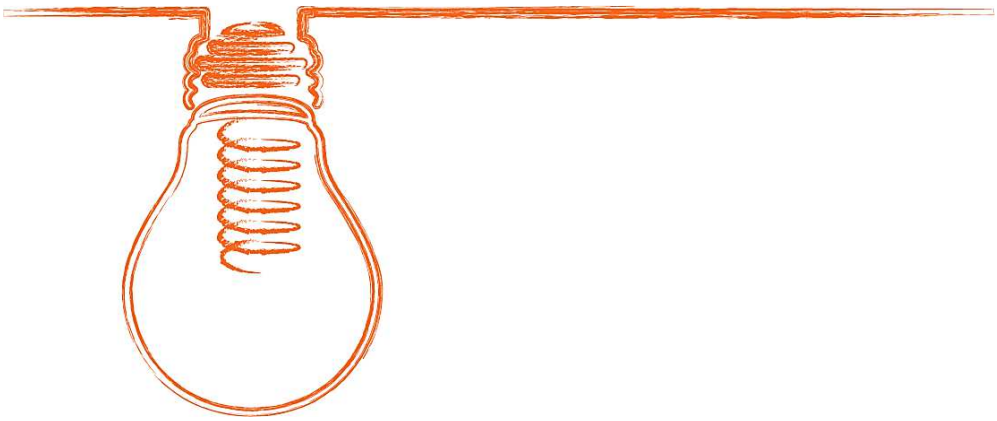

Prot n. 2397622 del 16/03/2023

Progetto tecnico ai sensi art. 23 comma 15 D. Lgs. n. 50/2016

Rinnovo delle licenze d'uso "Elastic – Platinum Subscription"

Sommario

1 Premessa

Il prossimo 26 giugno 2023, scadrà il contratto in essere con il Fornitore Kiratech S.p.A. per le licenze d'uso "Elastic Platinum Subscription", attualmente impiegate all'interno del sistema informativo di Agenzia delle entrate– Riscossione (di seguito anche AdeR), per l'utilizzo di una piattaforma software finalizzata alla gestione della cybersecurity.

La piattaforma in uso presso AdeR è LogOS per la Cyber Security. LogOS è una verticalizzazione basata sulle soluzioni Elasticsearch e Wazuh in grado di operare una corretta gestione della cybersecurity.

La legge 29 dicembre 2022, n. 197, all'articolo 1, comma 258, prevede lo scorporo del ramo d'azienda di AdeR dedicato all'IT in favore di Sogei, entro il 31 dicembre 2023.

Nelle more del suddetto scorporo e per il tempo necessario ad un'eventuale integrazione con i servizi di sicurezza già implementati in Sogei, risulta necessario avere in dotazione le licenze d'uso atte a garantire il funzionamento della già menzionata piattaforma per tutto il tempo necessario a consentire la continuità del servizio.

2 Descrizione del fabbisogno

In ambito cybersecurity sono stati identificati da AdeR un insieme di azioni che definiscono puntualmente il fabbisogno che poi è stato declinato in una serie di obiettivi intermedi raggiungibile mediante la piattaforma LogOS in uso. Di seguito i tre principali.

- **Log degli Amministratori di Sistema**: Ai fini della normativa vigente risulta necessario implementare una infrastruttura atta alla conservazione dei log degli accessi degli amministratori di sistema mediante i seguenti step implementativi:
  - mapping delle fonti contenenti le informazioni relative agli accessi da sottoporre a indicizzazione e valutazione volumi ai fini del dimensionamento della infrastruttura.
  - installazione degli agent deputati alla raccolta delle informazioni tramite sistema di distribuzione automatizzata del software.
  - definizione dei sistemi parsing e trasformazione dei log acquisiti.
  - implementazione dei sistemi di reporting e delle dashboard di fruizione statistiche per tale ambito.
- **Attivazione di funzionalità SIEM**: Risulta necessario un sistema dedicato alla cybersecurity e la distribuzione di agent per la raccolta di informazioni che consenta l'utilizzo di una serie di tool che possono implementare le seguenti funzionalità:
  - inventario di sistema per il censimento e monitoraggio di HW, OS, Interfacce di rete, pacchetti installati, porte e processi.
  - attivazione di funzionalità di verifica dei file monitorati sulle macchine tramite hash per l'identificazione di virus.
  - configurazione di Job di machine learning e sistemi di alerting per la verifica dinamica di anomalie sulle metriche acquisite.
  - implementazione dei sistemi di reporting e delle dashboard di fruizione statistici per tale ambito.
- **Raccolta eventi mirati al NIDS**: Sarà operata la raccolta ed il monitoraggio dei log provenienti dagli apparati di rete per presidiare in maniera efficace il traffico proveniente dagli apparati di rete della infrastruttura informatica, in dettaglio:
  - censimento dei dispositivi di rete e servizi correlati (proxy, radius, etc.)
  - attivazione Syslog su apparati da sottoporre a monitoraggio.
  - definizione dei sistemi parsing e trasformazione dei log acquisiti.

