



Consip S.p.A.

"Fornitura di un accesso per 24 mesi a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet"

CAPITOLATO TECNICO

***FORNITURA DI UN ACCESSO PER 24 MESI A BITSIGHT SECURITY PERFORMANCE
ADVANCED, COMPRENSIVA DELLE SUBSIDIARY AGGIUNTIVE PER IL MONITORAGGIO
DELLE SUBNET E DEI SERVIZI EROGATI DA SOGEI SU INTERNET***



INDICE

1	PREMESSA	3
1.1	Definizioni.....	3
1.2	Contesto di riferimento	3
2	OGGETTO DEL SERVIZIO.....	5
2.1	Comunicazione di vulnerabilità e/o DataBreach.....	5
2.2	Verifica di conformità.....	5
3	GESTIONE DEL SERVIZIO	7
3.1	Responsabile delle attività contrattuali	7
3.2	Modalità di comunicazione	7
3.3	Adempimenti per la Sicurezza.....	7
3.4	Lingua	7
3.5	Riservatezza.....	7
4	PENALI	10
5	MODALITÀ DI FATTURAZIONE.....	11



1 PREMESSA

1.1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- CONSIP: la società che, in qualità di stazione appaltante, affida la fornitura oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A., beneficiaria della Fornitura;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi la fornitura;
- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- Fornitura: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria della fornitura;
- 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;
- Produttore: la società BitSight Technologies;
- Responsabile delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali;
- Sistema Informativo: il sistema informativo gestito da Sogei con sede in Via Mario Carucci 99.

1.2 CONTESTO DI RIFERIMENTO

La piattaforma di Bitsight Security fornisce una classificazione oggettiva basata sull'osservazione esterna delle performance di sicurezza di un'azienda.

L'algoritmo di Bitsight tramite sensori e crawler sulla rete colleziona terabyte di dati di sicurezza provenienti da sensori sparsi sul globo. A partire dai dati raccolti sono ottenuti indicatori di compromissione, di macchine infette, configurazioni improprie e scarso livello di sicurezza. I dati raccolti e normalizzati vengono mappati sulla base dell'indirizzamento Internet pubblico di ogni singola azienda, creando, in questo modo, una classificazione delle prestazioni di sicurezza.

Tale classificazione è oggettiva, basata su dati accessibili esternamente e fornisce una visibilità continua su tali prestazioni e consente di intervenire specificatamente su ciascuna problematica.



"Fornitura di un accesso per 24 mesi a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet"

Le valutazioni di sicurezza di BitSight sono composte da due classi principali di dati:

- dati di evento
- dati di diligenza

I dati di evento vengono raccolti passivamente. Tramite appositi sensori sui dati pubblici che rilevano evidenze di infezioni da botnet, messaggi di spam, evidenze di server di malware, e altre indicazioni che potrebbero identificare uno stato compromesso della rete osservata.

I dati di diligenza raccolti da Bitsight sono relativi alla sicurezza di quanto è visibile su internet della azienda analizzata come le configurazioni SSL, SPF e DKIM.

Il CERT Sogei al fine di una migliore valutazione del rischio informatico ha acquisito l'utilizzo della piattaforma Bitsight che effettua il monitoraggio continuo dello stato di salute dei sistemi esposti su Internet dal punto di vista della sicurezza.

L'Analisi fornita dalla piattaforma Bitsight, a partire da tutto ciò che visibile su Internet, viene ottenuta tramite una serie di indicatori tecnici quali: presenza di Botnet, di Spam, di porte aperte sui server, qualità dei certificati, dei protocolli usati, presenza di protocolli di comunicazioni non usuali, quale ad esempio Torrent, ed altri ancora.

La soluzione si sposa appieno con un'ampia serie di misure previste dalla NIST CSF e risponde anche alla richiesta della GDPR di evitare perdite di dati ed effettuare costanti risk assessment.



2 OGGETTO DEL SERVIZIO

Il presente Capitolato disciplina la fornitura di un accesso a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet per 24 (ventiquattro) mesi, da erogarsi in favore della 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 e dalle Condizioni Particolari.

La Società, in particolare, dovrà fornire l'accesso a BitSight Security Performance Advanced.

Il servizio di accesso al portale deve essere disponibile H24, 7 giorni su 7.

La Società dovrà attivare le credenziali già in possesso di Sogei per 24 (ventiquattro) mesi decorrenti dalla data di stipula del contratto.

2.1 COMUNICAZIONE DI VULNERABILITÀ E/O DATA BREACH

Il fornitore si impegna fermamente nel fornire al contraente tutte le informazioni necessarie per proteggere la propria azienda segnalando tempestivamente le vulnerabilità di sicurezza dei prodotti oggetto del presente contratto siano essi hw, sw o Open source per tutta la durata del contratto.

Le segnalazioni devono riguardare non solo le vulnerabilità rilevate da organizzazioni esterne, ma anche tutte quelle che vengono trovate internamente a prescindere dall'esistenza o meno di appositi contratti di manutenzione. In particolare, deve essere data tempestiva comunicazione, anche telefonica, di tutte le vulnerabilità verificate dal brand siano esse di tipo Self-disclosure, Third-party disclosure, Vendor disclosure, Full disclosure.

