ALLEGATO 4

CAPITOLATO TECNICO

GARA PER LA FORNITURA DI ACCESSI ALLE BANCHE DATI E FEED RECORDED FUTURE E VIRUS TOTAL PER IL SUPPORTO ALLE ATTIVITÀ DI THREAT INTELLIGENCE DEL CERT SOGEI — ID 2169 — CIG 8029173B28

INDICE

1. PREMESSA

Il presente documento, nell'ambito della "*Gara a procedura aperta ai sensi del D.Lgs. 50/2016 e s.m.i., per la fornitura di accessi alle banche dati e feed «Recorded Future» e «Virus Total» per il supporto alle attività di Threat intelligence del CERT SOGEI*", descrive le condizioni, le modalità, le caratteristiche ed i livelli di servizio oggetto delle prestazioni.
Per agevolare la lettura del presente Capitolato tecnico viene di seguito riportato il glossario dei termini più frequentemente utilizzati:

Capitolato tecnico	il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi la fornitura
CERT	Computer Emergency Response Team beneficiaria della fornitura
Consip	la Società che, in qualità di stazione appaltante, aggiudica la fornitura del servizio oggetto del presente Capitolato
Committente	si intende la SOGEI, Società Generale di Informatica S.p.A.
Contratto	il contratto che verrà stipulato tra la SOGEI e l'Aggiudicatario che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura
DDE	Direttore della Esecuzione di SOGEI
Fornitura	il complesso delle attività oggetto del presente Capitolato tecnico
Fornitore o Impresa o Aggiudicatario	Si intende l'Impresa fornitrice, il Raggruppamento temporaneo d'imprese, il Consorzio o in generale il soggetto aggiudicatario della gara che stipula il presente contratto con la Committente
Listini	si intendono gli elenchi dei prodotti e/o servizi relativi alle componenti di sicurezza delle categorie tecnologiche (Brand) Recorded Future e Virus Total
Malfunzionamento	qualsiasi anomalia funzionale dei prodotti software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso
MEF	Ministero dell'Economia e delle Finanze
Produttori	si intendono le categorie tecnologiche relative ai (Brand) Recorded Future e Virus Total
Responsabile della fornitura	persona individuata dall'Aggiudicatario come interlocutore di SOGEI e responsabile di tutte le attività contrattuali
Sistema Informativo	il Sistema Informativo della fiscalità con sede in Via Mario Carucci n.99

Se non diversamente specificato, i termini temporali espressi nel presente Capitolato sono tutti da intendersi come solari (di calendario).

Nel prosieguo della presente Capitolato, laddove vengano riportate caratteristiche tecniche, queste sono sempre da intendersi come requisiti minimi della Fornitura, se non diversamente specificato.

2. CONTESTO DI RIFERIMENTO

Il presente documento descrive gli aspetti relativi alla fornitura per il supporto alle attività di threat intelligence necessari per l'aggiornamento e il potenziamento dei sistemi che costituiscono le attuali infrastrutture per la sicurezza informatica del CERT SOGEI.
Il Computer Emergency Response Team di SOGEI, istituito come struttura nel 2015 e costituito da un gruppo di esperti in ambito cyber security, ha infatti come obiettivo quello di rilevare le minacce che si originano nel cyber spazio e di fornire – tra gli altri – servizi di prevenzione e reazione agli incidenti di sicurezza informatica.
Le attività di prevenzione atte a mitigare i rischi in maniera proattiva, così come di analisi svolta durante un attacco informatico ovvero in seguito all'accaduto, richiedono la disponibilità di una base di conoscenza che raccolga le evidenze tecniche riguardanti minacce e/o la sicurezza degli asset aziendali.
L'acquisizione è richiesta al fine di garantire l'azione Amministrativa e la fornitura dei servizi per lo svolgimento delle attività di threat intelligence nel rispetto del piano strategico della cyber security del CERT SOGEI, a tutela dei clienti (Costituency del MEF), cittadini, dipendenti, nonché dei propri asset aziendali.

