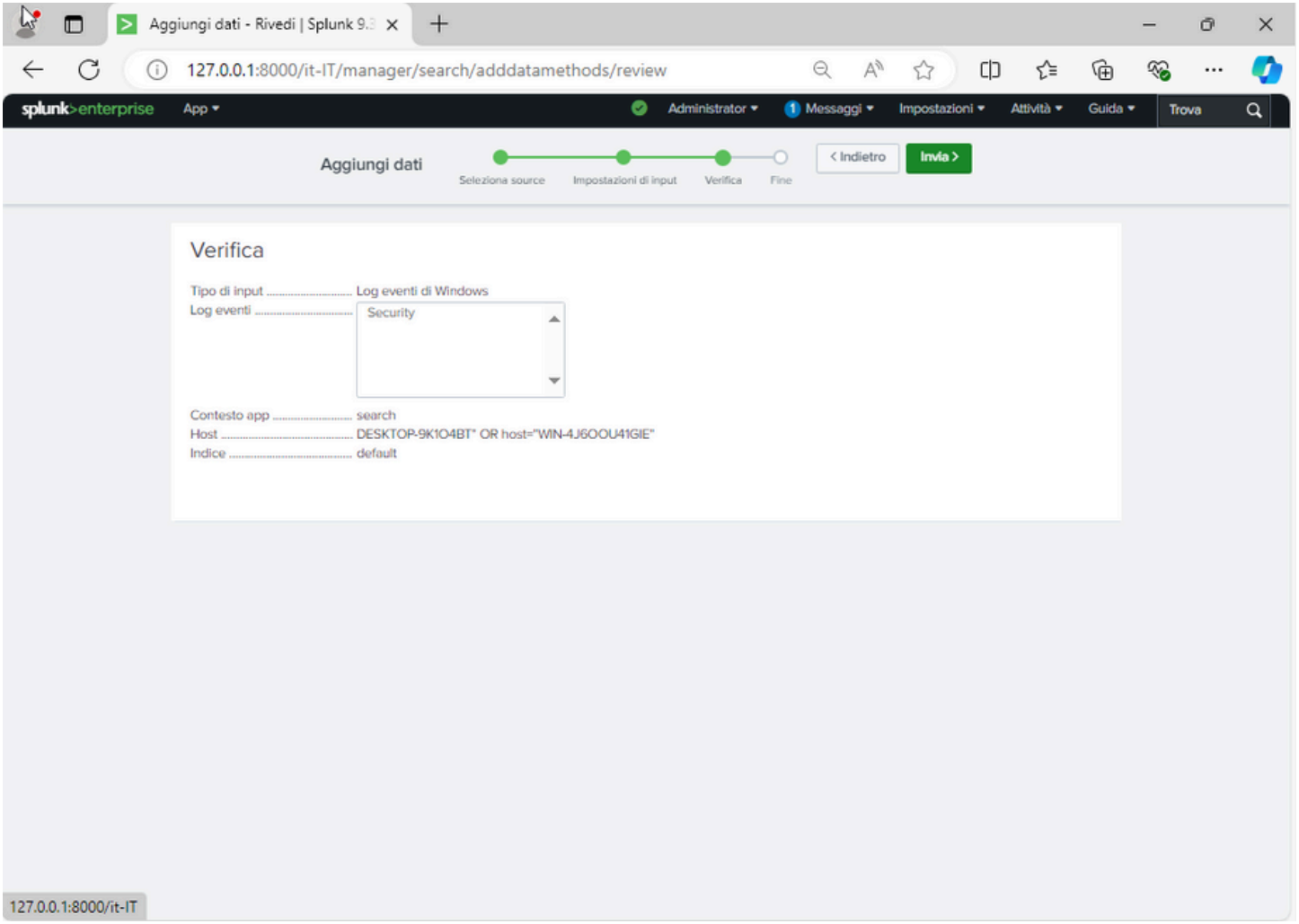
Clicchiamo impostazioni, inoltro e ricezione,configura ricezione.



