

SPLUNK

Splunk è una piattaforma software che si concentra sull'analisi dei dati in tempo reale, con un'attenzione particolare alla gestione e monitoraggio dei log e dei dati di macchina. È utilizzato principalmente da professionisti IT, esperti di sicurezza e team operativi per raccogliere, indicizzare e analizzare enormi volumi di dati non strutturati provenienti da una varietà di fonti. Splunk è ampiamente usato in ambiti come il monitoraggio delle prestazioni, la gestione degli incidenti di sicurezza e l'analisi dei dati aziendali.

The screenshot displays the Splunk Enterprise web interface in a browser window. The address bar shows the URL: `127.0.0.1:8000/it-IT/app/search/search?q=search%20windows&sid=1733151079.4...`. The interface features a dark navigation bar with the 'splunk>enterprise' logo and various menu items like 'App', 'Administra...', 'Messaggi', 'Impostazioni', 'Attività', 'Guida', and 'Trova'. Below the navigation bar, the 'Ricerca' (Search) tab is active, showing a search bar with the query 'windows'. The search results indicate '6.908 eventi' (6,908 events) for the time range '01/12/24 15:00:00,000 - 02/12/24 15:51:19,000'. The interface includes a timeline visualization and a table of events. The table has columns for 'Ora' (Time) and 'Evento' (Event). The first event is dated '02/12/24' at '15:50:44,000' and contains log data for 'LogName=Application' and 'Message=Windows Installer: installazione del prodotto completata. Nome prodotto: UniversalForwarder. Versione prodotto: 9.3.2.0. Lingua prodotto: 1033. Prodotto: Splunk, Inc. Installazione riuscita o stato di errore: 0'.

Ora	Evento
02/12/24 15:50:44,000	12/02/2024 03:50:44 PM LogName=Application ... 10 lines omitted ... TaskCategory=None OpCode=Informazioni Message=Windows Installer: installazione del prodotto completata. Nome prodotto: UniversalForwarder. Versione prodotto: 9.3.2.0. Lingua prodotto: 1033. Prodotto: Splunk, Inc. Installazione riuscita o stato di errore: 0

L'obiettivo dell'esercizio di oggi era configurare SPLUNK in modalità monitoring.