Trattativa Diretta (TD) su MePA ai sensi dell'art. 50, comma 1, lett. b) del D.lgs. n. 36/2023 per garantire l'acquisizione di servizi di Cybersecurity per il CERT-AgID necessari alla sicurezza informatica dell'Agenzia per l'Italia Digitale. -

Disciplinare per il perfezionamento dell'affidamento MePA

INDICE

Art.1.CONTESTO TECNICO, OBIETTIVI ATTESI. OGGETTO, IMPORTO, DURATA, CONTENUTI DELL'AFFIDAMENTO 2

Art.2.PIATTAFORMA DI ACQUISTO. DOCUMENTAZIONE AI FINI DEL PERFEZIONAMENTO DELLA TD CON CONFRONTO PREVENTIVI SU MePA. COMUNICAZIONI. CHIARIMENTI. ACCESSO AGLI ATTI 3

2.1. ESPD (European Single Procurement Document) 4

2.2. Soccorso Istruttorio 5

2.3. Garanzia definitiva 5

Art.3 ADEMPIMENTI CONNESSI ALLA STIPULA DEL CONTRATTO E ALLA ESECUZIONE DELL'AFFIDAMENTO. 6

Art.4. PENALI E RISOLUZIONE 7

Art.5.ATTESTAZIONE/CERTIFICATI DI REGOLARE ESECUZIONE DEI SERVIZI. TERMINI E MODALITÀ DI FATTURAZIONE E PAGAMENTO 7

Art.6.OBBLIGHI DI TRACCIABILITÀ 8

Art.7.RISERVATEZZA 9

Art.8.INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI 9

Art.9.OBBLIGHI IN MATERIA DI PREVENZIONE DELLA CORRUZIONE 10

Art.10.CODICE DI COMPORTAMENTO/PATTO DI INTEGRITÀ 10

Art.11. FORO COMPETENTE 11

ALLEGATO: SPECIFICHE DI DETTAGLIO DEL PACCHETTO SERVIZI DENOMINATO "IoC Phish Leak CTI" 12

Ad integrazione di quanto disposto nelle Condizioni relative al capitolato/bando MePA di riferimento, si conviene quanto segue. Il presente documento, debitamente sottoscritto digitalmente per accettazione, anche ai sensi dell'art. 1341 c.c. per le clausole indicate in calce, va restituito alla stazione appaltante sia su MePA che alla PEC: protocollo@pec.agid.gov.it, all'attenzione del Responsabile Unico del Progetto (RUP) e Direttore dell'esecuzione (DE) e all'Ufficio Contabilità, Finanza e Funzionamento.

Art.1.CONTESTO TECNICO, OBIETTIVI ATTESI. OGGETTO, IMPORTO, DURATA, CONTENUTI DELL'AFFIDAMENTO

1.L'Agenzia per l'Italia Digitale (AgID) è il soggetto istituzionale che ha il compito di coordinare il processo di attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026, all'interno del quale una delle principali linee strategiche è costituita dalla Sicurezza informatica.

Il Piano Triennale, al punto 7.6 della Sicurezza Informatica, ha previsto che AgID metta a disposizione della Pubblica Amministrazione una serie di piattaforme e di servizi, che verranno erogati tramite il proprio CERT, finalizzati alla conoscenza e al contrasto dei rischi cyber legati al patrimonio ICT della PA. Questi servizi comprendono tra gli altri le attività di monitoraggio e identificazione delle minacce presenti sui canali underground che potrebbero interessare la constituency del CERT-AGID e, più in generale, il dominio della PA nazionale.

2.Nel caso specifico, AgID, che già svolge attività di ricerca in ambito di Cyber Threat Intelligence, Data Leak, Malware, Phishing e condivisione di Indicatori di Compromissione **(IoC Phish Leak CTI),** ha necessità di ampliare la qualità di informazioni da mettere a disposizione della PA, potenziando i servizi già svolti, sia dal punto di vista della quantità sia da quello della completezza, potendo avere accesso ad altre fonti informative complementari a quelle attuali, acquisendo i seguenti servizi di Cybersecurity per il CERT-AgID, legati ad attività di ricerca in ambito di Cyber Threat Intelligence, Data Leak, Malware, Phishing e condivisione di Indicatori di Compromissione, contenuti nel pacchetto IoC Phish Leak CTI, per un periodo di 24 mesi a decorrere dalla stipula del contratto e per l'importo complessivo massimo di € 70.000,00 IVA esclusa, pari a € 85.400,00 IVA inclusa:

Servizio	Descrizione	Durata
Phishing Monitor	Servizio per individuare il diffondersi di frodi on-line della tipologia phishing miranti a carpire dati personali, sensibili e finanziari di utenti finali o del personale in servizio presso il cliente.	24 Mesi
Brand Monitor	Monitoraggio delle diverse tecniche di typosquatting applicate ai domini istituzionali. In particolare identifica i domini di nuova registrazione aventi nomi sospetti e similari ai brand/domini del cliente che potrebbero essere impiegati per: • rivendita/cessione speculativa del nome dominio; • phishing utenza customers; • spear-phishing: phishing mirato all'organizzazione del cliente; • attacco all'immagine del cliente, con la pubblicazione di false notizie.	24 Mesi
Data Leak/Breach Monitor	Servizi di: • Data Leak Monitor: monitoraggio degli ambienti underground al fine di rilevare il rilascio di dati estrapolati da siti web di qualsiasi dimensione in cui i dipendenti si siano registrati con l'indirizzo email aziendale, con il rischio di riutilizzo sui sistemi aziendali della medesima password; • Recupero Email da Phishing: deputato a recuperare gli indirizzi email di coloro che cadono vittime di phishing a danno di qualsiasi tipologia di ente.	24 Mesi
CTI Main Core	Attività di monitoraggio dei contenuti presenti sul Web: • monitoraggio automatizzato delle piattaforme accessibili sul web emerso, attraverso connettori sviluppati ad hoc per collegare le sorgenti di informazioni alla Threat Intelligence Platform; • frequentazione dagli ambienti underground/cyber criminali, identificabili in Deep e Dark web, da parte dell'operatore del fornitore facendo uso di profili ad hoc (sock puppets) credibili.	24 Mesi
IoC Zone	Servizio finalizzato alla condivisione di indicatori di compromissione (IoC) derivanti dall'analisi statica ed in sandbox dei malware per sistemi desktop e mobili, identificati attraverso la raccolta su apposite spamtrap gestite ed attraverso i monitoraggi web svolti con automatismi e ricerche condotte da operatori.	24 Mesi

3.AgID si riserva altresì la facoltà di avvalersi delle opzioni e modifiche previste dall'art. 120 del D.lgs. 36/2023, entro la soglia prevista dall'art. 50, comma 1 lett. e), qualora ne emergesse la necessità; in tal caso, sarà cura del RUP, al momento dell'attivazione delle opzioni, allinearsi con gli Uffici competenti per la copertura di budget e con l'operatore economico.
4.Ai fini della stipula della trattativa diretta, il fornitore dovrà prestare, ai sensi dell'art. 53 comma 4 del D.lgs. n. 36/2023, una garanzia fideiussoria, come precisato anche nel prosieguo al **par. 2.3**.
5.Il Fornitore dovrà garantire per tutta la durata del servizio il necessario supporto per tutti gli aspetti operativi e svolgere le attività nel rispetto delle indicazioni e direttive del RUP.

Art.2.PIATTAFORMA DI ACQUISTO. DOCUMENTAZIONE AI FINI DEL PERFEZIONAMENTO DELLA TD CON CONFRONTO PREVENTIVI SU MePA. COMUNICAZIONI. CHIARIMENTI. ACCESSO AGLI ATTI
1.Per l'affidamento l'AgID procede tramite la piattaforma MePA, che l'OE si impegna a conoscere osservandone le relative regole.
2.Eventuali richieste di chiarimento e comunicazioni verranno svolte tramite le funzionalità della piattaforma.
3.Ove necessario sarà garantito l'accesso agli atti nel rispetto degli artt. 35 e 36 del D.lgs. n. 36/2023.
4.La documentazione per il perfezionamento dell'affidamento su MePA include:
- il presente Disciplinare per il perfezionamento dell'affidamento MePA e le fasi di esecuzione, con allegate le specifiche di dettaglio dei servizi offerti;
- il modello di Patto di integrità;
- il modello di dichiarazione di conto corrente dedicato;
- il modello per l'autodichiarazione del fornitore in ottemperanza all'art. 53, co. 16 ter, del D.Lgs. 30/03/2001 n. 165 (c.d. antipantouflage);
- il file xml dell'ESPD (European Single Procurement Document) generato dalla piattaforma.

5.Il prestatore dovrà compilare e caricare sulla piattaforma MePA:
- l'xml dell' ESPD (European Single Procurement Document);
- il Patto di integrità, secondo il template allegato, compilato e firmato da parte del legale rappresentante o da persona munita dei poteri di firma;
- il modello di dichiarazione di conto corrente dedicato, compilato e firmato, (ai sensi dell'art. 3 comma 7 della Legge 13 agosto 2010 n. 136 va inviata una dichiarazione attestante gli estremi identificativi del/i conto/i corrente bancario/i, dedicato/i anche non in via esclusiva alla presente procedura); generalità e codice fiscale delle persone delegate ad operare su detto/i conto/i, fermo l'obbligo dell'OE di comunicare al RUP/all'AgID entro e non oltre 7 (sette) giorni, qualsivoglia variazione relativa ai richiamati dati;
- il modello per l'autodichiarazione del fornitore in ottemperanza all'art. 53, co. 16 ter, del D.Lgs. 30/03/2001 n. 165 (c.d. antipantouflage), compilato e firmato da parte del legale rappresentante o da persona munita dei poteri di firma;
- l'offerta economica, dettagliata sulla base delle esigenze dell'Agenzia come elencate nell'Allegato, entro l'importo massimo spendibile;
- eventuale documentazione amministrativa di propria iniziativa;