3. OGGETTO DELLA FORNITURA

La presente acquisizione ha ad oggetto la fornitura degli accessi alle banche dati Recorded Future e Virus Total per supportare le attività di threat intelligence del CERT SOGEI.
L'accesso alle banche dati deve essere disponibile H24, 7 giorni su 7.
In particolare sono oggetto di fornitura tutte le componenti di sicurezza appartenenti ai listini delle categorie tecnologiche (Brand) di seguito elencate:

- **Recorded Future** (produttore Recorded Future Inc.);
- **Virus Total** (servizio offerto dalla Società Chronicle Security Ltd., sussidiaria di Alphabet Inc.).

per aggiornamento e/o potenziamento delle soluzioni delle rispettive categorie merceologiche da erogarsi in favore del CERT SOGEI, ivi comprese tutte le attività connesse allo svolgimento delle prestazioni medesime così come regolamentate, oltre che dal presente Capitolato, anche dallo Schema di contratto.

La tabella 1 riporta componenti di sicurezza appartenenti ai suddetti listini:

Tabella 1

Brand	Item (descrizione)
Recorded Future	**Advanced–1** (**Annual license** for one named user of the Recorded Future Portal with Advanced level access)
	1 Advanced user License (**Annual license** for one named users of Recorded Future Enterprise Edition with full analyst access level)
	Automation API (Hosted **1 year** API **subscription license** for 50 credits per day)
	CON-INT (Hosted **1 year** Connect API for 1 product integration **subscription license** product selected from this list: https://www.recordedfuture.com/available-integrations/)
	Analyst On–Demand (**12 credits** for on-demand RFIs (requests for information) or recurring threat reports delivered by Recorded Future Intelligence Services. **Credits expire 1 year from date of purchase :**Flash Report (1 credit); Threat Profile (3 credits); Weekly Threat Landscape (3 credits per 3 months); Focused Long-Form Intel Report (5 credits)).
	2 Training Credit (**8 hours of live, onsite delivery of training courses** available in the Recorded Future Training Catalog. Includes access to the training course supporting materials via the Recorded Future online learning management system. **Credits expire 1 year from date of purchase**)

Brand	Item (descrizione)
Virus Total	VIRUSTOTAL ENTERPRICE – **Starter** Profile (**1 year Subscription** Starter Profile included: 100 Search&Download per Month; API Automation calls 500 per day; 25 YARA Rules; Support)
	VIRUSTOTAL ENTERPRICE – **Basic** Profile (**1 year Subscription** Basic Profile included: 300 Search&Download per Month; API Automation calls 1000 per day; 2 Retrohunts per Month; 25 YARA Rules; Support)
	VIRUSTOTAL ENTERPRICE – **Professional** Profile (**1 year Subscription** Professional Profile included: 5.000 Search&Download per Month; API Automation calls 10.000 per day; 5 Retrohunts per Month; 25 YARA Rules; Support)
	VIRUSTOTAL ENTERPRICE – **Enterprise** Profile (**1 year Subscription** Enterprise Profile included: 5.000 Search&Download per Month; API Automation calls 30.000 per day; 25 Retrohunts per Month; 100 YARA Rules; Private Graph 25 Graphs; threat hunter pro - 1year retrohunt; Support)

La tabella 2 riporta le quantità delle componenti di sicurezza – appartenenti ai listini delle categorie tecnologiche sopra indicate – utilizzate solo ai fini della determinazione della base d'asta:

Tabella 2

categoria merceologica	Item (descrizione)	Q.tà
Recorded Future	**Advanced–1** (**Annual license** for one named user of the Recorded Future Portal with Advanced level access)	2
	1 Advanced user License (**Annual license** for one named users of Recorded Future Enterprise Edition with full analyst access level)	3
	Automation API (Hosted **1 year** API **subscription license** for 50 credits per day)	5
	CON-INT (Hosted **1 year** Connect API for 1 product integration **subscription license** product selected from this list: https://www.recordedfuture.com/available-integrations/)	1

categoria merceologica	Item (descrizione)	Q.tà
Virus Total	**VIRUSTOTAL ENTERPRICE – Professional Profile** (**1 year Subscription** Professional Profile included: 5.000 Search&Download per Month; API Automation calls 10.000 per day; 5 Retrohunts per Month; 25 YARA Rules; Support)	1

Resta fermo che la Committente potrà variare le quantità sopra indicate così come acquistare le componenti non quantificate, secondo il proprio fabbisogno, nel rispetto dell'importo massimo contrattuale come meglio precisato nel successivo par. 6.2.

