csi piemonte

PROVVEDIMENTO

ACQUISIZIONE DEI SERVIZI DI MANUTENZIONE DELLE LICENZE "RSA - SECURITY ANALYTICS" E SUPPORTO SPECIALISTICO SOFTWARE SU PIATTAFORMA SIEM (SECURITY INCIDENT EVENT MANAGEMENT) NELL'AMBITO DELL'ADESIONE AL "CONTRATTO ESECUTIVO OPO" DI CONSIP S.P.A.

(AC16_03)

PREMESSE

Viste le motivazioni di cui all'Allegato 1 "Motivazioni dell'approvvigionamento", ai sensi della normativa vigente in materia, si rende necessario procedere all'acquisizione dei servizi di "Manutenzione delle licenze "RSA - Security Analytics" e supporto specialistico software su piattaforma SIEM (Security Incident Event Management)" nell'ambito dell'adesione al "Contratto esecutivo OPO" di Consip S.p.A., aggiudicato alla società Olivetti S.p.A. (già Telecom Italia Digital Solutions S.p.A.).

PROSPETTO ECONOMICO COMPLESSIVO DELL'APPALTO

Il prospetto economico complessivo degli oneri necessari per l'acquisizione dei servizi in oggetto, individua le seguenti voci:

A) Importo servizi oggetto d'appalto

A1	Importo per manutenzione delle licenze "RSA - Security Analytics"	Euro 9.900,00
A2	Importo massimo spendibile per supporto specialistico software su piattaforma SIEM (Security Incident Event Management)	Euro 29.400,00
	Totale A	**Euro 39.300,00**

B) Importo per oneri per la sicurezza da interferenza non soggetti a ribasso

B1	Oneri per la sicurezza da interferenza	Euro 0,00
	Totale B	Euro 0,00

	Totale A + B	**Euro 39.300,00**

C) Somme a disposizione dell'Amministrazione

C1	Spese per contributo ANAC (*Autorità Nazionale Anticorruzione Vigilanza Contratti Pubblici*)	Euro 0,00
	IVA ed eventuali altre imposte:	
C2	IVA *(al 22%)* di A)	Euro 8.646,00
C3	IVA *(al 22%)* di B)	Euro 0,00
	Totale C	**Euro 8.646,00**

	Totale A + B + C	**Euro 47.946,00**

Il valore dell'appalto, ai sensi dell'art. 35 del D. Lgs. 50/2016, comprensivo degli oneri per la sicurezza da interferenza non soggetti a ribasso, è pari a Euro 39.300,00 (oltre oneri di legge), salvo eventuali maggiori oneri derivanti da rischi da interferenza come definiti preliminarmente alla stipula del Contratto.

DURATA

Il servizio di manutenzione delle licenze "RSA - Security Analytics" dovrà essere erogato nel periodo dal 1° luglio 2016 al 30 giugno 2017.

Il servizio di supporto specialistico software su piattaforma SIEM (Security Incident Event Management) dovrà essere erogato nel periodo dal 25 luglio 2016 al 31 dicembre 2016.

TIPOLOGIA DI PROCEDURA

Con riferimento a quanto previsto dalla normativa vigente in materia si giustifica l'adesione al "Contratto esecutivo OPO" di Consip S.p.A. il cui fornitore aggiudicatario è la società Olivetti S.p.A. (già Telecom Italia Digital Solutions S.p.A.).

RESPONSABILE UNICO DEL PROCEDIMENTO

Visto il Provvedimento di nomina assunto dal Direttore Generale il 31 marzo 2016 - in esecuzione della decisione assunta dal Consiglio di Amministrazione del 26 gennaio 2016 - con cui veniva individuato Stefano Lista quale Responsabile Unico del Procedimento (RUP) per la Direzione Datacenter per le procedure di gara afferenti alla propria Direzione, si conferma tale nomina per la presente procedura.

Considerato quanto sopra descritto, il Direttore Generale:

- autorizza, ai sensi della normativa vigente in materia, l'acquisizione dei servizi di "Manutenzione delle licenze "RSA - Security Analytics" e supporto specialistico software su piattaforma SIEM (Security Incident Event Management)" per il periodo dal 1° luglio 2016 al 30 giugno 2017, per un importo complessivo pari a Euro 39.300,00 (trentanovemilatrecento/00) (oltre oneri di legge, inclusi oneri per la sicurezza da interferenza pari a Euro zero), nell'ambito dell'adesione al "Contratto esecutivo OPO" di Consip S.p.A., aggiudicato alla società Olivetti S.p.A. (già Telecom Italia Digital Solutions S.p.A.);
- approva il prospetto economico complessivo degli oneri necessari per l'adesione al "Contratto esecutivo OPO" in oggetto.