6. Ai sensi dell'art. 5 della Delibera ANAC 262/2023, tramite l'xml dell'ESPD ai fini dei controlli previsti dalla normativa vigente e propedeutici alla stipula, l'OE autorizza l'accesso al FVOE (Fascicolo Virtuale dell'Operatore Economico) da parte della stazione appaltante o ente concedente interessato, con le funzionalità messe a disposizione dal sistema.
7.La medesima documentazione dovrà essere spedita anche alla PEC: protocollo@pec.agid.gov.it all'attenzione del RUP e all'Ufficio Contabilità, Finanza e Funzionamento.
8.Nel firmare per accettazione il presente Disciplinare si raccomanda, ai sensi e per gli effetti dell'art. 1341 c.c. di approvare specificatamente le pattuizioni contenute negli articoli indicati (art. 1 Contesto Tecnico, Obiettivi Attesi. Oggetto, importo, durata, contenuti dell'affidamento; art. 4 Penali e risoluzione; art. 5 Attestazione/certificati di regolare esecuzione dei servizi. Termini e modalità di fatturazione e pagamento; art. 11 Foro competente), apponendo apposita firma digitale.

2.1. ESPD (European Single Procurement Document)

1.L'operatore economico, in linea con le disposizioni del D.lgs. n. 36/2023 e con le indicazioni che è possibile rinvenire al link https://espd.eop.bg/espd-web/filter?lang=it, dovrà presentare il file xml dell'ESPD, successivamente verificabile, firmato dal legale rappresentante (se procuratore, allegare copia autentica della procura speciale), ai sensi degli artt. 46 e 47 del DPR n. 445/2000, che attesta:

a) di non trovarsi nelle condizioni previste nell'art. 94, comma 1, lettere a), b), c), d), e), f), g), h) comma 2, comma 3, lettere a), b), c), d), e), f), g), h), comma 4, comma 5 lettere a), b), c), d), e), f) e comma 6, del Codice (compilare, in ogni sua parte, la Parte III "Motivi di esclusione" dell'ESPD); si rappresenta che la dichiarazione sull'assenza della causa di esclusione di cui all'art. 94, comma 1 e comma 2, del Codice, dovrà essere riferita per tutti i soggetti (in carica e cessati) che rivestono le cariche di cui all'art. 94, comma 3, del Codice; nell'ESPD, parte II "Informazioni sull'operatore economico", Sezione B, tale dichiarazione dovrà essere riferita ai seguenti soggetti, ed in particolare:

- al titolare e al direttore tecnico, se si tratta di impresa individuale;
- ai soci e al direttore tecnico, se si tratta di società in nome collettivo;
- ai soci accomandatari e al direttore tecnico, se si tratta di società in accomandita semplice;
- se si tratta di altro tipo di società o consorzio:
  - ai membri del consiglio di amministrazione cui sia stata conferita la legale rappresentanza, ivi compresi institori e procuratori generali, dei membri degli organi con poteri di direzione o di vigilanza;
  - ai soggetti muniti di poteri di rappresentanza (tra questi rientrano i procuratori muniti di poteri decisionali di particolare ampiezza e riferiti ad una pluralità di oggetti così che, per sommatoria, possano configurarsi omologhi, se non di spessore superiore, a quelli che lo statuto assegna agli amministratori e gli institori ex art. 2203 cc), di direzione o di controllo;
  - al direttore tecnico;
  - al socio unico persona fisica, ovvero al socio di maggioranza in caso di società con meno di quattro soci, se si tratta di altro tipo di società o consorzio (si precisa in proposito che, nel caso di società con due soli soci persone fisiche i quali siano in possesso, ciascuno, del 50% della partecipazione azionaria, le dichiarazioni prescritte dall'art. 94, del Codice, devono essere riferite per entrambi i suddetti soci);
- ai soggetti sopra indicati cessati dalla carica nell'anno antecedente la data di indizione e comunque fino alla presentazione dell'offerta;
- in caso di incorporazione, fusione societaria o cessione d'azienda, le dichiarazioni di cui all'art. 94, commi 1, 2 e 5, del Codice, devono riferirsi anche ai soggetti di cui all'art. 94 comma 3 del Codice che hanno operato presso la società incorporata, fusasi o che ha ceduto l'azienda nell'anno antecedente la data di pubblicazione del presente affidamento.

b) l'iscrizione nel registro della Camera di commercio, industria, agricoltura e artigianato o ad altro Albo, ove previsto, capace di attestare lo svolgimento delle attività nello specifico settore, con espressa indicazione della Camera di Commercio nel cui registro delle imprese il concorrente è iscritto, degli estremi d'iscrizione (numero e data), della forma giuridica e dell'attività per la quale il concorrente è iscritto, che deve corrispondere a quella oggetto della presente procedura di affidamento (compilando l'ESPD);

c) l'assenza delle cause di incompatibilità di cui all'art. 53, comma 16-ter, del D.lgs. n. 165/2001 nei confronti della Stazione appaltante (AgID).