- configurazione di Job di machine learning e sistemi di alerting per la verifica dinamica di anomalie sui dati acquisiti.
- dashboard e sistemi di reporting per la visualizzazione grafica di quanto acquisito del sistema.

La piattaforma LogOS fornisce meccanismi che garantiscono:

- un Host-based intrusion detection system (HIDS), offrendo template di comparazione di pattern di file, Log e traffico di rete, al fine di individuare le attività malevoli nativi o realizzati ad hoc per le proprie esigenze;
- la conservazione dei LOG in maniera inalterabile, in modo da soddisfare i requisiti di legge di conservazione del dato;
- la fornitura delle tradizionali funzionalità di raccolta e restituzione del dato in forma aggregata e correlata;
- un approccio proattivo alla rilevazione dell'accadimento delle anomalie grazie al componente di machine learning;
- la realizzazione di dashboard di consultazione e reporting dei dati raccolti dalle varie fonti.

Le informazioni gestite da LogOS vengono gestite in maniera duplice per garantire:

- la conservazione in maniera inalterabile;
- l'immediata fruibilità a scopi consultativi e proattivi.

Per garantire entrambe le funzionalità, LogOS raccoglie le informazioni dalle varie fonti dati (tramite agent o tramite Syslog) e la disponibilità dei log provenienti dalle varie fonti, sottoposti ad indicizzazione e la presenza di agent consentono, di:

- raccogliere, aggregare, indicizzare e analizzare i dati di sicurezza,
- scansionare i sistemi monitorati alla ricerca di malware, rootkit e anomalie sospette.
- leggere i log del sistema operativo e delle applicazioni monitorate per identificare configurazioni errate, attività dannose tentate e/o riuscite, violazioni delle policy e altri aspetti legati alla sicurezza.
- monitorare i file system, identificando i cambiamenti nel contenuto, nei permessi, la proprietà e gli attributi dei file.
- valutare in maniera automatica eventuali vulnerabilità del sistema grazie a database remoti continuamente aggiornati.
- monitorare le impostazioni di configurazione del sistema e delle applicazioni per garantire che siano conformi alle politiche di sicurezza e agli standard.
- eseguire in remoti comandi o query di sistema, identificando indicatori di compromissione (IOC) e aiutando ad eseguire altre attività di live forensics o di risposta agli incidenti.
- fornire controlli di sicurezza necessari per conformarsi agli standard e alle normative di settore in fatto di compliance.

Tanto ciò premesso, in considerazione della norma contenuta nell'ultima Legge di Bilancio che ha previsto il trasferimento delle attività informatiche a Sogei entro il 31.12.2023 attraverso la cessione del ramo d'azienda, il fabbisogno è costituito dal rinnovo, per 12 mesi, delle licenze d'uso "Elastic – Platinum Subscription", i cui parametri dimensionali sono riportati nella seguente tabella:

Tipo	N° nodi
Platinum	10

3 Considerazioni sulla procedura acquisitiva da espletare

Per soddisfare il fabbisogno di cui sopra, a fronte della mancanza di Convenzioni Consip attive, si è proceduto alla verifica della presenza delle Elastic – Platinum sul MePA.

A sensi dell'art. 6.2 del "Regolamento per le acquisizioni di forniture e servizi di importo inferiore alla soglia comunitaria", fino al 30 giugno 2023, ai sensi dell'art. 1, comma 2, lett. a) della L. 11 settembre 2020 n. 120 e s.m.i., di conversione del D.L. 16 luglio 2020, n. 76 e salva un'eventuale proroga del medesimo termine, AdeR procede all'acquisizione di servizi e forniture fino ad Euro 139.000,00 ovvero al diverso importo come eventualmente modificato da provvedimenti normativi successivi, tramite affidamento diretto, previa consultazione informale di almeno due operatori economici.

