“Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – Lotto 1 (ID 2296)”

PIANO DEI FABBISOGNI

Agenzia per l'Italia Digitale (AgID)

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1	Prima emissione	04/07/2025
2		

La scrivente Amministrazione:

DATI ANAGRAFICI AMMINISTRAZIONE	
Ragione sociale Amministrazione	Agenzia per l'Italia Digitale
Tipologia Amministrazione	Agenzia governativa
Indirizzo Sede Legale (Via, N° civico e CAP)	Via Liszt, 21 - 00144
Comune (Provincia)	Roma
Codice Fiscale/P.IVA	97735020584
Indirizzo mail Amministrazione	info@agid.gov.it
PEC Amministrazione	protocollo@pec.agid.gov.it
DATI ANAGRAFICI R.U.P.	
Nome	Chiara
Cognome	Basile
Telefono	3920968349
Indirizzo mail Referente Amministrazione	basile@agid.gov.it

chiede che venga realizzato quanto di seguito indicato (barrare i servizi richiesti con il presente piano dei fabbisogni):

☐ **L1.S1 - Security Operation Center - SOC** (Compilare sezione A)
☐ **L1.S2 - Next Generation Firewall - NGFW** (Compilare sezione B)
☐ **L1.S3 - Web Application Firewall - WAF** (Compilare sezione C)
X **L1.S4 - Gestione continua delle vulnerabilità di sicurezza** (Compilare sezione D)
X **L1.S5 - Threat Intelligence & Vulnerability Data Feed - TI & VDF** (Compilare sezione E)
L1.S6 - Protezione navigazione Internet e Posta elettronica - SWG e SEG (Compilare sezione F)
☐ **L1.S7 - Protezione degli end-point – EPP** (Compilare sezione G)
☐ **L1.S8 - Certificati SSL** (Compilare sezione H)
☐ **L1.S9 - Servizio di Formazione e Security awareness** (Compilare sezione I)
☐ **L1.S10 - Gestione dell'identità e l'accesso utente** (Compilare sezione L)
☐ **L1.S11 - Firma digitale remota** (Compilare sezione M)
☐ **L1.S12 - Sigillo elettronico** (Compilare sezione N)
☐ **L1.S13 - Timbro elettronico** (Compilare sezione O)
☐ **L1.S14 - Validazione temporale elettronica qualificata** (Compilare sezione P)
X **L1.S15 - Servizi specialistici** (Compilare sezione Q)

FIRMA DEL REFERENTE DELL'AMMINISTRAZIONE

NOTA: tale documento deve essere inviato a:

- RTI: TIM quale mandataria del RTI all'indirizzo PEC: *aq.sicurezzadaremoto@pec.telecomitalia.it*
- CONSIP all'indirizzo PEC: *sicurezzaremoto.2296.l1@postacert.consip.it*

Contratto finanziato dal PNRR

Il contratto esecutivo è finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC.

☐ **SI** X **NO**

Comunicazione preventiva al CVCN

☐ **SI** X **NO**

Categorizzazione degli interventi

Indicare, nel contesto del Piano Triennale di riferimento per la specifica fornitura di servizi, l'ambito di I livello e uno o più ambiti di II livello, numerandoli in ordine di prevalenza (dove 1= priorità massima)

Ambito (layer)	Obiettivi Piano Triennale
X Servizi	2 Servizi al cittadino
	3 Servizi a imprese e professionisti
	4 Servizi interni alla propria PA
	1 Servizi verso altre PA
X Dati	1 Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	☐ Aumentare la qualità dei dati e dei metadati
	☐ Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
☐ Piattaforme	☐ Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	☐ Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	☐ Incrementare e razionalizzare il numero di piattaforme per le amministrazioni
☐ Infrastrutture	☐ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	☐ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
	☐ Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
☐ Interoperabilità	☐ Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	☐ Adottare API conformi al Modello di Interoperabilità
X Sicurezza Informatica	☐ Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	1 Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

SEZIONE D - L1.S4 - Gestione Continua Delle Vulnerabilita' Di Sicurezza

Descrizione del Servizio

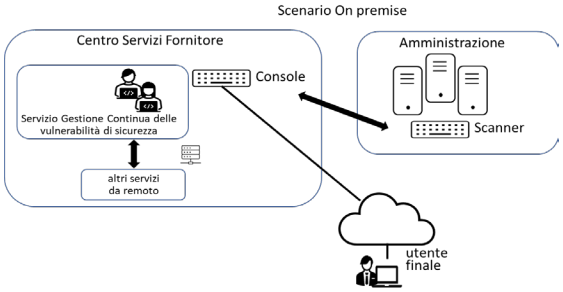
Il servizio di "Gestione continua delle vulnerabilità di sicurezza" consente alle Amministrazioni, tramite un processo automatico di assesment delle vulnerabilità, di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i propri sistemi informatici. Il servizio si avvarrà dell'utilizzo di uno scanner che produrrà un report con le specifiche indicazioni di rischio relative alle vulnerabilità rilevate.

