Consultazione preliminare di mercato, ai sensi dell'art. 66 comma 1 del D. Lgs 50/2016, per il rinnovo della componente Elasticsearch della piattaforma di gestione della cyber security

Agenzia delle entrate-Riscossione
Via G. Grezar 14
00142 Roma
pianif.acquisti.monit.contratti@pec.agenziariscossione.gov.it

PREMESSA E MODALITA' DI INVIO DEI CONTRIBUTI

L'Ente Pubblico Economico "Agenzia delle entrate-Riscossione" (di seguito anche solo Agenzia) intende procedere al rinnovo delle licenze "Elastic – Platinum Subscription" comprensive del servizio di manutenzione software come di seguito meglio dettagliato. Preliminarmente all'avvio della relativa procedura di affidamento, l'Agenzia ritiene opportuno procedere ad una consultazione del mercato ai sensi dell'art. 66 comma 1 del D. Lgs 50/2016, al fine di verificare se tali licenze abbiano un mercato di riferimento, appurando altresì l'esistenza sul mercato di sistemi alternativi a quello attualmente in uso aventi caratteristiche e funzionalità analoghe (con la preferenza per sistemi aperti e licenze open source), valutandone l'eventuale convenienza rispetto al sistema in uso.

Pertanto, in considerazione di quanto sopra espresso, si richiede agli operatori economici interessati di fornire il proprio contributo - previa presa visione dell'informativa sotto riportata ed autorizzazione al trattamento dei dati personali – compilando **– anche solo per le parti di interesse -** il questionario di seguito allegato, che dovrà essere sottoscritto da persona munita di idonei poteri di rappresentanza.

Il documento dovrà essere inviato entro **30 (trenta) giorni** dalla data di pubblicazione, sotto riportata, al seguente indirizzo PEC:

pianif.acquisti.monit.contratti@pec.agenziariscossione.gov.it.

Tutte le informazioni fornite con il presente documento saranno utilizzate ai soli fini dello sviluppo dell'iniziativa in oggetto.

Dall'utilizzo di tale procedura di consultazione non derivano vincoli per l'Agenzia, né alcuna aspettativa, di fatto o di diritto, da parte degli operatori di mercato relativa allo svolgimento del procedimento selettivo.

L'Agenzia si riserva la facoltà di interrompere, modificare, prorogare, sospendere la procedura, consentendo, a richiesta dei soggetti intervenuti, la restituzione della documentazione eventualmente depositata, senza che ciò possa costituire, in alcun modo, diritto o pretesa a qualsivoglia risarcimento o indennizzo.

L'Agenzia, salvo quanto di seguito previsto in materia di trattamento dei dati personali, si impegna a non divulgare a terzi le informazioni raccolte con il presente documento.

I contributi forniti non possono contenere offerte o proposte contrattuali e sono trasmessi all'Agenzia secondo le modalità previste nell'avviso.

I soggetti che partecipano alla consultazione indicano se i contributi forniti contengono informazioni, dati o documenti protetti da diritti di privativa o comunque rivelatori di segreti aziendali, commerciali o industriali, nonché ogni altra informazione utile a ricostruire la posizione del soggetto nel mercato e la competenza del soggetto nel campo di attività di cui alla consultazione.

La partecipazione alla consultazione preliminare non costituisce condizione di accesso alla successiva procedura selettiva. Dalla partecipazione al procedimento di consultazione non possono derivare, per il soggetto partecipante, vantaggi, di qualunque natura, nello svolgimento della successiva procedura selettiva.

Roma, **19/12/2019**

Dati Azienda

Azienda
Indirizzo
Nome e Cognome del referente
Ruolo in azienda
Telefono
Fax
Indirizzo e-mail
Data di compilazione

INFORMAZIONI PER L'INTERESSATO [art. 13 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - Regolamento generale sulla protezione dei dati]Agenzia delle entrate - Riscossione, con sede legale in via Giuseppe Grezar, 14 – 00142 Roma, codice fiscale e partita IVA: 13756881002 è Titolare del trattamento dei dati personali da Lei conferiti.

Agenzia provvede alla raccolta ed al trattamento dei Suoi dati personali, forniti mediante la compilazione del presente documento di consultazione di mercato, con il suo consenso, che può essere revocato in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca.

