

CAPITOLATO TECNICO

ACQUISIZIONE DELLA SOLUZIONE HADRIAN PER L'AUTOMAZIONE DEL PENETRATION TEST DEI SERVIZI ESPOSTI SU INTERNET

Indice

1	PREMESSA	3
1.1	Definizioni	3
2	OGGETTO E DURATA	4
2.1	Piattaforma e funzioni richieste	5
2.2	Servizi Professionali di supporto	7
2.3	Durata	8
3	GESTIONE DEL CONTRATTO	9
3.1	Responsabile delle attività contrattuali e modalità di comunicazione	9
3.2	Luogo di svolgimento delle attività	9
3.3	Verifica di conformità	9
3.4	Livelli di servizio	10
3.5	Adempimenti per la Sicurezza	11
3.6	Riservatezza	11
4	MODALITÀ DI FATTURAZIONE E PAGAMENTO	13
5	PENALI	14

1 PREMESSA

Consip, in quanto società inclusa nell'elenco consolidato ISTAT, è soggetta agli obblighi previsti dalla normativa nazionale in materia di sicurezza informatica, con particolare riferimento alla Legge n. 90 del 28 giugno 2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" e al Piano Triennale per l'Informatica nella PA 2024-2026, (rif. capitolo 7 "Sicurezza informatica" all'interno del quale si affronta la gestione del rischio cyber).

In linea con quanto richiesto da tali disposizioni e in coerenza con l'obiettivo 7.3 – "Gestione e mitigazione del rischio cyber" (RA7.3.1) del Piano Triennale AGID, risulta fondamentale per Consip dotarsi di strumenti capaci di rafforzare la resilienza delle infrastrutture IT, attraverso test proattivi del livello di sicurezza.

In considerazione della crescente complessità delle minacce cyber e della necessità di una verifica costante dell'efficacia delle difese adottate, si rende quindi necessario acquisire una soluzione software avanzata che garantisca la protezione degli asset critici nonché la continuità operativa di Consip, riducendo i rischi legati a potenziali compromissioni.

1.1 DEFINIZIONI

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

- **Consip S.p.A.:** la Società che, in qualità di stazione appaltante e Committente, affida la fornitura oggetto del presente Capitolato;
- **Capitolato tecnico:** il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi la fornitura;
- **Contratto:** il contratto, che verrà stipulato tra Consip e l'Impresa, che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- **Fornitura:** il complesso dei beni e delle attività oggetto del presente Capitolato;
- **Società:** l'Impresa aggiudicataria della fornitura;
- **Responsabile delle attività contrattuali:** la persona individuata dalla Società come interlocutore di Consip e responsabile di tutte le attività contrattuali.

2 OGGETTO E DURATA

Oggetto dell'appalto è la sottoscrizione delle licenze per l'utilizzo della Piattaforma External Attack Surface Management (EASM) di Hadrian per l'automazione del penetration test dei servizi esposti su internet, comprensiva di servizi professionali di supporto per tutta la durata contrattuale.

La fornitura dovrà ricomprendere le seguenti voci:

CODICE	DESCRIZIONE	QUANTITÀ
A	Canone Triennale per Subscription Hadrian Platform (subscription fino a 100 Assets, integrazione di piattaforme complementari, attivazione, configurazione e supporto completo)	A corpo
B	Servizi professionali di supporto	48 giornate

La soluzione che si intende acquistare deve essere in grado di:

- **mappare e monitorare costantemente la superficie di attacco esterna**, con un focus specifico sui siti web e sulle applicazioni online, identificando vulnerabilità sfruttabili in tempo reale,
- garantire l'**automazione completa del processo di penetration testing**, riducendo tempi e interventi manuali e garantendo un'analisi continua e non intrusiva,
- effettuare una **simulazione realistica di attacchi informatici avanzati**, replicando il comportamento di attori malevoli per verificare l'efficacia delle difese adottate,
- garantire l'**analisi contestualizzata delle vulnerabilità in relazione al rischio aziendale**, evidenziando le potenziali catene di attacco capaci di compromettere le risorse esposte, con particolare attenzione a quelle accessibili via web,
- **eseguire test differenziati** in base al livello di rischio e alla criticità delle risorse esposte su web, simulando tecniche avanzate come privilege escalation, lateral movement ed exfiltration di dati,
- **fornire report dettagliati e prioritizzati**, evidenziando le vulnerabilità con il maggiore impatto potenziale e suggerendo azioni di mitigazione mirate,
- **monitorare continuamente la postura di sicurezza**, adattandosi alle modifiche della superficie di attacco esterna senza necessità di configurazioni manuali,
- **integrare i risultati con altri strumenti di cybersecurity**, migliorando la capacità di prevenzione, rilevamento e risposta agli incidenti.