Si allega:

- Motivazioni dell'Approvvigionamento della Direzione Datacenter e della Direzione Amministrazione e Approvvigionamenti , (Allegato 1)

Torino, 25.07.2016

Il Direttore Generale
FIRMATO IN ORIGINALE
(Ferruccio Ferranti)

Allegato 1

MOTIVAZIONI DELL'APPROVVIGIONAMENTO

MANUTENZIONE LICENZE "RSA – SECURITY ANALYTICS" E SUPPORTO SPECIALISTICO SOFTWARE SU PIATTAFORMA SIEM (SECURITY INCIDENT EVENT MANAGEMENT)

(Riferimento RdA n.ro 2016000423 e 2016000344)

Motivazione della richiesta e contesto in cui si inserisce la fornitura

La Direzione Datacenter, unità organizzativa Processi Gestionali e Trasversali, nell'ambito delle attività di individuazione degli eventi e incidenti di sicurezza sui vari sistemi del CSI-Piemonte e dei Clienti e per conformità al provvedimento del Garante privacy in materia di Amministratori di Sistema, necessita di strumenti di analisi e correlazione dei log prodotti da numerosi sistemi informatici.

Nel 2012, nell'ambito della gara n.06/12 relativa alla "Fornitura di apparati e sistemi per l'evoluzione dell'infrastruttura del Data Center, e dei relativi servizi correlati" - Lotto 2, il CSI-Piemonte ha acquisito una piattaforma SIEM sviluppata con il prodotto RSA.
Nel 2014, volendo rafforzare la soluzione acquisita introducendo elementi di maggiore controllo e a seguito di diverse prove sul campo (POC) volte a valutare i prodotti offerti dal mercato, la direzione Datacenter ha scelto di acquistare, tramite affidamento a Telecom Italia S.p.A., il prodotto RSA – Security Analitics, che ha dato i risultati ricercati in termini di prestazioni, facilità di analisi e correlazione dei log.

Il prodotto ha infatti consentito la valutazione delle possibili categorie di minacce evidenziate dai log di sistema. Ciò ha permesso quindi di stabilire, per ciascuna tipologia di evento, le opportune soglie di allarme dandone evidenza mediante la creazione di report e di dashboard personalizzate.

Visti i risultati positivi ottenuti finora e che hanno portato al censimento delle possibili minacce ai sistemi informatici del Consorzio e degli Enti, è necessario proseguire il monitoraggio e introdurre nuove correlazioni di log per poter individuare e bloccare categorie di minaccia più complesse quali, ad esempio, tentativo di furto di dati, deturpazione (i.e. *defacement*) dei siti istituzionali e compromissione dei sistemi, sviluppando ulteriormente la piattaforma SIEM e mantenendo quindi l'utilizzo del prodotto RSA - Securitiy Analytics.

Oggetto dell'affidamento

Si richiede il servizio di manutenzione del prodotto RSA – Security Analytics, per la durata di un anno a decorrere dal 01/07/2016, con la seguente configurazione:

Q.tà	Codice Fornitore	Descrizione
1	SA-ESALLINONEL-SW	Upg ES to All in One for Logs plus 5 TB S/W
1	SA-ESA-SW-U	RSA SECANLYTICS HYBRID4LOGS S/W ENV UPG
24	SA-AIO-L-SWE1	All-in-One for Logs S/W EnhMnt1Mo
24	SA-ESA-SWE1	Event Stream Analysis S/W EnhMnt1Mo
1	PS-CUS-SA	RSA Prof Svcs Security Analytics (SOW da creare)
1	ED SA ADMIN 110	Security Analytics Administration open enrollment

Si richiede inoltre l'attivazione di un servizio specialistico a consumo per lo svolgimento di attività professionali, mirate a specifici sviluppi, a supporto del prodotto RSA – Security Analytics, per il periodo dal 25/07/2016 al 31/12/2016.

Allegato 1

Le giornate a consumo sono necessarie per lo sviluppo di "use case" (correlazioni di log), relativi alle seguenti categorie di minaccia:

- Data exfiltration, per bloccare tentativi di furti di dati;
- Web defacement, per bloccare tentativi di deturpazione dei siti istituzionali;
- System compromised, per bloccare la compromissione (controllo da remoto, azioni di malware, ecc.) dei sistemi gestiti dal CSI Piemonte.