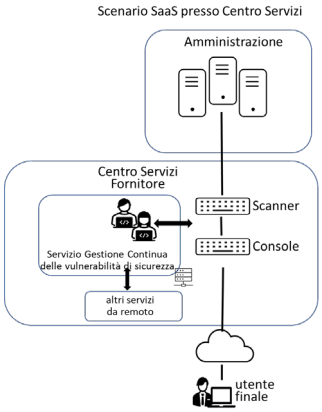
L'aumento degli attacchi informatici e i metodi sempre più sofisticati con cui vengono condotti, ha accresciuto la consapevolezza dei responsabili della sicurezza e della compliance in merito alla necessità di integrare nelle strategie di difesa strumenti e metodologie di verifica continuative. Il servizio proposto dal RTI segue le logiche della **Continuous Adaptive Risk & Trust Assessment** (**CARTA**). L'approccio adottato dal RTI per garantire la sicurezza delle infrastrutture e dei dati delle Amministrazioni promuove una valutazione continua del rischio in modo iterativo. Questa permette di monitorare i cambiamenti di stato e di reagire alla presenza di minacce o pericoli di sicurezza.

Il servizio sarà basato sulla piattaforma Tenable.sc.

L'infrastruttura di erogazione del servizio si avvale delle componenti di seguito descritte:

- Scanner – Software reso disponibile su sistema virtuale dell'Amministrazione e presente di default nel Centro Servizi, che esegue le verifiche di sicurezza sui dispositivi raggiungibili ed identificati come target, tramite comunicazioni basate su protocollo IP. La soluzione abilita le Amministrazioni a:
  - analizzare sia sistemi esposti su Internet sia sistemi interni;
  - eseguire ricerche di vulnerabilità sui propri sistemi senza soluzione di continuità.
- Console - Piattaforma centralizzata multi-tenant istanziata presso il Centro Servizi del RTI, utilizzata per la gestione del servizio. Consente la separazione logica delle PA contraenti in domini distinti (Tenant) garantendo la segregazione completa dei dati. È una singola console di management che consente di gestire dispositivi Scanner e fornire funzionalità di settings e update centralizzato per tutti gli apparati gestiti.





Modalità di erogazione:

Il modello operativo di erogazione del servizio prevede due possibili scenari architetturali di implementazione:

- installazione di appliance dedicati virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione, architettura di default proposta dal RTI in caso di IP privati;
- utilizzo di una istanza del servizio installata presso il Centro Servizi del RTI, architettura di default proposta dal RTI in caso di IP pubblici.

Metrica Servizio: Numero IP/anno

Indicare la fascia di erogazione richiesta:

Tipologia di servizio	Fasce di erogazione	Quantità (IP)
L1.S4 - Gestione continua delle vulnerabilità di sicurezza	☐ Fascia 1: fino a 50 IP	
	☐ Fascia 2: fino a 200 IP	
	☐ Fascia 3: > 200 IP	500

Modalità di remunerazione: Canone bimestrale

Durata Contrattuale: 13 mesi

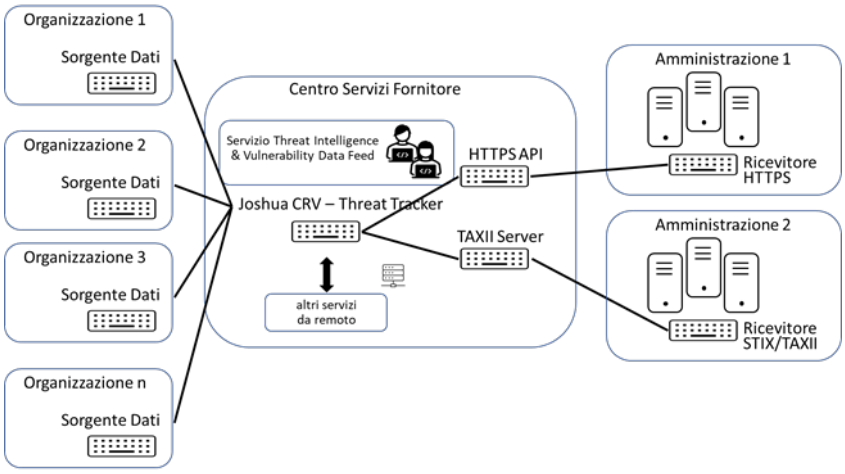
SEZIONE E - L1.S5 - Threat Intelligence & Vulnerability Data Feed (TI & VDF)

Descrizione del Servizio

Il servizio di "Threat intelligence e Vulnerability data feed" consente alle Amministrazioni di ricevere un flusso continuo di dati relativi a minacce e vulnerabilità di sicurezza del Sistema informativo permettendo così di prevedere/prevenire le minacce prima che entrino in azione, migliorando gli attuali controlli e le funzionalità forensi.