La società aggiudicataria sarà nominata “Responsabile del trattamento dei dati personali” ai sensi dell’art. 28 del Regolamento UE.

2.1 PIATTAFORMA E FUNZIONI RICHIESTE

La piattaforma, basata su cloud ed integrabile con diverse categorie di soluzioni aziendali, presenta le seguenti caratteristiche:

- Cloud-based no setup required
- SSO and MFA sign on
- Agentless operation
- Multitennant environment
- Non-intrusive scanning options
- Event-based probes
- 200+ hacker modules.
- Designated Customer Success Manager
- Fully guided onboarding
- Support on integrations in existing ecosystem
- Monthly reporting on value and performance
- Customer support without restrictions
- Continuous monitoring potential zero days and alerting on potential hits.

Le funzionalità richieste sono le seguenti:

Scoperta continua

Scansione continua dell'intera rete Internet per identificare nuove risorse e configurazioni in tempo reale. Caratteristiche:

- Continuous filepath scanning
- Detect new domains, subdomains and ports
- Certificate databases
- ML naming conventions prediction
- Dynamic IP tracking
- TCP and UDP port scanning
- ASN detection
- 3rd party SaaS detection - over 10,000 SaaS applications
- Vhost detection
- DNS records and wildcard detection.

Contesto dell'asset

Fingerprints informazioni sul sistema operativo, moduli, librerie, campi di input, metodi di autenticazione, ecc. Caratteristiche:

- Rescans assets when the asset configuration changes
- Technology detection
- Detecting 1000s of different software packages and versions
- Detecting common WordPress plugins
- Detecting OS repositories
- Open-source intelligence (OSINT)

- Threat intelligence - commonly used exploits.

Rischio passivo

Ha 1000 Fingerprint CVE, attacco DoS vulnerabilità, Host Header Injection, TLS vulnerabilità.

Caratteristiche:

- Passive vulnerability detection & validation
- 1000s of CVEs fingerprints
- 100s of CVEs exploit POC's
- DoS attack vulnerability detection
- Host header injection detection
- Exposed session cookies detection
- Weak TLS/certificate detection
- Active vulnerability detection & validation
- Zero-day vulnerability detection
- Active sub(domain) takeover detection
- SQL injection detection
- Open redirection detection
- Credential stuffing (Weak password detection)
- Unrestricted file upload detection
- Open-proxy detection
- Reconnaissance
- Open S3 bucket detection
- RDP exposure detection
- Sensitive files detection
- Backup file exposure detection
- Credential leak detection in exposed configuration files
- Credential leak detection in exposed Github environments
- API key detection
- Source code detection
- Insecure .xml file detection.

Rischio attivo

Ulteriori verifiche oltre i CVE con vulnerabilità zero-day, SQL injection, acquisizione di (sotto)domini, caricamento di file senza restrizioni e rilevamento di proxy aperti.

Convalida

Verifica automatica che i rischi siano sfruttabili prima di allertare i team di sicurezza.

Definizione delle priorità

Definizione delle priorità calcolata automaticamente utilizzando l'impatto tecnico CVSS, il contesto delle risorse, il catalogo KEV e l'intelligence sulle minacce Hadrian. Caratteristiche:

- Static scores Common Vulnerability Scoring System (CVSS 4.0)
- Threat Intelligence
- KEV catalog
- Asset tags

- Automatable

Remediation

Disponibilità delle spiegazioni dei rischi, comprese le descrizioni complete della catena di attacco e le istruzioni per la correzione. Esecuzione automatica di una nuova scansione delle risorse per confermare che i rischi sono stati mitigati correttamente. Caratteristiche:

- Risk descriptions
- Remediation instructions
- Risk archive
- Automatically rescan assets to confirm that risks have been successfully mitigated
- Full descriptions of the attack chain.

User experience

Avvisi personalizzabili e mirati. Grafico degli asset e tag per la visualizzazione e l'organizzazione dei dati. Caratteristiche:

- Customizable targeted alerting, which notifies you automatically of any potential exposures
- Asset graph for data visualization
- Asset tags for labeling, filtering and assignment
- Dashboard that highlights changes to the environment and open risks
- Reporting
- Asset exporting

Integrazioni e servizi

Si integra in 100 soluzioni, tra cui Slack, Jira, Rapid7 e strumenti SIEM/SOAR.

