

**PROCEDURA DI GARA  
FINALIZZATA ALL’AFFIDAMENTO DELLA FORNITURA ANNUALE  
DELLE LICENZE PER LA PIATTAFORMA SIEM SPLUNK  
PER LA RACCOLTA E L’ANALISI DEGLI EVENTS LOGS**

**CAPITOLATO TECNICO**

**CIG 8380455A3C**

## Art. 1 DESCRIZIONE DELLA FORNITURA

L'oggetto dell'appalto prevede l'acquisizione della licenza d'uso del software per il log monitoring denominato **SPLUNK** che fornisce una piattaforma completa per l'Operational Intelligence in grado di trasformare i dati macchina in informazioni significative attraverso tabelle, schemi, grafici e statistiche consultabili tramite interfaccia web.

Il software dovrà essere anche dotato della funzionalità "*Security Information and Event Management*" tramite l'app di **Enterprise Security - SIEM**.

La fornitura dovrà comprendere anche l'attività di installazione e setup iniziale del software **SPLUNK** da svolgere presso la sede di Torino su un server dedicato messo a disposizione dall'Autorità di regolazione dei trasporti (di seguito: ART), nonché la configurazione dell'app **Enterprise Security – SIEM** cosicché la piattaforma sia in grado di acquisire e analizzare i logs prodotti dagli apparati da sottoporre a monitoraggio.

## Art. 2 DETTAGLI FORNITURA

A seguito del dimensionamento effettuato dall'Ufficio ICT dell'ART è stato stimato che i sistemi in uso in ART generano circa 10 Gb di logs al giorno.

Sulla base di tale dato, si riporta di seguito il dettaglio della la fornitura da acquisire:

- **Licenza Splunk Enterprise** - Term License with Standard Success Plan, con gestione dati fino a 10 GB/day
- **Licenza Splunk Enterprise Security** - Term License with Standard Success Plan, , con gestione dati fino a 10 GB/day
- **Installazione e configurazione di Splunk Enterprise e dell'app Security**, da assicurare tramite:
  - 10 gg. uomo **Splunk Specialist**
  - 4 gg. uomo **Splunk Architect**

## Art. 3 CONDIZIONI

Il fornitore dovrà essere un reseller SPLUNK almeno di tipo **Premier** e le attività di installazione e configurazione dovranno essere erogate da personale dotato di certificazione SPLUNK.

Alla data di consegna dovrà essere assicurata la fornitura dell'ultima versione disponibile del software, nell'edizione rilasciata ufficialmente dal produttore, comprensiva dei relativi manuali e/o documentazione di supporto all'uso.

## Art. 4 DURATA

La durata delle licenze dovrà essere di dodici mesi a partire dalla data di collaudo.