Il servizio predisposto dal RTI offre alle PA una soluzione end-to-end per definire, monitorare, analizzare e migliorare il proprio livello di sicurezza cyber complessivo secondo un approccio predittivo e di analisi di contesto, seguendo logiche cyber-intelligence driven ad ampio spettro. In aggiunta, sfruttando tecniche e strumenti di automazione, consente di definire un livello di rischio in maniera statica e di studiarne le evoluzioni nel corso del tempo, grazie ad un monitoring costante della security posture di una specifica Amministrazione. Il servizio consente di identificare e definire eventuali minacce esterne, accertare le proprie aree di vulnerabilità e i propri asset a rischio di esposizione e compromissione. Il servizio si basa su una Threat Intelligence Platform consolidata denominata Joshua CybeRisk Vision™.

Elemento distintivo del servizio è la possibilità di ottenere, tramite **Joshua**, per ogni Amministrazione, specifici IoC di **Threat Analytics** per il proprio Sistema Informativo esposto su Internet, indicazioni di **Data Breach** presenti su GitHub, Pastebin o servizi FTP e SMB, gli **Info Leak** su Twitter, gli Asset della PA pubblicamente noti mediante **Postural Assessment**, gli account della specifica PA mediante **Theft Accounts**, minacce agli utenti della PA mediante **Web Malware Detection** sui principali siti della PA. Joshua, erogato nella modalità Threat Intelligence Data Feed, coniuga la capacità di ricercare codici di autenticazione, software, e-mail, dati GDPR rilevanti, etc., sui principali siti utilizzati da sviluppatori e Threat Actor, con la capacità di correlare gli elementi con i dati dello specifico Sistema Informativo esposto su Internet di una PA, **contestualizzando il subset informativo delle minacce**. Saranno infine utilizzate **tassonomie e schemi di classificazione** ben noti per supportare la classificazione standard utilizzata da ENISA, Europol, DHS, CSIRT o molte altre organizzazioni.



Modalità di erogazione:

Il modello operativo di erogazione del servizio prevede due possibili scenari architetturali di implementazione:

- comunicazione tramite HTTPS API Gateway;
- comunicazione tramite TAXII server.

Metrica Servizio: Data-Feed/anno

Indicare la fascia di erogazione richiesta:

Tipologia di servizio	Fasce di erogazione	Quantità (Feed)
L1.S5 - Threat Intelligence & Vulnerability Data Feed (TI & VDF)	☐ Fascia 1: fino a 10 feed;	
	☐ Fascia 2: fino a 50 feed;	
	☐ Fascia 3: > 50 feed.	80

Modalità di remunerazione: Canone bimestrale

Durata Contrattuale: 13 mesi

SEZIONE Q - L1.S15 - Servizi specialistici

Descrizione del Servizio
Il servizio "Servizi specialistici" consente all'Amministrazione di richiedere un supporto tecnico connesso all'attivazione dei servizi da remoto previsti nell'AQ.

A tale riguardo AgID richiede un supporto nei seguenti ambiti:
A. Supporto alla verifica della vulnerabilità degli applicativi in gestione
B. Supporto alla gestione delle Statistiche dei dati gestiti nell'ambito del Customer Service Tecnico
C. Supporto per la manutenzione del software di gestione identità e accesso
D. Supporto per la revisione dei processi interni al CST

In tutta la durata contrattuale deve essere fornito supporto alla gestione delle attività di progetto.

Modalità di erogazione: on site e/o da remoto

Metrica Servizio: 2.218 Giorni/Persona del Team ottimale (pari a 8 ore lavorative).