Caratteristiche:

- Designated Customer Success Manager
- Fully guided onboarding
- Support on integrations in existing ecosystem
- Monthly reporting on value and performance
- Customer support without restrictions
- Continuous monitoring potential zero days and alerting on potential hits.

La Società dovrà attivare la soluzione configurata per le specifiche esigenze di Consip, entro 10 giorni lavorativi dalla data di stipula del contratto.

2.2 SERVIZI PROFESSIONALI DI SUPPORTO

Consip si avvarrà di servizi professionali di supporto che verranno richiesti, ove necessario, per sviluppi mirati sulla piattaforma cloud e per integrazioni con prodotti di terze parti.

I servizi professionali di supporto dovranno essere erogati, a consumo, da Specialisti di tecnologie con almeno quindici anni di esperienza.

Per ciascun intervento, a fronte della richiesta di Consip, la Società effettuerà la stima dell'impegno in termini di costi e tempi. La stima dovrà essere formalmente approvata da Consip.

2.3 DURATA

Il contratto acquista efficacia dalla data di stipula e avrà una durata pari a 36 mesi a partire dalla "Data di accettazione della fornitura" (cfr. paragrafo "Verifica di conformità").

3 GESTIONE DEL CONTRATTO

3.1 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI E MODALITÀ DI COMUNICAZIONE

La Società dovrà comunicare il nominativo del Responsabile della fornitura, il quale provvederà in piena autonomia al coordinamento e all'organizzazione delle attività contrattuali, nel rispetto delle specifiche e dei tempi concordati con Consip.

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.

La Società si impegna a comunicare 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 Consip eventuali modifiche.

3.2 LUOGO DI SVOLGIMENTO DELLE ATTIVITÀ

Tutte le attività oggetto del presente Capitolato saranno svolte da remoto.

In casi eccezionali, laddove non fosse possibile l'erogazione da remoto, le attività potranno essere svolte presso la sede di Consip in Roma, via Isonzo 19/E. Eventuali costi di trasferimento e soggiorno del personale coinvolto nelle attività saranno comunque a totale carico della Società.

3.3 VERIFICA DI CONFORMITÀ

All'attivazione della soluzione, Consip effettuerà la verifica del funzionamento della soluzione.

All'esito positivo della suddetta verifica, Consip rilascerà il **Verbale di verifica di conformità**, nel rispetto di quanto previsto dall'articolo "Verifica di conformità" delle Condizioni contrattuali.

All'interno del Verbale di verifica di conformità con esito positivo, sarà indicata la **"Data di accettazione della fornitura"**.

Inoltre, per i Servizi professionali di supporto, ciascun intervento autorizzato verrà sottoposto a verifica di conformità, al completamento dello stesso, da parte di Consip, nel rispetto di quanto previsto dall'articolo "Verifica di conformità" delle Condizioni contrattuali.

Al completamento di ciascun intervento, seguirà la verifica del funzionamento (test). All'esito positivo

La verifica di conformità si intende positivamente superata solo se tutte le prestazioni contrattuali siano state eseguite a perfetta regola d'arte, secondo le modalità indicate nel presente Capitolato tecnico, nel contratto nonché secondo le indicazioni di Consip.

In caso di esito negativo della verifica di conformità, la Società dovrà eliminare i vizi accertati entro il termine massimo di 5 (cinque) giorni lavorativi, salvo il diverso termine che sarà concesso dalla Committente in sede di verifica di conformità. In tale ipotesi la verifica di conformità verrà ripetuta.

Nell'ipotesi in cui anche la seconda verifica di conformità dia esito negativo, la Committente avrà facoltà di risolvere il contratto, fatto salvo in ogni caso, il diritto al risarcimento di tutti i danni comunque subiti.

Il verbale di verifica di conformità positiva è elemento essenziale per la presentazione della fattura da parte della Società affidataria.

3.4 LIVELLI DI SERVIZIO

Per tutta la durata contrattuale, la Società dovrà garantire i livelli di servizio per l'assistenza sistemistica, così come previsti dai Service Level Agreement ("SLA") di Hadrian, che vengono di seguito riportati.

