DIRECTOR OF STRATEGY
SECURITY

Oggetto : Specifica Tecnica per rinnovo Licenza Splunk

Descrizione del contesto

All'interno della struttura Security - Cyber Security del gruppo ENAV opera il *Security Operation Center* (di seguito *SOC*) che è la struttura operativa aziendale che ha in carico:

1. il monitoraggio real-time degli eventi di sicurezza su tutti i sistemi informativi del gruppo con l'obiettivo di intercettare e gestire ogni anomalia che abbia avuto, o possa avere, impatto su disponibilità, riservatezza od integrità di sistemi ed informazioni aziendali;
2. la gestione di eventi e incidenti di sicurezza garantendo i coordinamenti con il personale e con le strutture di gruppo che erogano servizi informativi;
3. la raccolta e la gestione di informazioni inerenti vulnerabilità software o indicatori di compromissione e lo scambio di informazioni con enti istituzionali o altri enti omologhi (CERT) di infrastrutture nazionali od internazionali;
4. il monitoraggio della sicurezza dei sistemi e delle reti individuando vulnerabilità e contromisure di contenimento e ripristino, proponendo soluzioni ai fini del mantenimento e miglioramento dei livelli di security stabiliti.

Strumento principale per l'esecuzione di tali attività all'interno di un SOC è una piattaforma software denominata *Security Information and Event Management* (SIEM); la piattaforma utilizzata in ENAV come SIEM è basata su software Splunk ed è in esercizio all'interno del SOC di ENAV dal 2017. L'utilizzo di tale piattaforma software è imprescindibile per l'esecuzione di tutte le attività del SOC secondo quanto previsto dai processi aziendali in essere.

La licenza attuale di ENAV del software *Splunk Enterprise* è dimensionata per 300 GB/giorno ed è installata ed utilizzata nelle piattaforme del SOC ENAV presenti nel sito ENAV di Ciampino in due CED distinti tra loro in alta affidabilità (uno in ACC e l'altro a Piastra e Stecca).

Descrizione della fornitura

Per quanto sopra indicato, si necessita di acquisire:

- una licenza "*Splunk Enterprise*" per un totale di 300 GB/giorno e con una validità di 24 mesi.

ENAV S.p.A.
Via Salaria, 716 – 00138 Roma
Tel. +39 06 81661 – Cap. Soc. € 541.744.385,00 I.V.
P.IVA 02152021008 – Reg. Imp. Roma
C.F. e CCIAA 97016000586 – REA 965162
www.enav.it