Secondo quanto previsto all'art. 8 del "Regolamento per le acquisizioni di forniture e servizi di importo inferiore alla soglia comunitaria" gli operatori da consultare vengono individuati, nel rispetto dei principi di trasparenza, rotazione e parità di trattamento, fra i partner del produttore indicati nell'Allegato "Partner del Fornitore" presenti nei bandi MePA:

- BENI - Licenze software-MePA Beni – CPV 48218000 – 9 "Pacchetti software per la gestione di licenze";
- SERVIZI - Licenze software-MePA Servizi CPV 72261000 – 2 "Servizi assistenza software";

e che al momento offrono il prodotto in parola al prezzo più basso.

Si propone, quindi, di richiedere agli operatori sopra elencati un preventivo per il tramite di RDO MEPA evoluta in ragione del fatto che i CPV afferiscono a bandi differenti. Il preventivo dovrà presentare i canoni unitari per singolo nodo e il prezzo massimo complessivo.

All'esito della stessa si procederà ad un affidamento diretto ai sensi dell'art.1, c.2 lett. a) del DL 76/2020 convertito dalla legge 120/2020.

4 Determinazione della base della Base di gara – Durata dell'Appalto

L'importo complessivo dell'appalto, per una durata dell'appalto pari a 12 mesi dalla data di stipula del Contratto, risulta essere pari a complessivi € 69.500,00 al netto di IVA, determinato sulla base della quotazione di listino fornita dal produttore, tenendo conto di:

- un numero utile di asset attualmente da monitorare pari a 35.200;
- un ipotetico tasso di sconto applicato dal produttore a tutti i rivenditori in maniera uniforme stimato nel 10%;
- un margine di guadagno dei rivenditori stimato nel 7%, in dettaglio:

Tipo licenza d'uso	Numero nodi	Canone annuo per singolo nodo	Totale
Platinum	10	6.950,00 €	69.500,00 €

Il valore dell'appalto stimato è pari a € 69.500,00 (di cui € 0,00 per i costi per l'eliminazione delle interferenze) a cui si aggiunge:

- il contributo ANAC pari a € 30,00 (In caso l'avvio della procedura superasse il 1° aprile 2023, il contributo ANAC sarà pari a 35 euro);
- l'IVA indetraibile per l'Ente pari ad € 305,80 € (2% del valore dell'IVA).

L'impegno di spesa complessivo trova copertura nel Budget Economico 2023-2025 deliberato dal Comitato di gestione di AdeR del 27 ottobre 2022.

Il codice di iniziativa interno all'Ente è 2023.7.009.I e il CUI è F13756881002202200006.

4.1 Clausola sociale

In relazione a quanto definito nelle Linee Guida n.13 ANAC, approvate dal Consiglio dell'Autorità con delibera n. 114 del 13.2.2019, recanti "La disciplina delle clausole sociali", per la indicenda procedura de quo non trova applicazione la disciplina di cui all'art. 50 del D. Lgs. n. 50/2016 in quanto trattasi di servizi di natura intellettuale.

5 Indicazione per la stesura dei documenti inerenti la sicurezza

Inoltre, in considerazione della tipologia dell'affidamento, riferito a servizi di natura intellettuale, ai sensi dell'art. 26 c. 3 del D. Lgs. 81/2008 e s.m.i. e della determinazione dell'ANAC nr. 3 del 05/03/2008, si esclude la predisposizione del DUVRI; i costi per oneri della sicurezza per rischi interferenziali sono pari a € 0,00.

6 Suddivisione in lotti

Le licenze "Elastic – Platinum Subscription" che rappresenta il fabbisogno di AdeR sono indispensabili per il funzionamento di una piattaforma software che rende disponibili informazioni esaustive e dettagliate in maniera centralizzata. Risulta pertanto non possibile la suddivisione in lotti dell'affidamento.

7 Garanzie

In considerazione che la procedura è svolta sul MePA e che verrà affidata ai sensi dell'art. 1, c. 2 lett. a) del DL 76/2020 convertito dalla legge 120/2020, in base all'art. 9, c. 3 e 4 del Regolamento per le acquisizioni di forniture e servizi di AdeR, non si richiederà la cauzione provvisoria, mentre occorrerà prevedere quella definitiva ai sensi dell'art. 103 del D. Lgs. n. 50/2016 per l'esecuzione del contratto, fissata nella misura del 10% del valore dell'importo aggiudicato.

Ai fini della stipula del Contratto, non sono richieste al fornitore altre tipologie di garanzie perché non necessarie e la loro produzione genererebbe un aggravio di costo non giustificato.

8 Modalità di fatturazione

La fatturazione dovrà avvenire previo rilascio della regolare esecuzione e sarà annuale anticipata.

Allegati

- Partner del Fornitore

Il Responsabile del Procedimento

Francesco Ferri

(firmato digitalmente)