Tutte le comunicazioni al riguardo devono essere inviate cifrate mediante la Public Key PGP CERT, disponibile al link del CERT SOGEI <https://www.sogei.it/it/sogei-homepage/it-governance/sicurezza-e-tutela-dei-dati/computer-emergency-response-team.html>, ad uno dei seguenti indirizzi: cert@pec.sogei.it o cert@sogei.it.

Segnalazioni di gravità rilevante dovranno essere segnalate tempestivamente anche telefonicamente al numero mobile +39 320 4314519 disponibile h24 7/7.

Eventuali ulteriori modalità di comunicazione delle segnalazioni di vulnerabilità verranno concordate tra il responsabile del contratto per il fornitore e il RUP/DDE di SOGEI entro 10 giorni dalla loro nomina o comunque all'atto della 1° riunione formale di kick off del contratto.

2.2 VERIFICA DI CONFORMITÀ

Entro 15 (quindici) giorni a decorrenti dalla consegna e attivazione delle credenziali dei prodotti software, queste ultime saranno sottoposte a verifica di conformità, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale.

La Società è tenuta a prestare alla Sogei, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Sogei quanto necessario alle operazioni di verifica di conformità.



"Fornitura di un accesso per 24 mesi a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet"

La Società potrà intervenire alla verifica di conformità, anche attraverso propri rappresentanti. In tal caso detti rappresentanti sono tenuti a sottoscrivere i documenti di verifica di conformità che verranno redatti da Sogei (verbali, certificato, ecc.)

In caso di esito negativo della verifica di conformità, ferma restando l'applicazione delle penali, di cui al successivo paragrafo 4, la Società dovrà provvedere, a propria cura e spese, entro il termine che le verrà comunicato dalla Sogei, alla eliminazione dei difetti e/o delle carenze riscontrati entro il termine massimo di 5 giorni lavorativi, oppure di 3 giorni lavorativi se il malfunzionamento segnalato riguarda problemi di sicurezza del prodotto, ovvero una vulnerabilità tecnica che metta in pericolo l'integrità della piattaforma e dei contenuti esposti

Dopo la comunicazione, da parte della Società, dell'avvenuta eliminazione dei difetti e/o delle carenze, la Sogei procederà a nuova verifica di conformità nei termini e con le modalità di cui ai commi precedenti.

In caso di ulteriore esito negativo della verifica di conformità, la Sogei avrà facoltà di risolvere il contratto e di fare eseguire tutta o in parte la fornitura a terzi in danno della Società e fatto salvo in ogni caso il diritto al risarcimento di tutti i danni comunque subiti.

A completamento della verifica positiva sarà prodotto la "Nota di Verifica di conformità del servizio" che dovrà essere sottoscritta dal Responsabile della Fornitura e dal Responsabile Sogei.



3 GESTIONE DEL SERVIZIO

Il contratto avrà efficacia dalla data della sua stipula e avrà una durata di 24 (ventiquattro) mesi e, comunque, sino al completo adempimento di tutte le obbligazioni contrattuali.

3.1 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI

La Società dovrà comunicare, trasmettendolo con la documentazione per la stipula, il nominativo del Responsabile del Servizio, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni. La Società deve provvedere in piena autonomia al coordinamento e all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti da Sogei.

Sarà compito del Responsabile curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

3.2 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare, contestualmente alla presentazione della documentazione per la stipula, un numero di fax, un indirizzo e-mail, un indirizzo pec e un numero di telefono al quale rivolgersi, senza alcun limite sul numero di chiamate, per ogni comunicazione relativa alla fornitura.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Sogei eventuali modifiche.

3.3 ADEMPIMENTI PER LA SICUREZZA

La Società s'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 e degli uffici dell'Amministrazione Finanziaria 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).

3.4 LINGUA

Tutte le attività e la documentazione saranno in lingua italiana e/o lingua inglese.

3.5 RISERVATEZZA

Tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra la Società e Sogei sono riservati; pertanto, è richiesta la massima attenzione per il loro utilizzo, in particolare se questo avviene al di fuori delle sedi Sogei.



"Fornitura di un accesso per 24 mesi a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet"

La Società non potrà utilizzare o condividere con terzi, a nessun titolo e in nessun modo, la documentazione, i dati o qualsiasi altra informazione fornita da Sogei, ancorché inserita attraverso il portale sui sistemi Bitsight o al di fuori delle attività oggetto del contratto.

Nello specifico, con "Informazioni Riservate" si intendono tutte le informazioni di una delle Parti, di natura tecnica, commerciale o di altro tipo (inclusi, a titolo esemplificativo ma non esaustivo, segreti commerciali, know-how e informazioni relative alla tecnologia, partner strategici, clienti, piani aziendali, attività promozionali e di marketing, finanze e altri affari commerciali di detta Parte), che sono rese note dalla Parte divulgante alla Parte ricevente o che sono altrimenti apprese dalla Parte ricevente nel corso dei propri dialoghi o rapporti commerciali con la Parte divulgante, oppure durante il suo accesso fisico o elettronico ai locali o ai servizi della Parte divulgante, e che sono state identificate come di proprietà e/o riservate o di cui la Parte ricevente, per la natura delle circostanze relative alla divulgazione o alla ricezione, dovrebbe essere informata che queste debbano essere trattate come di proprietà e riservate.