2.Nel caso in cui nell'ESPD siano dichiarate condanne o conflitti di interesse o fattispecie relative a risoluzioni o altre circostanze idonee ad incidere sull'integrità o affidabilità del concorrente (di cui all'art. 94, commi 1 e 5 del Codice, sulla base delle indicazioni eventualmente rese nelle Linee guida dell'ANAC) o siano state adottate misure di self cleaning, dovranno essere prodotti tutti i documenti pertinenti (ivi inclusi i provvedimenti di condanna) al fine di consentire alla Stazione appaltante (AgID) ogni opportuna valutazione.

3.L'operatore economico in linea con le disposizioni del D.lgs. n. 36/2023, dovrà ai sensi degli artt. 46 e 47 del DPR n. 445/2000, dichiarare:

a. di non incorrere nelle cause di esclusione di cui all'art. 94 del Codice;
b. di non incorrere nelle cause di esclusione di cui all'art. 94, comma 5, lett. c-bis), c- ter) e c- quater) del Codice (in caso affermativo, descrivere la situazione concreta);

c. di non incorrere nelle cause di esclusione di cui all'art. 95 del Codice;
d. i dati identificativi (nome, cognome, data e luogo di nascita, codice fiscale, comune di residenza etc.) dei soggetti di cui all'art. 94, comma 3 del Codice, ovvero indica la banca dati ufficiale o il pubblico registro da cui i medesimi possono essere ricavati in modo aggiornato alla data di presentazione dell'offerta; remunerativa l'offerta economica presentata giacché per la sua formulazione ha preso atto e tenuto conto:
    1) delle condizioni contrattuali e degli oneri compresi quelli eventuali relativi in materia di sicurezza, di assicurazione, di condizioni di lavoro e di previdenza e assistenza in vigore nel luogo di svolgimento dei servizi;
    2) di tutte le circostanze generali, particolari e locali, nessuna esclusa ed eccettuata, che possono avere influito o influire sia sulla prestazione dei servizi, sia sulla determinazione della propria offerta.

2.2. Soccorso Istruttorio

1.Le carenze di qualsiasi elemento formale della documentazione e, in particolare, la mancanza, l'incompletezza ed ogni altra irregolarità essenziale degli elementi, dell'ESPD e delle restanti dichiarazioni sostitutive, con esclusione di quelle afferenti all'offerta tecnica ed economica, ove presenti, potranno essere sanate attraverso la procedura di soccorso istruttorio di cui all'art. 101, del Codice.
2.Costituiscono irregolarità essenziali non sanabili le carenze della documentazione che non consentono l'individuazione del contenuto o del soggetto responsabile della stessa.
3.L'irregolarità essenziale è sanabile laddove non si accompagni ad una carenza sostanziale del requisito alla cui dimostrazione la documentazione omessa o irregolarmente prodotta era finalizzata.
4.La successiva correzione o integrazione documentale è ammessa laddove consenta di attestare l'esistenza di circostanze preesistenti, vale a dire requisiti previsti per la partecipazione e documenti/elementi a corredo dell'offerta. Nello specifico valgono le seguenti regole:
a) il mancato possesso dei prescritti requisiti di partecipazione non è sanabile mediante soccorso istruttorio e determina l'esclusione dalla procedura di gara;
b) l'omessa o incompleta nonché irregolare presentazione delle dichiarazioni sul possesso dei requisiti di partecipazione e ogni altra mancanza, incompletezza o irregolarità dell'ESPD e della domanda, ivi compreso il difetto di sottoscrizione, sono sanabili, ad eccezione delle false dichiarazioni;
c) la mancata presentazione di condizioni di partecipazione gara (es. mandato collettivo speciale o impegno a conferire mandato collettivo), aventi rilevanza in fase di gara, sono sanabili, solo se preesistenti e comprovabili con documenti di data certa, anteriore al termine di presentazione dell'offerta;
d) la mancata presentazione di dichiarazioni e/o elementi a corredo dell'offerta, che hanno rilevanza in fase esecutiva (es. dichiarazione delle parti del servizio o della fornitura ai sensi dell'art.68, comma 2 del Codice) sono sanabili.
5.Ai fini della sanatoria, si assegnerà al concorrente un termine di 10 (dieci) giorni perché siano rese, integrate o regolarizzate le dichiarazioni necessarie, indicandone il contenuto e i soggetti che le devono rendere. Nel medesimo termine il concorrente è tenuto a comunicare alla stazione appaltante l'eventuale volontà di non avvalersi del soccorso istruttorio. Ove il concorrente produca dichiarazioni o documenti non perfettamente coerenti con la richiesta, la stazione appaltante può chiedere ulteriori precisazioni o chiarimenti, fissando un termine perentorio a pena di esclusione. In caso di comunicazione del concorrente della volontà di non avvalersi del soccorso istruttorio e, comunque, in caso di inutile decorso del termine, la stazione appaltante procede all'esclusione del concorrente dalla procedura di gara.
6.Al di fuori delle ipotesi di cui all'articolo 101, del Codice è facoltà della stazione appaltante invitare, se necessario, i concorrenti a fornire chiarimenti in ordine al contenuto dei certificati, documenti e dichiarazioni presentati.