La raccolta ed il trattamento dei predetti dati personali sono effettuati al solo fine di consentire ad Agenzia di condurre le attività connesse alla consultazione preliminare di mercato avvalendosi della facoltà prevista dall'art. 66 comma 1 del D. Lgs. n. 50/2016.

Il conferimento dei dati è facoltativo, ma la mancata comunicazione degli stessi comporta l'impossibilità di partecipare alla consultazione.

Il trattamento dei dati avviene anche mediante l'utilizzo di strumenti elettronici, per il tempo e con logiche strettamente correlati alle predette finalità e comunque in modo da garantirne la sicurezza e

la riservatezza, nel rispetto delle previsioni normative, anche europee, in materia di protezione dei dati personali.

La conservazione, da parte di Agenzia, dei dati personali conferiti avverrà per il tempo necessario alla gestione della consultazione stessa.

I dati personali conferiti, se necessario per le finalità di cui sopra, potranno essere comunicati:

ai soggetti cui la comunicazione dei dati debba essere effettuata in adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, ovvero per adempiere ad un ordine dell'Autorità Giudiziaria;

ai soggetti designati dal Titolare, in qualità di Responsabili ovvero alle persone autorizzate al trattamento dei dati personali che operano sotto l'autorità diretta del Titolare o del Responsabile;

ad altri eventuali soggetti terzi, nei casi espressamente previsti dalla legge, ovvero ancora se la comunicazione si renderà necessaria per la tutela di Agenzia in sede giudiziaria, nel rispetto delle vigenti disposizioni in materia di protezione dei dati personali.

I dati personali conferiti non saranno oggetto di diffusione se non per ottemperare ad obblighi espressamente previsti dalla legge.

Lei ha il diritto, in qualunque momento, di ottenere la conferma dell'esistenza o meno dei medesimi dati e/o verificarne l'utilizzo. Ha, inoltre, il diritto di chiedere, nelle forme previste dall'ordinamento, la rettifica dei dati personali inesatti e l'integrazione di quelli incompleti; nei casi indicati dal Regolamento UE n. 679/2016, fatta salva la speciale disciplina prevista per alcuni trattamenti. Può altresì chiedere - decorsi i previsti termini di conservazione - la cancellazione dei dati o la limitazione del trattamento; l'opposizione al trattamento, per motivi connessi alla Sua situazione particolare, è consentita salvo che sussistano motivi legittimi per la prosecuzione del trattamento.

Esclusivamente per esercitare i diritti sopra indicati potrà utilizzare, secondo le modalità indicate al seguente link: https://www.agenziaentrateriscossione.gov.it/export/it/Gruppo/Modalita-di-presentazione-istanze.pdf, i dati di contatto del Titolare del trattamento:

Agenzia delle entrate-Riscossione, Struttura a supporto del Responsabile della protezione dei dati, Via Giuseppe Grezar n. 14 – 00142 Roma oppure l'indirizzo di posta elettronica certificata: protezione.dati@pec.agenziariscossione.gov.it.

Il dato di contatto del Responsabile della protezione dei dati è: dpo@pec.agenziariscossione.gov.it.

Qualora ritenga che il trattamento sia avvenuto in modo non conforme al Regolamento UE n. 679/2016, Lei potrà inoltre rivolgersi all'Autorità di controllo, ai sensi dell'art. 77 del medesimo Regolamento.

Ulteriori informazioni in ordine ai Suoi diritti sulla protezione dei dati personali sono reperibili sul sito web del Garante per la protezione dei dati personali all'indirizzo www.garanteprivacy.it.

Si dichiara di aver preso visione dell'informativa sul trattamento dei dati personali conferiti mediante la compilazione del presente documento e si autorizza il trattamento dei medesimi dati.

Obiettivo della Consultazione

L'Agenzia, ai sensi dell'art. 66 comma 1 del D. Lgs 50/2016 e in conformità alle Linee Guida dell'ANAC n. 8 del 10 ottobre 2017 "Ricorso a procedure negoziate senza previa pubblicazione di un bando nel caso di forniture e servizi ritenuti infungibili", nonché delle Linee Guida dell'ANAC n. 14 del 6 marzo 2019 "Indicazioni sulle consultazioni preliminari di mercato", tramite la presente iniziativa intende:

- garantire la massima pubblicità all'iniziativa stessa al fine di assicurare la più ampia diffusione delle informazioni e ottenere la più efficace partecipazione da parte dei soggetti interessati;
- conoscere se le licenze "Elastic – Platinum Subscription" (per le funzionalità soggette a licenze) ed il relativo servizio di manutenzione, attualmente in uso, abbiano un mercato di riferimento e le eventuali soluzioni tecniche disponibili, nonché le condizioni di prezzo mediamente praticate;
- rilevare l'effettiva esistenza di più operatori economici potenzialmente interessati alla prestazione dei servizi di cui al precedente punto;
- verificare l'esistenza sul mercato di eventuali soluzioni alternative a quella attualmente in uso, aventi caratteristiche e funzionalità analoghe, con la preferenza per sistemi aperti e licenze open, nonché le relative condizioni di prezzo mediamente praticate, al fine di valutarne l'eventuale convenienza rispetto al sistema in uso;
- descrivere al meglio le caratteristiche qualitative e tecniche dei prodotti e servizi oggetto di analisi;
- acquisire ogni ulteriore elemento utile ad effettuare una valutazione comparativa di tipo tecnico ed economico delle diverse soluzioni disponibili sul mercato, ai sensi dell'art. 68 del D.lgs. n. 82/2015 (Codice dell'Amministrazione Digitale) e delle Linee Guida su acquisizione e riuso di software per le pubbliche amministrazioni, adottate da AGID con Determinazione n. 115 del 9 maggio 2019;
- valutare, ove ne ricorrano i presupposti, di procedere all'affidamento, ai sensi dell'art. 63, comma 2, lett. b), per le eccezioni di cui ai punti 2 e 3, del D. Lgs. 50/2016, tramite procedura negoziata.

1. Descrizione del fabbisogno

Da alcuni anni è emersa l'esigenza di adottare una piattaforma software finalizzata alla gestione della cybersecurity ed anche l'Agenzia se n'è dotata per il proprio sistema informativo, utilizzando soluzioni *open source*.

In ambito della cybersecurity infatti sono stati identificati dall'Agenzia un insieme di azioni che definiscono puntualmente l'esigenza e che sono poi stati declinati in una serie di obiettivi intermedi necessari. Nello specifico di seguito i tre principali che sono stati implementati dalla piattaforma in uso:

Log degli Amministratori di Sistema: Ai fini della normativa è necessario mettere in atto una infrastruttura atta alla conservazione in compliance dei log degli accessi degli amministratori di sistema. Per tale tipologia di attività prevediamo 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: L'adozione di un sistema dedicato alla cybersecurity e la distribuzione di agent per la raccolta di informazioni consente 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: Particolare attenzione sarà data alla raccolta e monitoraggio dei log provenienti dagli apparati di rete per presidiare in maniera efficace il traffico proveniente dagli apparati di rete della infrastruttura informatica, tale task prevede:

- 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 soluzione deve essere dimensionata per 600 end-point (sistemi che producono log) per un volume di dati grezzi da gestire pari a 400 GB al giorno.

Si stima un importo complessivo per l'acquisizione delle licenze e relativo servizio di manutenzione, per la durata di 36 mesi, pari ad Euro 214.000 (duecentoquattordicimila/00) IVA esclusa.

All'esito della consultazione l'Agenzia effettuerà la valutazione comparativa di cui alle superiori premesse, analizzando la fattibilità e la convenienza di soluzioni tecniche presenti sul mercato che abbiano caratteristiche e funzionalità analoghe a quella in uso.

2. Descrizione delle specifiche del prodotto in uso

La piattaforma adottata dall'Agenzia è LogOS per la Cyber Security. LogOS è una verticalizzazione basata sulle soluzioni Elasticsearch e Wazuh.

Grazie all'utilizzo sinergico di tali componenti, LogOs fornisce meccanismi per garantire il fabbisogno attraverso:

- 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.
- Conservare i LOG in maniera inalterabile, in modo da soddisfare i requisiti di legge di conservazione del dato.
- Fornire le tradizionali funzionalità di raccolta e restituzione del dato in forma aggregata e correlata.
- Fornire un approccio proattivo alla rilevazione dell'accadimento delle anomalie grazie al componente di machine learning.
- Realizzare dashboard di consultazione e reporting dei dati raccolti dalle varie fonti.

Flusso delle informazioni e componenti: 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), le firme e le invia al manager in maniera sicura.

Qui vengono classificate, ne vengono valutati e filtrati gli eventi e conservate in compliance.