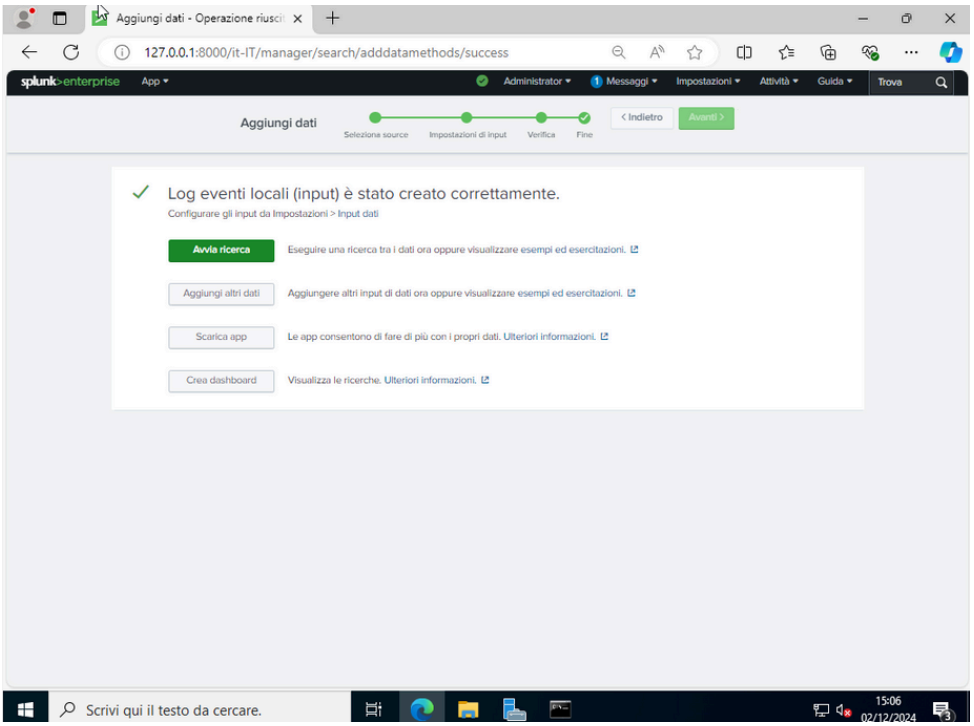
Impostiamo la porta che abbiamo configurato anche su splunk portforward (9997) e la abilitiamo. Una volta fatto questo partiamo con la ricerca, torniamo sulla homepage e premiamo “aggiungi dati”, a seguire monitora e selezionamo l’evento “security” (interessato dall’esercizio) ci darà tutti gli eventi relativi alla sicurezza di windows.