2.3. Garanzia definitiva

1.Ai fini della stipula della trattativa diretta su MePA, il fornitore dovrà prestare, una garanzia fideiussoria ai sensi dell'art. 53, comma 4 del D.lgs. 36/2023, da rilasciare con le modalità indicate nel codice.

2.La garanzia deve contenere la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, comma 2, del codice civile, l'operatività della garanzia medesima - anche per il recupero delle penali contrattuali - entro quindici giorni, a semplice richiesta scritta della Amministrazione contraente.
3.Deve essere munita, in deroga all'art. 1945 del codice civile, della clausola "a prima richiesta" con espressa rinuncia, altresì, alla preventiva escussione del debitore principale di cui all'art. 1944 del codice civile.
4.Al fine di fruire del beneficio della riduzione previsto dall'art. 106, comma 8 del D.lgs. n. 36/2023, il Fornitore deve produrre, anche in copia conforme all'originale, mediante idonea dichiarazione resa ai sensi dell'art. 47del D.P.R. 445/2000, la certificazione di qualità conforme alle norme europee UNI CEI ISO 9000; ovvero rientrare in tutte le altre ipotesi indicate nel codice dei contratti.
5. Si precisa che:

- in caso di partecipazione in R.T.I. e/o Consorzio ordinario di cui all'art. 65, comma 2, lett. e) del D.lgs. 36/2023, il Fornitore può godere del beneficio della riduzione della garanzia solo se tutte le imprese che lo costituiscono siano in possesso della predetta certificazione, attestata da ciascuna impresa secondo le modalità sopra previste;
- in caso di partecipazione in Consorzio di cui alle lettere b), c) e d) dell'art. 65, comma 2, del D.lgs.36/2023, il Fornitore può godere del beneficio della riduzione della garanzia solo se il Consorzio è in possesso della predetta certificazione.

6.Qualora l'ammontare delle garanzie dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, l'affidatario dovrà provvedere al reintegro entro il termine di 30 (trenta) giorni lavorativi dal ricevimento della relativa richiesta. In caso di inadempimento al reintegro, la Stazione Appaltante ha facoltà di dichiarare risolto il contratto, fermo restando il risarcimento del danno.
7.La mancata costituzione della garanzia definitiva determina l'impossibilità di stipulare e la decadenza dall'affidamento. La cauzione copre gli oneri per il mancato od inesatto adempimento dell'appalto e cessa di avere effetto a completa ed esatta esecuzione delle obbligazioni nascenti dallo stesso.
8.Si ricorda che la garanzia è progressivamente svincolata in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80% dell'iniziale importo garantito secondo quanto stabilito all'art. 117, comma 8, D.lgs. 36/2023.

Art.3 ADEMPIMENTI CONNESSI ALLA STIPULA DEL CONTRATTO E ALLA ESECUZIONE DELL'AFFIDAMENTO.

1.A seguito dell'affidamento sulla piattaforma elettronica, si richiede, come in parte già chiarito, di far pervenire all'indirizzo PEC: protocollo@pec.agid.gov.it, all'attenzione del RUP e del Direttore dell'esecuzione e all'Ufficio Contabilità, Finanza e Funzionamento entro il termine di 10 (dieci) giorni naturali e consecutivi la prova del pagamento dell'imposta di bollo che l'appaltatore è tenuto a versare al momento della stipula del contratto secondo l'articolo 1, comma 1, dell'allegato I.4 al d.lgs. n. 36/2023. I contratti stipulati con la Pubblica Amministrazione attraverso il Mercato Elettronico della PA scontano l'imposta di bollo, in linea anche con la risoluzione n. 37/E del 28 giugno 2023 dell'Agenzia delle Entrate.
2.Le modalità di versamento utilizzabili per assolvere l'imposta di bollo sui contratti pubblici, così come rideterminata nel valore, in funzione delle fasce di importo del contratto, dalla tabella A dell'articolo 3 del citato Allegato I.4, prevedendo l'utilizzo del diffuso sistema di pagamento F24. Tale strumento è idoneo a consentire, da un lato, il versamento in via telematica attraverso gli appositi servizi messi a disposizione dall'Agenzia delle entrate, dalle banche e dagli altri prestatori di servizio di pagamento e, dall'altro, mediante utilizzo dello specifico modello "F24 ELIDE", ad assicurare la possibilità di un'univoca associazione del versamento stesso con il contratto soggetto ad imposta, mediante la valorizzazione del campo elementi identificativi (con l'indicazione del CIG o di altro identificativo univoco).
3.Il RUP principalmente e nel rispetto delle norme vigenti:

- cura il corretto e razionale svolgimento della procedura su MePA, esercitando una funzione di coordinamento e controllo anche sulla documentazione da inviare tramite piattaforma (e coordinandosi con il punto ordinante e i servizi competenti) adottando decisioni conseguenti alle valutazioni effettuate;
- verifica, ove lo ritenga necessario anche con il supporto degli uffici competenti, il possesso dei requisiti previsti dal Codice e dalle altre disposizioni vigenti in capo all'aggiudicatario e il costante mantenimento dei

requisiti e adempimenti essenziali a garantire il rispetto della normativa in tema di GDPR e la sicurezza informatica;
- richiede al punto ordinante di procedere attraverso le funzionalità del MePA alla stipula del contratto (se vi sono urgenze di avvio del servizio, anche una volta avviate le verifiche di cui al precedente punto);
- comunica al Prestatore e agli Uffici competenti, anche ai fini degli adempimenti legati alla normativa in materia di trasparenza e avvio della fase di gestione, controllo, esecuzione, pagamento dei servizi resi in forza del contratto, la data di avvio delle attività;
- rilascia l'Attestazione di regolare esecuzione (ARE)/il certificato di pagamento, entro i termini previsti e lo invia all'OE e all'ufficio competente, ai fini dell'autorizzazione alla fatturazione e per il pagamento, previa ricezione della fattura, coerente con l'ARE.

Art.4. PENALI E RISOLUZIONE

1.In caso di ritardo rispetto ai termini indicati dal RUP e in caso di inadempimento nell'erogazione dei servizi richiesti per assicurare tutti i servizi previsti dal contratto, per ogni difetto contestato formalmente, anche via mail, il RUP si riserva di applicare una penale del'1‰ dell'importo contrattuale per ogni giorno solare di ritardo e per ogni inadempienza contestata.
2.L'ammontare della penale sarà detratto dal corrispettivo dovuto, salvo che il danno sia così grave da preludere alla risoluzione del contratto.
3.Le penali saranno applicabili fino ad un massimo del 10% (dieci per cento) dell'importo contrattuale.
4.Oltre tale limite, l'Agenzia si riserva la facoltà di risolvere il rapporto mediante PEC, senza bisogno di messa in mora o di azione giudiziaria, con rivalsa nei confronti della contraente anche dell'eventuale maggior onere rispetto alle condizioni economiche di cui alla presente procedura, salvo le richieste di risarcimento dei danni subiti.
5.Il protrarsi dell' inadempimento del contratto, costituisce condizione risolutiva espressa, ai sensi dell'art. 1456 cc., senza che l'inadempiente abbia nulla a pretendere, e fatta salva l'esecuzione in danno con facoltà dell'Agenzia di risolvere il rapporto mediante PEC, senza bisogno di messa in mora o di azione giudiziaria, con rivalsa nei confronti della contraente anche dell'eventuale maggior onere rispetto alle condizioni economiche di cui alla presente procedura e salvo le richieste di risarcimento dei danni subiti.
6.Resta in ogni caso salva la facoltà per l'AgID di richiedere il risarcimento di eventuali danni subiti a seguito di inadempienze verificatesi nel periodo di erogazione del servizio/fornitura.
7.Qualora nell'arco della durata del contratto dovessero registrarsi inadempienze con frequenza ritenuta eccessiva dall'Agenzia, quest'ultima potrà in ogni momento, a proprio insindacabile giudizio, considerare risolto di diritto il contratto, in danno e per colpa del Prestatore, ovvero acquisendo anche i prodotti in danno dell'OE da altro fornitore, ferma restando la facoltà dell'Agenzia stessa di richiedere danni diretti e indiretti derivanti dalla risoluzione.
8.L'Agenzia, inoltre, procederà alla risoluzione del contratto, in danno e colpa del Prestatore, in caso di:
- frode o grave negligenza nell'esecuzione degli obblighi e delle condizioni contrattuali;
- circostanze, determinatesi per colpa del Prestatore, tali da rendere impossibile la prosecuzione dei rapporti fra le parti;
- cessione contratto, cessazione attività, concordato preventivo, fallimento.

Art.5.ATTESTAZIONE/CERTIFICATI DI REGOLARE ESECUZIONE DEI SERVIZI. TERMINI E MODALITÀ DI FATTURAZIONE E PAGAMENTO.