La Fornitura si intende omnicomprensiva dell'invio e attivazione delle credenziali delle componenti di sicurezza (all'indirizzo e-mail che sarà fornito da SOGEI) e dei servizi di supporto alla configurazione (se prevista), supporto al collaudo e garanzia.

Tutte le attività e la documentazione relative all'oggetto di fornitura dovranno essere in lingua italiana e/o inglese.

4. DURATA DEL CONTRATTO

Il contratto ha durata di **36 mesi** a decorrere dalla data di sottoscrizione.

La Committente si riserva di redigere apposito verbale di avvio dell'esecuzione del contratto in contraddittorio con il Fornitore.

Durante il periodo di durata contrattuale SOGEI potrà emettere gli ordinativi di fornitura.

All'atto della stipula l'Aggiudicatario fornirà a Sogei i listini (di cui al par. 3) aggiornati e completi alla data.

Sogei si riserva di acquistare le componenti di sicurezza appartenenti ai listini delle categorie tecnologiche indicate al par. 3 (eventualmente aggiornate alla data della stipula e/o in fase di esecuzione contrattuale) Recorded Future Analytics Package per 2 Utenti (no API) e *VIRUSTOTAL ENTERPRICE – Basic Profile* a partire dal mese di settembre 2020.

Gli ordinativi di fornitura emessi nell'ultimo mese di vigenza del contratto avranno ad oggetto prestazioni di durata non superiore a 12 (dodici) mesi.

5. LUOGO DI LAVORO

L'erogazione dei servizi di fornitura avverrà c/o la sede SOGEI di Via Mario Carucci in Roma.

6. MODALITÀ DI EROGAZIONE DEI SERVIZI

Vengono di seguito specificate le modalità di erogazione dei servizi oggetto di fornitura.

6.1. ATTIVITÀ PRELIMINARI ALLA EMISSIONE DEGLI ORDINATIVI DI FORNITURA

Contestualmente alla stipula del contratto, l'Aggiudicatario dovrà comunicare alla SOGEI:

- il nominativo del proprio rappresentante designato quale *Responsabile della fornitura*, il quale assumerà il ruolo di referente per tutte le attività previste dal contratto, nonché di interlocutore unico della SOGEI;
- un apposito indirizzo di posta elettronica, al quale SOGEI inoltrerà richiesta della/e componente/i di sicurezza di cui al par.3, attraverso invio/i di ordinativo/i di fornitura ed un numero telefonico/fax per tutte le altre comunicazioni (come meglio dettagliato nel successivo par.9).

Sarà cura del Responsabile della fornitura curare la gestione amministrativa del contratto, delle attività legate alla fatturazione e di verificare il rispetto di tutti gli adempimenti contrattuali.
Si precisa che, ove richiesto da SOGEI, l'Aggiudicatario dovrà fornire il nominativo di un referente, anche prima della stipula del contratto, ai fini degli adempimenti prodromici alla relativa sottoscrizione.
La fornitura del primo ordinativo, sarà attinta dai Listini, forniti dall'Impresa all'atto della stipula, delle categorie tecnologiche Recorded Future e Virus Total a totale discrezione della Committente.
SOGEI, per tutta la durata contrattuale, si riserva di attingere dai Listini, eventualmente aggiornati/integrati secondo le modalità descritte al par. 7 del presente Capitolato tecnico.