In particolare, si specifica che le "Informazioni Riservate" della Sogei sono costituite dall'elenco delle organizzazioni che Sogei sta monitorando e dalle informazioni dell'Utente incluse nel portale amministrativo, nonché tutte informazioni trattate e i documenti scambiati tra con la Società, mentre le "Informazioni Riservate" della Società, relative anche ai servizi BitSight includono, a titolo esemplificativo ma non esaustivo, i Servizi BitSight, i Dati BitSight e i termini, le condizioni e i prezzi inclusi nel presente Capitolato e nel Contratto.

Ciascuna Parte si impegna a mantenere la riservatezza delle Informazioni Riservate dell'altra Parte e a non divulgare tali Informazioni Riservate a individui che non siano dipendenti, membri del consiglio di amministrazione, consulenti legali, contabili, partner, appaltatori o consulenti, purché abbiano la necessità di conoscere le informazioni e che siano soggetti ad obblighi di riservatezza non meno restrittivi di quelli qui esposti. Una Parte che riceve le Informazioni Riservate dell'altra Parte non dovrà utilizzare tali informazioni per scopi diversi da quelli ragionevolmente richiesti ai sensi del presente Capitolato.

Si specifica inoltre che, la definizione di Informazioni Riservate non deve includere le informazioni che la Parte ricevente può dimostrare, attraverso documentazione scritta, come già note alla Parte ricevente prima della relativa divulgazione alla medesima, che erano o sono state rese note o che sono generalmente disponibili al pubblico (in modo diverso dall'azione della Parte ricevente), che sono divulgate o rese disponibili per iscritto alla Parte ricevente senza obbligo di riservatezza da una terza parte avente il diritto in buona fede di farlo, che sono sviluppate in modo indipendente dalla Parte ricevente senza l'utilizzo di nessuna delle Informazioni Riservate dell'altra Parte o, nel caso della Committente, che sono destinate ad essere messe a disposizione di terzi nell'ambito dei Servizi BitSight (come, ad es., annotazioni contrassegnate come "pubbliche" da Sogei che spiegano gli aspetti della sua valutazione, o informazioni fornite dalla Committente per creare, correggere o aggiornare i rispettivi indirizzi IP o domini valutati). Inoltre, ciascuna delle Parti sarà autorizzata a divulgare le Informazioni Riservate, come richiesto, a un ente regolatore con giurisdizione competente su tale Parte o mediante procedura legale obbligatoria, a condizione che la Parte ricevente notifichi tempestivamente alla Parte divulgante la richiesta di tale divulgazione, e dovrà cooperare con la Parte divulgante per precludere o minimizzare tale divulgazione.



Consip S.p.A.

"Fornitura di un accesso per 24 mesi a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet"

Le Parti riconoscono che l'eventuale violazione delle prescrizioni di cui al presente paragrafo può causare danni immediati e irreparabili alla Parte lesa e che i danni monetari possono essere inadeguati a risarcire la Parte lesa per tale violazione. Dopo aver preso atto di quanto precede, le Parti convengono che, in caso di violazione, la Parte lesa avrà il diritto di chiedere un provvedimento ingiuntivo, senza la necessità di porre vincolo, oltre a tutti gli altri rimedi a sua disposizione secondo la legge o in equità. Il presente paragrafo non limita in alcun modo la responsabilità o i danni che possono essere valutati nei confronti della Parte inadempiente in caso di violazione di una qualsiasi delle disposizioni sopra indicate.



4 PENALI

Sogei applicherà le penali, secondo le modalità previste in contratto, nei seguenti casi:

- per ogni giorno lavorativo di ritardo nell'attivazione delle credenziali si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale;
- in caso di esito negativo della verifica di conformità di cui al paragrafo 2.2, si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale, per ogni giorno intercorrente tra la data del verbale negativo e quello positivo.

Nell'ipotesi in cui l'importo delle penali applicabili superi l'ammontare del 10% (dieci per cento) dell'importo contrattuale complessivo, la Sogei avrà il diritto di risolvere, totalmente o parzialmente, il contratto in danno della Società, salvo il diritto dell'eventuale maggior danno.



Consip S.p.A.

"Fornitura di un accesso per 24 mesi a BitSight Security Performance Advanced, comprensiva delle Subsidiary aggiuntive per il monitoraggio delle subnet e dei servizi erogati da SOGEI su internet"

5 MODALITÀ DI FATTURAZIONE

La Società potrà emettere fattura successivamente alla sottoscrizione della nota di verifica di conformità positiva.

Tutte le fatture dovranno riportare il numero di repertorio del contratto ed il codice CIG.

Si precisa che la mancanza di uno di questi elementi consente al committente di rifiutare la fattura entro il termine previsto.