

Esercitazione S10-L1

- Modalità “monitora” sulla macchina locale per analisi log

The screenshot shows the Splunk Enterprise Search & Reporting interface. The search bar contains the query: `source="WinEventLog:*" host="DESKTOP-8CAJRT0"`. The results show 3,264 events. The left sidebar displays the search results in a table format, with columns for time, host, source, and sourcetype. The main panel shows a list of events with details for each, including the event code, type, and message.

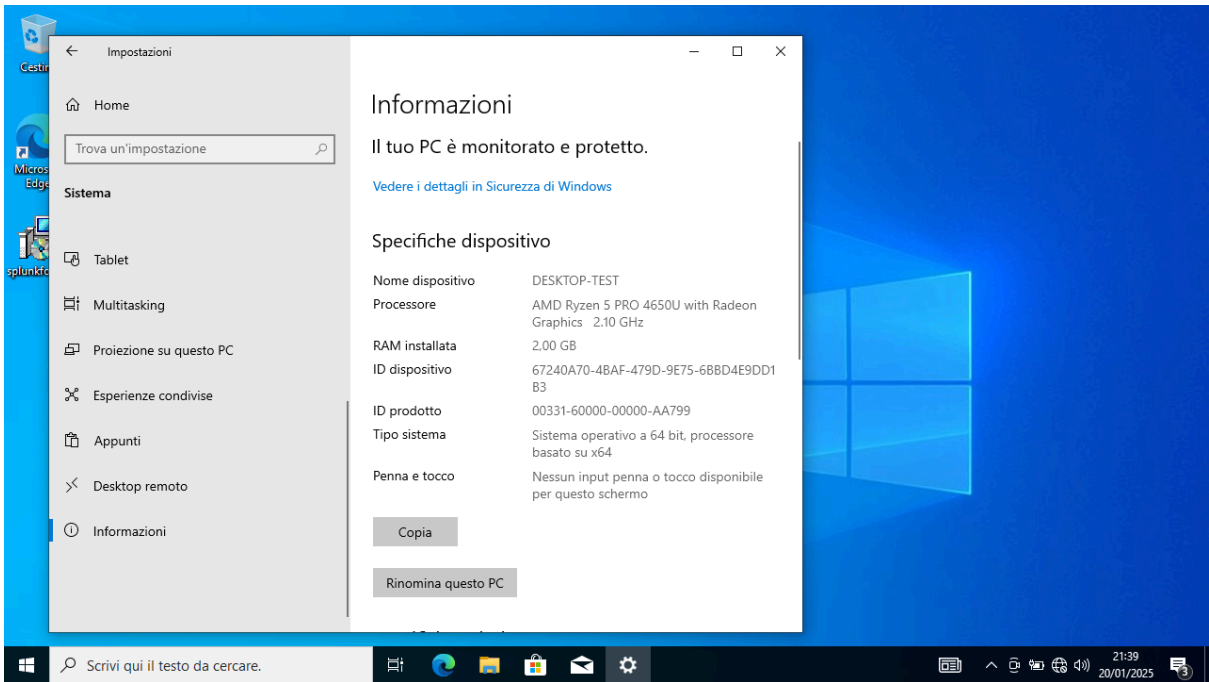
The screenshot shows the details of a specific event. The event details include the time, host, source, and sourcetype. The event message is: "Un account è stato disconnesso. Soggetto: ID sicurezza: S-1-5-21-623064250-797055843-3829581938-1001 Nome account: User Dominio account: DESKTOP-8CAJRT0 ID accesso: 0x83DA7A Tipo di accesso: 2 Questo evento viene generato quando una sessione di accesso viene eliminata. Può essere correlato positivamente con un evento di accesso mediante il valore ID accesso. Gli ID di accesso sono univoci solo tra riavvii nello stesso computer." The event details are displayed in a table format, with columns for the field name and the value.

- Splunk Forwarder e raccolta informazioni da macchina esterna

Impostazione porta su server Splunk

The screenshot shows the Splunk Enterprise Settings interface. The "Ricevi dati" (Receive data) section is active, showing the configuration for a new data port. The port number is 9997, and the state is "Abilitato" (Enabled). The "Azioni" (Actions) column shows a link to "Elimina" (Delete).

Identificazione nome macchina host “DESKTOP_TEST”



Raccolta informazioni su server Splunk