6.2. RICHIESTE DI FORNITURA: PRIMO ORDINATIVO ED ORDINATIVI SUCCESSIVI

La fornitura inizierà ad essere erogata con il primo ordinativo di fornitura e comprenderà prodotti acquisiti dai listini (forniti dall'Aggiudicatario all'atto della stipula e/o, eventualmente, aggiornati/integrati) la cui composizione sarà a totale discrezione della Committente.
Per effettuare una successiva richiesta di Fornitura, la SOGEI comunicherà nuovamente all'Impresa l'elenco delle componenti di sicurezza che intende acquisire, per il tramite dell'invio di un nuovo ordinativo di fornitura, sulla base dei listini delle categorie tecnologiche (Brand) oggetto di fornitura.
In particolare la richiesta di fornitura, avverrà mediante invio di un ordinativo di fornitura via e-mail all'indirizzo indicato dall'Impresa di cui al paragrafo 6.1. La data di notifica di consegna

dell'invio della suddetta e-mail costituirà il riferimento temporale per il rispetto dei tempi esecutivi della Fornitura.
In fase di predisposizione dell'ordinativo di fornitura, la Committente si riserva di variare autonomamente – in base alle proprie esigenze tecnico organizzative – i quantitativi da acquisire delle componenti di sicurezza di ciascun listino, nel rispetto dell'importo di aggiudicazione globale del contratto.
Le componenti di sicurezza attinte dai listini saranno acquisite dalla Committente – per tutta la durata contrattuale – mediante applicazione della (unica) percentuale di sconto di offerto.
Anche in seguito agli aggiornamenti tecnologici (cfr. par. 7) il Fornitore sarà obbligato a fornire lo stesso sconto percentuale offerto in aggiudicazione anche sulle nuove voci di listino per tutte le componenti di sicurezza oggetto di fornitura.

6.3. ATTIVITÀ ESECUTIVE RELATIVE AGLI ORDINATIVI (PRIMO E SUCCESSIVI)

Entro 10 (dieci) giorni lavorativi dalla data di notifica di consegna relativa all'e-mail di richiesta di Fornitura della Committente, l'Impresa dovrà provvedere all'invio e attivazione di tutte le credenziali di accesso delle componenti di sicurezza ordinate, pena l'applicazione delle penali di cui al successivo par. 12.
La comunicazione della attivazione ed invio delle credenziali di accesso delle componenti di sicurezza ordinate, dovrà essere inviata all'indirizzo di posta elettronica del DDE e a eventuali ulteriori destinatari indicati da SOGEI all'Aggiudicatario prima della stipula.
Il Fornitore dovrà inviare a tale indirizzo ogni informazione utile e/o necessaria al fine di permettere l'identificazione del/i prodotto/i e la conseguente possibilità di immediato e pieno utilizzo degli stessi.

6.4. MODALITÀ DI EROGAZIONE DEI SERVIZI A LISTINO

Eventuali Servizi Specialistici/Servizi di Formazione presenti nei listini dei Brand, che prevedano la possibilità di erogazione in modalità on-site, dovranno essere erogati direttamente dai Brand attraverso l'impiego di proprio personale, presso il luogo di lavoro di cui al par. 5.
Si precisa che:

- l'erogazione dei Servizi Specialistici/Servizi di Formazione in modalità on-line saranno consuntivati da SOGEI e quindi fatturati dal Fornitore a consuntivo e per l'intero importo, rispetto al/i servizio/i fruito/i;
- l'erogazione dei Servizi Specialistici/Servizi di Formazione in modalità on-site saranno consuntivati da SOGEI e quindi fatturati dal Fornitore a consuntivo e per l'intero importo, rispetto al/i servizio/i fruito/i. Tutte le eventuali spese di trasferta non ricomprese nella/e voce/i di listino per l'erogazione dei suddetti servizi in modalità on-site, dovranno essere preventivamente concordate con SOGEI e quindi fatturate dal Fornitore (in aggiunta al/i servizio/i erogato/i) ed andranno ad erodere l'importo di aggiudicazione che in ogni caso non potrà essere superato.