Modalità di remunerazione: Progettuale (a corpo)

Durata Contrattuale: 13 mesi

SEZIONE R – Tabella Riepilogativa

Cod. Serv.	Servizio	Fascia di acquisizione	Quantità	Durata Contrattuale (Mesi)	Importo Totale del servizio [€]
L1.S1	Security Operation Center (SOC)	Fascia 1: fino a 300 EPS			
		Fascia 2: fino a 600 EPS			
		Fascia 3: fino a 1200 EPS			
		Fascia 4: fino a 6.000 EPS			
		Fascia 5: >6.000 EPS			
L1.S2	Next Generation Firewall	Fascia 1: fino a 250 Mbps			
		Fascia 2: fino a 2 Gbps			
		Fascia 3: fino a 4 Gbps			
		Fascia 4: fino a 7 Gbps			
		Fascia 5: fino a 15 Gbps			
		Fascia 6: > 15 Gbps			
L1.S3	Web Application Firewall	Fascia 1: fino a 500 Mbps			
		Fascia 2: fino a 5 Gbps			
		Fascia 3: > 5 Gbps			
L1.S4	Gestione continua delle vulnerabilità di sicurezza	Fascia 1: fino a 50 IP			
		Fascia 2: fino a 200 IP			
		Fascia 3: > 200 IP	500	13	7.817,33 €
L1.S5	Threat Intelligence & Vulnerability Data Feed	Fascia 1: fino a 10 feed			
		Fascia 2: fino a 50 feed			
		Fascia 3: > 50 feed	80	8	10.915,67 €
L1.S6	Protezione navigazione Internet e Posta elettronica	Fascia 1: fino a 1.000 Utenti			
		Fascia 2: fino a 5.000 Utenti			
		Fascia 3: fino a 10.000 Utenti			
		Fascia 4: fino a 20.000 Utenti			
		Fascia 5: >20.000 Utenti			
L1.S7	Protezione degli end-point	Fascia 1: fino a 500 Nodi			
		Fascia 2: fino a 1.000 Nodi			
		Fascia 3: fino a 5.000 Nodi			
		Fascia 4: > 5.000 Nodi			
L1.S8	Certificati SSL	Fascia 1: SSL OV			
		Fascia 2: SSL OV Wildcard			
		Fascia 3: SSL EV			
		Fascia 4: SSL DV			
		Fascia 5: SSL Code Signing			
		Fascia 6: SSL Client Auth			
L1.S9	Servizio di Formazione e Security awareness	Giorni/persona del Team Ottimale			
L1.S10	Gestione dell'identità e l'accesso utente	Fascia 1: fino a 10.000 Utenti			
		Fascia 2: fino a 100.000 Utenti			
		Fascia 3: fino a 500.000 Utenti			
		Fascia 4: > 500.000 Utenti			
L1.S11	Firma digitale remota	Fascia 1: > 50 e fino a 200 Utenti			
		Fascia 2: > 200 e fino a 500 Utenti			
		Fascia 3: > 500 e fino a 1.000 Utenti			

Cod. Serv.	Servizio	Fascia di acquisizione	Quantità	Durata Contrattuale (Mesi)	Importo Totale del servizio [€]
		Fascia 4: > 1.000 Utenti			
L1.S11	Firma digitale remota massiva [SLA GARANTITO – 1 firma/sec]	Garantita - N. 1 firma			
		Garantita - N. 5 firme aggiuntive			
L1.S12	Sigillo elettronico [SLA GARANTITO – 1 sigillo/sec]	Garantita - N. 1 sigillo			
		Garantita - N. 5 sigilli aggiuntivi			
L1.S13	Timbro elettronico	Fascia 1: fino a 1.000 Timbrature			
		Fascia 2: > 1000 e fino a 1.000 Timbrature			
		Fascia 3: > 10000 e fino a 100.000 Timbrature			
		Fascia 4: > 100.000 e fino a 1.000.000 Timbrature			
		Fascia 5: > 1.000.000 e fino a 10.000.000 Timbrature			
		Fascia 6: > 10.000.000 Timbrature			
L1.S14	Validazione temporale elettronica qualificata	Fascia 1: fino a 1.000 Marcature			
		Fascia 2: > 1.000 e fino a 10.000 Marcature			
		Fascia 3: > 10.000 e fino a 100.000 Marcature			
		Fascia 4: > 100000 e fino a 1.000.000 Marcature			
		Fascia 5: > 1.000.000 e fino a 10.000.000 Marcature			
		Fascia 6: > 10.000.000 Marcature			
	Validazione temporale elettronica qualificata [SLA GARANTITO – 1 marcatura/sec]	Garantita - N. 1 marcatura			
		Garantita - N. 1 marcatura aggiuntiva			
L1.S15	Servizi specialistici	Giorni/persona del Team Ottimale	2.218	13	521.230,00 €
				IMPORTO TOTALE CONTRATTO (IVA esclusa) =	**539.963,00 €**