1.Il servizio e quanto richiesto al Prestatore entro i termini indicati, saranno oggetto di verifica di conformità e funzionalità da parte del RUP. L'importo sarà liquidato solo a seguito dell'attestazione di regolare esecuzione del RUP e previa verifica di conformità positiva del servizio di Cybersecurity.
2.Il pagamento dell'importo è in ogni caso subordinato alla stipula del contratto e sarà effettuato entro 30 (trenta) giorni dalla data di presentazione della fattura. La fattura potrà essere emessa solo successivamente all'attestazione di regolare esecuzione del RUP
3.La fattura pervenuta prima dell'attestazione di regolare esecuzione è passibile di rifiuto da parte dell'AgID.

4.Il Prestatore dovrà produrre esclusivamente fatture elettroniche, in ottemperanza a quanto previsto dal D.M. n. 55 del 3 aprile 2013, così come integrato dal Decreto del 24 agosto 2020, n. 132 del Ministero dell'Economia e delle Finanze, inerente al "*Regolamento recante individuazione delle cause che possono consentire il rifiuto delle fatture elettroniche da parte* delle *amministrazioni pubbliche. (20G00148) (GU n.262 del 22-10-2020)*".
5.L'AgID sarà costretta a procedere al rifiuto delle fatture:

a) riferite ad una operazione che non è stata posta in essere in favore del soggetto destinatario della trasmissione;
b) in caso di omessa o errata indicazione del Codice identificativo di Gara (CIG) o del Codice unico di Progetto (CUP), da riportare in fattura ai sensi dell'articolo 25, comma 2, del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89;
c) che non rispettino le norme del codice in tema di verifica di conformità e contenuti e non consentano la comprensione del contratto o progetto cui si riferiscono.

6.Sono elementi essenziali della fattura ai fini dei precedenti punti a), b) e c) i seguenti:

- Denominazione Ente: Agenzia per l'Italia Digitale;
- Codice Univoco Ufficio: F7VRDL;
- C.F.: 97735020584;
- i riferimenti (protocollo e data) della lettera contratto di affidamento del servizio e/o della fornitura e alla determinazione a contrarre e di copertura di budget;
- il CIG (Codice Identificativo Gara), in base all'art 25 comma 2 del D.L. n. 66/2014 (convertito dalla L. 23 giugno 2014, n. 89);
- i riferimenti al progetto e al CUP se presenti;
- la descrizione del servizio o della fornitura cui la fattura fa riferimento;
- la "competenza temporale del servizio", l'anno cui si riferisce il costo del servizio/fornitura (es. dal gg/mm/aa …… al gg/mm/aa….); ovvero il periodo (gg.mm.aa.) di erogazione del servizio/di effettuazione della fornitura, nonché tutti gli elementi utili alla comprensione degli importi unitari e totali che hanno condotto all'importo fatturato (limitando il più possibile il ricorso a documenti collegati);
- tutti gli elementi utili alla comprensione degli importi unitari e totali che hanno condotto all'importo fatturato (limitando il più possibile il ricorso a documenti collegati);
- eventuale titolo di non imponibilità o esenzione IVA;
- l'indicazione dello split payment;
- l'esposizione in fattura delle ritenute dello 0,50% di cui all'art. 11, comma 6 del D.lgs. n. 36/2023.

Split payment: Come detto, AgID, ai sensi del D.L. n. 50/2017 del 24/04/2017 "*Disposizioni urgenti in materia finanziaria, iniziative a favore degli enti territoriali, ulteriori interventi per le zone colpite da eventi sismici e misure per lo sviluppo*", è compresa nella platea dei destinatari del meccanismo della scissione dei pagamenti (split payment) previsto dall'articolo 1, comma. 629, lettera b), della legge 23 dicembre 2014, n. 190. L'Agenzia provvederà a versare direttamente all'Erario l'IVA addebitata in fattura, pagando al fornitore esclusivamente l'imponibile. La fattura elettronica, nella sezione "Dati di riepilogo per aliquota IVA e natura" dovrà contenere, alla voce: "Esigibilità IVA" l'indicazione: "S (scissione dei pagamenti)". Fatture non conformi a quanto indicato sono passibili di rifiuto tramite lo SDI (Sistema di Interscambio) dell'Agenzia delle Entrate.

Art.6.OBBLIGHI DI TRACCIABILITÀ

1.Il Fornitore assume gli obblighi di tracciabilità dei flussi finanziari di cui alla legge 13 agosto 2010, n. 136 e ss.mm. e ii., "Piano straordinario contro le mafie". Pertanto lo stesso deve comunicare all'Agenzia gli estremi identificativi dei conti correnti bancari o postali dedicati; la comunicazione deve essere effettuata entro sette giorni dall'accensione del conto corrente ovvero, nel caso di conti correnti già esistenti, dalla loro prima utilizzazione in operazioni finanziarie relative ad una commessa pubblica. In caso di persone giuridiche, la comunicazione de quo deve essere sottoscritta da un legale rappresentante ovvero da un soggetto munito di apposita procura.
2.L'omessa, tardiva o incompleta comunicazione degli elementi informativi comporta, a carico del soggetto inadempiente, l'applicazione di una sanzione amministrativa pecuniaria.