1. Service Availability

Hosting Availability

Parameter Standard: Availability $\geq 99.00\%$

Backup procedure Weekly backup tape

Downtime due to backup None

Definitions

- "Availability" means that the dashboard of the Hadrian Platform can be accessed and used by the Customer, excluding any Permitted Unavailability.
- "Permitted Unavailability" includes Planned Outages and any unavailability due to causes beyond the reasonable control of Hadrian, including but not limited to:
 - Software, hardware, or telecommunication failures
 - Interruption or failure of digital transmission links
 - Internet slowdowns or failures
 - Failures or defaults of third-party software, vendors, or products
 - Unavailability resulting from the actions or inactions of the Customer, or a failure of the Customer's communications link or systems.
- "Planned Outages" means the period of time during which Hadrian conducts standard systems maintenance. Hadrian shall use commercially reasonable efforts to schedule Planned Outages during non-peak hours.

2. Service Level Agreements (SLAs) and Operational Targets

Vulnerability Remediation SLAs

Hadrian applies risk-based response timelines for addressing identified vulnerabilities:

- Critical vulnerabilities: patched within 24 hours
- High vulnerabilities: patched within 3 days
- Medium vulnerabilities: patched within 7 days
- Low vulnerabilities: patched within 30 days

- General patches: deployed within a maximum of 30 days from release

Disaster Recovery Target

Hadrian targets full restoration of operations within 24 hours of a disaster or outage.

This is supported by documented IT continuity plans and semi-annual tabletop and technical recovery tests.

Data Retention

Customer data is retained only while an account is active. Upon closure:

- Voluntary closures: data enters an expired state and is removed within 90 days.
- Involuntary suspensions: 30-day grace period + 30-day retention post-closure (unless legally required otherwise).

3. Support Mechanisms and Processes

Customer Communication

Clients are notified in advance of any impactful changes to services.

All changes undergo formal change management, including risk and dependency assessments.

Incident Response and Notification

- Hadrian maintains a tested and documented Incident Response Plan.
- Suspected or confirmed incidents must be reported within 24 hours.
- A preliminary investigation and severity assessment are conducted by the Information Security Manager within 48 hours.
- For Medium or High-severity incidents, a formal communications plan is initiated — including customer notification as required.
- A post-mortem analysis follows each incident to capture lessons learned.

3.5 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.

3.6 RISERVATEZZA

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



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 Consip.

4 MODALITÀ DI FATTURAZIONE E PAGAMENTO

In relazione all'oggetto del presente Capitolato, le fatture elettroniche dovranno essere prodotte secondo il tracciato allegato alle Condizioni contrattuali, nel rispetto di quanto previsto all'articolo "Fatturazione e modalità di pagamento" e all'articolo "Verifica di conformità" delle suddette Condizioni contrattuali e come dettagliato di seguito.

Con riferimento alla voce *"A - Canone Triennale per Subscription Hadrian Platform (subscription fino a 100 Assets, integrazione di piattaforme complementari, attivazione, configurazione e supporto completo)"*, riportata nella tabella del paragrafo 2, la fornitura sarà remunerata "a corpo" e la Società potrà emettere fattura in un'unica soluzione, successivamente al rilascio da parte di Consip del relativo verbale di Verifica di conformità, con esito positivo.

Con riferimento alla voce *"B – Servizi professionali di supporto"*, riportata nella tabella del paragrafo 2, ciascun intervento sarà remunerato "a consumo", secondo le stime approvate da Consip, e la Società potrà emettere fattura successivamente al rilascio da parte di Consip del relativo verbale di Verifica di conformità, con esito positivo.

Ai fini del pagamento del corrispettivo, la Società dovrà obbligatoriamente allegare alle fatture il relativo verbale di verifica conformità.

Il pagamento del corrispettivo verrà effettuato dalla Consip secondo le modalità di cui alla vigente normativa, D.Lgs n. 231/2002 e s.m.i., e in coerenza con quanto previsto dalle Condizioni contrattuali.

5 PENALI

La Committente applicherà le penali secondo le seguenti modalità:

- in caso di ritardo nell'attivazione della soluzione Hadrian, rispetto a quanto indicato al precedente paragrafo 2.1 "Piattaforma e funzioni richieste", la Committente si riserva di applicare una penale pari all'1 (uno) per mille dell'importo totale del contratto, per ogni giorno lavorativo di ritardo;
- in caso di ritardo nel completamento del singolo intervento, di cui al paragrafo 2.2 "Servizi professionali di supporto", rispetto ai tempi approvati da Consip, la Committente si riserva di applicare una penale pari all'1 (uno) per mille dell'importo totale del contratto, per ogni giorno lavorativo di ritardo.

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