Quanto acquisito e conservato viene inviato ad Elasticsearch, ove costituisce una base dati per la consultazione.

Il dato indicizzato in Elasticsearch potrà infatti essere visualizzato con Kibana (l'interfaccia nativa di visualizzazione dello stack Elasticsearch).

In tale ambito la componente di Machine Learning di Elasticsearch permette inoltre di aggiungere proattività all'attività di monitoraggio.

L'algoritmo di Machine Learning adottato dal sistema rileva automaticamente lo schema di comportamentale standard delle componenti analizzate, sia singolarmente che aggregate tra loro e predice eventuali anomalie che si discostano da quanto rilevato storicamente.

Funzionalità di interesse di Elasticsearch: La disponibilità dei log provenienti dalle fonti sottoposti ad indicizzazione e la presenza di agent consentono inoltre 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 remoto 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: tramite la interfaccia utente web fornisce indicazioni rispetto l'adempimento delle normative GDPR, PCI DSS, GPG13.

Domande

1) L'Azienda ha la capacità tecnica per soddisfare il fabbisogno per l'acquisizione delle licenze "Elastic – Platinum Subscription" e dei relativi servizi di manutenzione indicato nei paragrafi precedenti e in uso presso l'Agenzia? In caso positivo, quali certificazioni possiede e/o quali accordi commerciali ha in essere con la società produttrice per la fornitura delle licenze e l'erogazione del servizio di manutenzione richiesti?

   Risposta:

   _____

   _____

   _____

2) Nel caso l'Azienda fosse interessata alla fornitura delle licenze "Elastic – Platinum Subscription" e dei relativi servizi di manutenzione quali elementi potrebbero essere considerati punti di forza, ovvero costituire un limite alla partecipazione all'iniziativa in oggetto?

   Risposta:

   _____

   _____

   _____

3) Qual è il fatturato specifico medio annuo dell'Azienda relativo a servizi analoghi a quelli di interesse riferito agli ultimi tre esercizi finanziari disponibili?

   Risposta:

   _____

   _____

   _____

4) L'Azienda potrebbe offrire soluzioni tecnologiche alternative in grado di garantire le stesse funzionalità della soluzione di gestione della cyber security in uso presso l'Agenzia? In caso affermativo, si chiede di descrivere le caratteristiche delle soluzioni tecnologiche alternative e gli eventuali ambiti in cui sono impiegate.

Risposta:

_____

_____

_____

5) Nel caso in cui l'Azienda fosse interessata ad offrire soluzioni alternative alla soluzione di gestione della cyber security in uso presso l'Agenzia in grado di garantire le stesse funzionalità, quali sono le variabili tecniche delle soluzioni proposte (es. servizio in cloud, open source, etc.)?

Risposta:

_____

_____

_____

6) Nel caso in cui l'Azienda fosse interessata ad offrire soluzioni alternative alla soluzione di gestione della cyber security in uso presso l'Agenzia in grado di garantire le stesse funzionalità della soluzione già presente, quali sono gli elementi che rappresentano i punti di forza di tali soluzioni, ovvero che costituiscono un limite alla partecipazione all'iniziativa in oggetto (es. costi ridotti, funzionalità/servizi aggiuntivi, etc.)?

Risposta:

_____

_____

_____

7) Nel caso in cui l'Azienda fosse interessata ad offrire soluzioni alternative alla soluzione di gestione della cyber security in uso presso l'Agenzia in

grado di garantire le stesse funzionalità della soluzione attualmente in uso, si chiede di descrivere le componenti chiave dei costi dei prodotti/servizi di tali soluzioni, fornendo un range di costo stimato per un tipico progetto di adozione della soluzione proposta, comprensivo di tutte le attività necessarie alla sostituzione (progetto "chiavi in mano") ed importazione delle informazioni esistenti in formato aperto, per la durata di un triennio.

Risposta:

_____

_____

_____

8) In caso di eventuali soluzioni alternative rispetto a quella in uso, è prevista la disponibilità di un ambiente "demo" con credenziali temporanee, per verificarne le caratteristiche e le funzionalità?

Risposta:

_____

_____

_____

9) L'Azienda può fornire ulteriori informazioni utili o suggerimenti per il miglior soddisfacimento del fabbisogno dell'Agenzia e/o dell'iniziativa d'acquisto necessaria?

Risposta:

_____

_____

_____

Data Firma

(Legale rappresentante o procuratore)