7. AGGIORNAMENTO TECNOLOGICO

L'Impresa − per tutta la durata del contratto – avrà facoltà di proporre aggiornamenti dei Listini, per far fronte ad evoluzioni delle tecnologiche/evoluzioni di prodotto dei rispettivi brand (ad esempio in termini di profili di accesso, eventuali nuove funzionalità, migliorie funzionali, condizioni di maggior vantaggio economico di fornitura, etc.) garantendo comunque la disponibilità delle componenti "core" oggetto di fornitura di ciascun listino e quindi del contratto ovvero:

- per *Recorded Future*, l'accesso alla piattaforma di analisi che include la Cyber Intelligence Analytics, l'alerting, le advanced query capabilities, le funzionalità di collaborazione e reporting;
- per *Virus Total*, l'accesso alla piattaforma VIRUSTOTAL INTELLIGENCE.

Le richieste di aggiornamento del Listino/i dovranno essere in ogni caso adeguatamente motivate/i, proponendo la sostituzione di singoli oggetti già presenti nel listino con altri componenti e/o l'aggiunta di componenti non presenti nella versione precedente del/i Listino/i medesimo/i, e dovranno riguardare le migliorie funzionali in termini di performance e/o le condizioni di maggior vantaggio economico di fornitura.

A fronte della proposta di aggiornamento tecnologico, la Committente si riserva la facoltà di valutare le motivazioni tecniche prodotte dall'Impresa mediante una commissione appositamente costituita da SOGEI che avrà facoltà di richiedere chiarimenti, e che se ritenuta giustificata l'istanza, fornirà il nulla osta all'aggiornamento del/i Listino/i.

8. AGGIORNAMENTO ECONOMICO

In base al Codice degli Appalti è prevista la possibilità di un aggiornamento economico dei Listini che sarà attuato sulla base di una richiesta/proposta del Fornitore, debitamente motivata (e documentata) rispetto alle effettive variazioni verificatesi sui prodotti dei Listini oggetto di Fornitura. Anche a fronte di tali aggiornamenti, la scontistica proposta dall'Impresa all'atto della presentazione dell'Offerta rimarrà invariata anche per il listino eventualmente aggiornato.

La Committente si riserva la facoltà di valutare le proposte dell'Impresa e di approvarle sulla base di una apposita attività istruttoria.

È piena facoltà della Committente la possibilità di rifiutare gli aggiornamenti anche interrompendo il contratto.

9. MODALITÀ DI COMUNICAZIONE

L'Aggiudicatario comunicherà a SOGEI, contestualmente alla presentazione della documentazione per la stipula del contratto:

- un numero di telefono con accesso prioritario;
- almeno un numero di fax;
- un indirizzo di e-mail diretto.

ai quali potrà essere inviata ogni comunicazione relativa all'esecuzione delle attività contrattuali.

In particolare l'Aggiudicatario dovrà garantire la presenza di un esperto specializzato nei prodotti, con conoscenza della lingua italiana, al quale rivolgersi, senza alcun limite sul numero delle chiamate, per ogni comunicazione relativa alla fornitura, ovvero per la soluzione di ogni problematica di malfunzionamento e/o di anomalia dei prodotti.

L'organizzazione del suddetto servizio di comunicazione dovrà essere a carico dell'Aggiudicatario. Resta inteso che, per tutta la durata contrattuale l'Aggiudicatario dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a SOGEI eventuali modifiche.

10. INFORMAZIONI IN MERITO AL TRATTAMENTO E PROTEZIONE DI DATI PERSONALI

L'accesso alle banche dati non prevede la condivisione di dati personali.

11. INFORMAZIONI IN MERITO ALLA SICUREZZA SUI LUOGHI DI LAVORO

L'Aggiudicatario si impegna a porre in essere quanto necessario a garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 "Testo Unico sulla sicurezza durante il lavoro", cooperando e coordinandosi, in particolare, con i referenti della Committente presso cui dovranno essere svolte le attività contrattuali, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.
Si evidenzia che le attività di cui al presente capitolato rientrano nelle fattispecie di cui al comma 3-bis del suddetto articolo, per le quali non sussiste l'obbligo di redigere il DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze).

12. PENALI SUI LIVELLI DI SERVIZIO

SOGEI applicherà le penali, secondo le modalità previste nell'Allegato Contratto C. Speciali art.10 S.