

ALLEGATO 2

CAPITOLATO TECNICO

PROCEDURA NEGOZIATA PER LA FORNITURA DELLE SOLUZIONI DI
SICUREZZA VIRUS TOTAL A SUPPORTO DELLE ATTIVITÀ THREAT
INTELLIGENCE PER IL CERT SOGEI – ID 2387

INDICE

1. PREMESSA	3
2. CONTESTO DI RIFERIMENTO	4
3. OGGETTO DELLA FORNITURA	4
4. DURATA DEL CONTRATTO	8
5. LUOGO DI LAVORO	9
6. MODALITÀ DI EROGAZIONE DEI SERVIZI	9
6.1. ATTIVITÀ PRELIMINARI ALLA EMISSIONE DEGLI ORDINATIVI DI FORNITURA	9
6.2. RICHIESTE DI FORNITURA: PRIMO ORDINATIVO ED ORDINATIVI SUCCESSIVI	9
6.3. ATTIVITÀ ESECUTIVE RELATIVE AGLI ORDINATIVI (PRIMO E SUCCESSIVI)	10
7. AGGIORNAMENTO TECNOLOGICO	10
8. AGGIORNAMENTO ECONOMICO	11
9. MODALITÀ DI COMUNICAZIONE.....	11
10. INFORMAZIONI IN MERITO AL TRATTAMENTO E PROTEZIONE DI DATI PERSONALI	11
11. PENALI SUI LIVELLI DI SERVIZIO	11

1. PREMESSA

Il presente documento - nell'ambito della Procedura Negoziata, ai sensi dell'art. 63, comma 2, lett. b), n. 3) del D.Lgs. n. 50/2016, per la fornitura delle soluzioni di sicurezza Virus Total di Chronicle Security a supporto delle attività threat intelligence per il 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, affida la fornitura 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 ed il Fornitore 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, aggiudicataria della presente procedura negoziata che stipula il contratto con la Committente
Listino	si intende l'elenco dei prodotti e/o servizi relativi alle componenti di sicurezza Virus Total di Chronicle Security
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
Produttore/Vendor	si intende la Società Chronicle Security
Responsabile della fornitura	persona individuata dal Fornitore come interlocutore verso 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).

Di seguito nel 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 e delle 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 proattiva e reattiva agli eventi ed 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 delle soluzioni di sicurezza a listino Virus Total di Chronicle Security a supporto delle attività threat intelligence per il CERT SOGEI.

L'accesso ai data base del produttore per l'erogazione dei servizi sopra detti, deve essere disponibile H24, 7 giorni su 7.

In particolare, costituiscono oggetto di fornitura tutte le componenti di sicurezza appartenenti al sopraindicato listino, **per aggiornamento e/o potenziamento delle soluzioni da erogarsi in favore del CERT SOGEI e del MEF**, 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 le componenti di sicurezza appartenenti al suddetto listino, oltre alla indicazione delle quantità, utilizzate solo ai fini della determinazione della base d'asta:

Chronicle Security (Listino Virus Total)	Descrizione prodotti di listino Virus Total	Livello di servizio	Q.tà
	Threat Hunter Pro (VTGREP, Retrohunt, faceted searches)	12 months retrospection	2
	Retrohunt	5/mese	1
	API	10.000/giorno	1
		20.000/giorno	1
		30.000/giorno	1
	VTI	1.000/mese	1
		15.000/mese	1
		50.000/mese	1
	Private Graph	5/anno	1
		25/anno	2

Tabella 1

Resta fermo che la Committente potrà variare l'acquisizione dei prodotti e/o delle quantità indicate in Tabella 1, così come acquistare le ulteriori componenti presenti a listino Virus Total, riportate in Tabella 2, secondo il proprio fabbisogno, sia rispetto ai prodotti che alle relative quantità, nel rispetto dell'importo massimo contrattuale come meglio precisato nel successivo par. 6.2.

Prodotto	Livello di servizio
VT - Basic	si veda Tabella 3
VT - Professional	si veda Tabella 3
VT - Enterprise	si veda Tabella 3
VT- DUET	si veda Tabella 3
VT - Unlimited	si veda Tabella 3
File Feed – add on	N.A.
URL Feed – add on	N.A.
Sandbox Feed – add on	N.A.
Prodotto	Livello di servizio
Threat Hunter Pro (VTGREP, Retrohunt, faceted searches)	12 months retrospection
Prodotto	Livello di servizio
VT Monitor	100 MB
	150 MB
	500 MB
	1 GB
	2 GB
	4 GB
Prodotto	Livello di servizio
Retrohunt	5/mese
	10/mese
	25/mese
	50/mese
Prodotto	Livello di servizio
Yara Rules	25/anno
	50/anno
	100/anno
Prodotto	Livello di servizio
API	1.000/giorno
	5.000/giorno
	10.000/giorno
	20.000/giorno
	30.000/giorno