Attraverso la creazione degli "use case", si intende ridurre la probabilità di accadimento delle minacce indicate e il relativo danno nel caso in cui si verifichi un eventuale incidente, nonché permettere la creazione di report per l'analisi forense di quanto accaduto. Gli automatismi introdotti con lo sviluppo dei nuovi "use case" consentiranno di migliorare la tracciatura e la gestione degli incident di sicurezza.
All'interno di tali scenari dovranno inoltre essere definite e implementate sulla piattaforma le regole di correlazione dei log prodotti dagli strumenti di sicurezza (es. firewall) e di erogazione dei servizi (es. webfarm)

Istruttoria ex Legge 208/2015

La legge 208/15 del 28/12/15 (nota anche come "legge di stabilità"), in particolare ai commi 512-516, impone alle Pubbliche Amministrazioni di provvedere all'approvvigionamento di beni e servizi informatici esclusivamente tramite Consip o altri soggetti aggregatori, il che implica che anche l'approvvigionamento di servizi informatici quali quelli oggetto del presente appalto, debba essere effettuato – ove ne ricorrano le condizioni – con questa modalità.

Dalla ricognizione delle Convenzioni/Strumenti attivi presso Consip, SCR (Società di Committenza Regionale della Regione Piemonte) e Città metropolitana di Torino (soggetto aggregatore accreditato per la Regione Piemonte), alla data del 6 Luglio 2016 emerge la seguente situazione:

- con riferimento a SCR (Centrale di Committenza Regionale) e alla Città Metropolitana di Torino – quale soggetto aggregatore - non è attiva alcuna convenzione/Accordo Quadro per i servizi oggetto del presente appalto;

- con riferimento a Consip si rileva che:
  - è stata aggiudicata il 19/05/2016 la Procedura Ristretta "SPC Cloud" relativa a un nuovo Contratto Quadro Lotto 2 per i "Servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni". A oggi, tuttavia, è in fase di redazione il Piano dei Fabbisogni del CSI-Piemonte, all'interno del quale si sta valutando se far rientrare anche il presente servizio, pertanto non risulta ancora possibile l'utilizzo di tale strumento per l'approvvigionamento in oggetto;
  - Consip ha prorogato fino al 24/05/2017 il Contratto Quadro Ripetizione "OPA" e il relativo Contratto Esecutivo "OPO" per la fornitura dei "Servizi di connettività, interoperabilità di base e sicurezza". Nell'ambito di tale proroga il CSI ha confermato l'adesione al Contratto Quadro e, quindi, prorogato il Contratto Esecutivo "OPO" stipulato con Telecom Italia Digital Solutions S.p.A. (oggi Olivetti S.p.A.), all'interno del quale sono previsti Servizi di security assimilabili all'oggetto dell'appalto;

- con riferimento al canale Consip del "Mercato Elettronico della Pubblica Amministrazione (MEPA)", dalla consultazione dell'iniziativa "ICT 2009", nell'ambito dei prodotti "Software di sicurezza e protezione dati" risulta disponibile il metaprodotto "CPV 72267100-0 - Manutenzione di software".

Stante la situazione sopra delineata, si evidenzia la possibilità di procedere all'utilizzo del Contratto Esecutivo "OPO" stipulato con Olivetti S.p.A. nell'ambito del Contratto Quadro Ripetizione "OPA" di Consip S.p.A.

Allegato 1

Disponibilità di spesa prevista per la fornitura oggetto di affidamento

Per il servizio di manutenzione del prodotto RSA – Security Analytics è previsto un impegno di spesa pari ad € 9.900,00 (oltre oneri di legge, inclusi oneri di sicurezza da interferenza pari a Euro zero).

Per il servizio specialistico a consumo è previsto un impegno di spesa pari a Euro 29.400,00 (oltre oneri di legge, inclusi oneri di sicurezza da interferenza pari a Euro zero) per un numero complessivo stimato di 18 giorni uomo.

L'importo è stato determinato sulla base di quanto corrisposto nell'anno 2015 per la manutenzione e il supporto specialistico in fase di avvio in esercizio del prodotto RSA – Security Analytics ed è commisurato alle attività previste nell'anno in corso.

L'importo rientra nelle previsioni di spesa comprese correntemente nel budget 2016 della Direzione Datacenter ed è quindi coperto dalle CTE di tutti gli Enti Consorziati che utilizzano i servizi del Datacenter per l'erogazione in continuità delle risorse elaborative attestate presso la Server Farm del CSI Piemonte.

Giustificazione della richiesta

In considerazione di quanto sopra esposto, si richiede di procedere all'approvvigionamento in oggetto attraverso il Contratto esecutivo "OPO" ancora vigente con Olivetti S.p.A., aggiornando il Piano dei Fabbisogni con l'inserimento dei servizi di manutenzione delle licenze RSA e i relativi Servizi professionali di supporto specialistico.

Torino, 6 Luglio 2016

Direzione Datacenter
(Stefano Lista)
FIRMATO IN ORIGINALE

Direzione Amministrazione e
Approvvigionamenti
(Franco Ferrara)
FIRMATO IN ORIGINALE