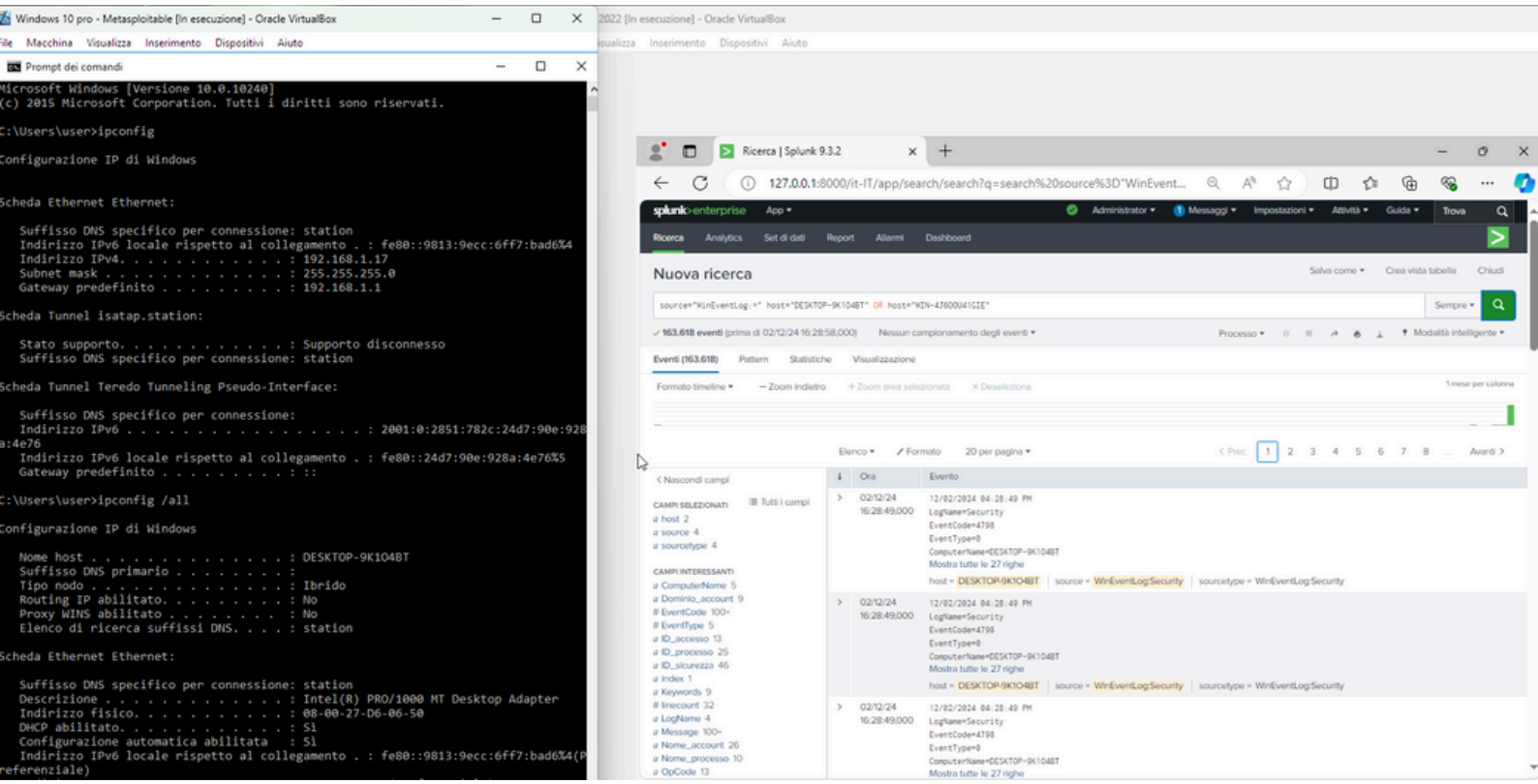
Andiamo avanti fino a verifica e nella schermata impostazioni input ho sostituito l’host predefinito (il server) con entrambi per avere una cosa un pò più completa con questo comando source="WinEventLog:*" host="DESKTOP-9K104BT" OR host="WIN-4J600U41GIE" (indentato correttamente come si vede dall’immagine, senza virgolette) (Potremo fare le ricerche direttamente tramite query, questo menù serve per “autoimpostare” le ricerche, un utente avanzato potrebbe fare ricerche più complesse come source="WinEventLog:*" host="DESKTOP-9K104BT" OR host="WIN-4J600U41GIE" che non è altro la stessa ricerca (security event) ma con HOST multipli. in poche parole il menu non fa altro che eseguire una ricerca tramite quello che si potrebbe considerare “gui”.)



Avviamo la ricerca ed una volta finita avremo i log raggruppati degli host interessati (e il tipo di log, “security only for now”) . Completando l’esercizio.



e Finita la ricerca, avremo i log degli host interessati (e il tipo di log, “security”) . Completando l’esercizio.



Osserviamo che l'hostname corrisponde a Windows 10 Pro, (in uso da noi e impostato con il forwarder) confermando la connessione tra le due macchine e l'associazione con i log del client

Extra:

Modifica delle query: **Se si è esperti, è possibile personalizzare direttamente la ricerca scrivendo query manuali, ad esempio aggiungendo filtri per eventi specifici o host. Per chi non ha familiarità con la sintassi, Splunk offre un'interfaccia intuitiva che consente di selezionare i campi di interesse e generare automaticamente le query. Questa funzionalità si utilizza, ad esempio, cliccando su "CAMPI SELEZIONATI" o altre opzioni per approfondire (o iniziare) una ricerca.**

Questo programma è un capolavoro di ingegneria, capace di rilevare le intrusioni in modo automatico grazie a sofisticate analisi dei dati