	50.000/giorno
	100.000/giorno
	250.000/giorno
	500.000/giorno
	750.000/giorno
	1.000.000/giorno
	2.000.000/giorno
	3.000.000/giorno
	4.000.000/giorno
	5.000.000/giorno
	10.000.000/giorno
	20.000.000/giorno
	30.000.000/giorno
	40.000.000/giorno
	50.000.000/giorno
Prodotto	Livello di servizio
VTI	100/mese
	300/mese
	1.000/mese
	5.000/mese
	15.000/mese
	30.000/mese
	50.000/mese
	100.000/mese
	200.000/mese
	300.000/mese
	400.000/mese
	500.000/mese
	600.000/mese
	700.000/mese
	800.000/mese
	900.000/mese
	1.000.000/mese
Prodotto	Livello di servizio

Classificazione del documento: Consip Public

Procedura negoziata ai sensi dell'art. 63 del D. Lgs. n. 50/2016, finalizzata alla stipula di un contratto per la fornitura delle soluzioni di sicurezza Virus Total a supporto delle attività threat intelligence per il CERT Sogei – ID 2387

Allegato 2 – Capitolato tecnico

Private Graph	5/anno
	25/anno
	100/anno

Tabella 2

	Basic	Professional	Enterprise	DUET	Unlimited
API	1k/giorno	10k/giorno	30K/giorno	100M/mese	100M/mese
VTI: Searches/Downloads	300/mese	5.000/mese	5.000/mese	20.000/mese	20.000/mese
Retrohunts (60 Day lookback)	2/mese	5/mese	25/mese	1k/mese	1k/mese
YARA Rules	25/anno	25/anno	100/anno	20.000/anno	20.000/anno
Threat Hunter Pro (VTGREP, Retrohunt, faceted searches) - 12 months retrospection	add on	add on	Included	Included	Included
Private Graph	add on	add on	25/anno	10.000/anno	10.000/anno
Supporto	included	included	included	included	included
File Feed	add on	add on	add on	add on	included
URL Feed	add on	add on	add on	add on	included
Sandbox Feed	add on	add on	add on	add on	included

Tabella 3

Si precisa che tutti gli elementi indicati a listino in Tabella 2 sono comprensivi del supporto da parte del team di ingegneri di Virus Total.

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.

Tutta la documentazione relativa all'oggetto di fornitura dovrà 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.

SOGEI si riserva di acquistare le componenti di sicurezza appartenenti al listino riportato in **Error! Reference source not found.**, ovvero **Tabella 2**, eventualmente aggiornate in fase di esecuzione contrattuale come indicato al successivo paragrafo 7.

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 n.99 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, il Fornitore 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, il Fornitore 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 dal Listino, fornito dall'Impresa all'atto della stipula, relativo alle componenti tecnologiche Virus Total, a totale discrezione della Committente.

SOGEI, per tutta la durata contrattuale, si riserva di attingere dal suddetto Listino, eventualmente aggiornato/integrato 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 dal Listino (forniti dal Fornitore all'atto della stipula e/o, eventualmente, aggiornato/integrato in corso di esecuzione contrattuale) 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 del listino oggetto di fornitura.

Classificazione del documento: Consip Public

Procedura negoziata ai sensi dell'art. 63 del D. Lgs. n. 50/2016, finalizzata alla stipula di un contratto per la fornitura delle soluzioni di sicurezza Virus Total a supporto delle attività threat intelligence per il CERT Sogei – ID 2387

Allegato 2 – Capitolato tecnico

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 delle componenti di sicurezza da acquisire, nel rispetto dell'importo di aggiudicazione globale del contratto.

Le componenti di sicurezza attinte dal Listino saranno acquisite dalla Committente – per tutta la durata contrattuale – mediante l'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.

Tutti i servizi presenti nel listino Virus Total di Chronicle Security, andranno ad erodere l'importo di aggiudicazione che in ogni caso non potrà essere superato.

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 inviata dalla 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. 11.

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 agli eventuali ulteriori destinatari indicati da SOGEI al Fornitore.

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.

7. AGGIORNAMENTO TECNOLOGICO

Il Fornitore – per tutta la durata del contratto – avrà facoltà di proporre aggiornamenti del Listino, per far fronte ad evoluzioni tecnologiche/evoluzioni di prodotto (ad esempio in termini di profili di accesso, nuove funzionalità, migliorie funzionali, condizioni di maggior vantaggio economico di fornitura, etc.).

Le richieste di aggiornamento del Listino dovranno essere in ogni caso adeguatamente motivate, 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 Listino medesimo, e dovranno riguardare le migliorie funzionali in termini di performance e/o le condizioni di maggior vantaggio economico di fornitura.

Classificazione del documento: Consip Public

Procedura negoziata ai sensi dell'art. 63 del D. Lgs. n. 50/2016, finalizzata alla stipula di un contratto per la fornitura delle soluzioni di sicurezza Virus Total a supporto delle attività threat intelligence per il CERT Sogei – ID 2387

Allegato 2 – Capitolato tecnico

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 Listino.

8. AGGIORNAMENTO ECONOMICO

A decorrere dal secondo anno di esecuzione del contratto 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 ferma ed 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

Il Fornitore comunicherà a SOGEI, contestualmente alla presentazione della documentazione per la stipula del contratto:

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

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

In particolare il Fornitore 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 del Fornitore.

Resta inteso che, per tutta la durata contrattuale il Fornitore 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. PENALI SUI LIVELLI DI SERVIZIO

SOGEI applicherà le penali, secondo le modalità previste nell'Allegato n.6 allo Schema di Contratto art.10.