3.Il mancato adempimento agli obblighi previsti per la tracciabilità dei flussi finanziari relativi all'appalto comporta la risoluzione di diritto del contratto. In occasione di ogni pagamento all'appaltatore o di interventi di controllo ulteriori si procede alla verifica dell'assolvimento degli obblighi relativi alla tracciabilità dei flussi finanziari.
4.Il contratto è sottoposto alla condizione risolutiva in tutti i casi in cui le transazioni siano state eseguite senza avvalersi di banche o di Società Poste Italiane S.p.A. o anche senza strumenti diversi dal bonifico bancario o postale che siano idonei a garantire la piena tracciabilità delle operazioni per il corrispettivo dovuto in dipendenza del presente contratto.

Art.7.RISERVATEZZA

Il Fornitore si impegna formalmente a dare istruzioni al proprio personale affinché tutti i dati e le informazioni patrimoniali, statistiche, anagrafiche e/o di qualunque altro genere di cui verrà a conoscenza in conseguenza dei servizi resi, vengano considerati riservati e come tali trattati, pur assicurando nel contempo la trasparenza delle attività svolte.

Art.8.INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

1.Con il presente articolo, si informa il personale dell'OE in merito al trattamento dei dati personali durante la fase procedurale e, in caso di affidamento, altresì durante la successiva fase di vigenza contrattuale. L'OE, in persona del proprio legale rappresentante, si impegna a fornire tale informativa al personale di cui saranno trattati i dati personali.
2.Qualora, ai fini della valutazione delle competenze, l'OE ritenga di inoltrare il curriculum vitae di propri dipendenti o collaboratori, tali curricula dovranno essere corredati della dichiarazione del sottoscrittore di autorizzazione al trattamento dei dati personali a sensi della normativa vigente e per le finalità di cui alla presente procedura.
3.Ai sensi del Regolamento (UE) 2016/679, si informa come segue:

- *Titolare del trattamento dei dati personali*: Agenzia per l'Italia Digitale (AgID), corrente in Roma, via Liszt n. 21, PEC: protocollo@pec.agid.gov.it.

- *Contatti del Responsabile della protezione dei dati personali*: Roma, via Liszt n. 21, e-mail: responsabileprotezionedati@agid.gov.it.

- *Autorità di controllo:* Garante per la protezione dei dati personali: https://www.garanteprivacy.it.

- *Categorie e fonti dei dati personali: i* dati personali acquisiti da AgID ineriscono unicamente informazioni anagrafiche e di contatto di persone fisiche che ricoprono cariche all'interno della società che partecipa alla procedura e che, eventualmente, risulterà affidataria del servizio o di referenti da questi nominati. Oltre a tali dati, possono essere trattati altresì dati personali di tipo giudiziario, all'unico fine di verificare la veridicità di quanto asserito dall'interessato ai fini del perfezionamento del vincolo contrattuale.

- *Finalità e base giuridica del trattamento dei dati:* i dati personali sono trattati per consentire la partecipazione alla procedura di affidamento e, successivamente, per gestire il conseguente vincolo contrattuale. Il conferimento dei dati richiesti è obbligatorio e il mancato conferimento non consentirà l'utile partecipazione alla procedura di affidamento. La base giuridica del trattamento è individuata nell'esecuzione di misure precontrattuali e, successivamente, contrattuali nonché nell'adempimento degli obblighi legali posti in capo ad AgID.

- *Categorie di destinatari dei dati*: AgID tratterà autonomamente i dati personali mediante il proprio personale incaricato e i propri fornitori di servizi tecnici e/o telematici e attraverso il portale MePA. I destinatari dei dati personali, qualora richiesto dalla normativa vigente, sono nominati responsabili del trattamento. AgID non trasferisce i dati personali a Paesi terzi né a organizzazioni internazionali.

- *Periodo di conservazione dei dati personali:*
  a) fase di definizione e procedura di affidamento: i dati personali sono conservati sino al termine della procedura di affidamento e, in seguito, per il periodo previsto dalla normativa vigente;
  b) fase successiva all'affidamento: i dati personali sono conservati sino al termine del periodo di vigenza contrattuale e, successivamente, per il periodo previsto dalla normativa vigente.

- *Diritti degli interessati*: gli interessati hanno il diritto di ottenere da AgID l'accesso ai propri dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento, il diritto di opporsi allo stesso e la portabilità dei propri dati personali, laddove ne ricorrano i presupposti.

Le richieste vanno rivolte ad AgID, anche mediante il responsabile della protezione dei dati personali ai contatti sopra indicati. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, è diritto degli interessati proporre reclamo al Garante per la protezione dei dati personali. AgID garantisce che non è prevista alcuna forma di processo decisionale automatizzato che comporti effetti giuridici sull'interessato.

Art.9.OBBLIGHI IN MATERIA DI PREVENZIONE DELLA CORRUZIONE

1.AgID informa la propria attività contrattuale secondo i contenuti di cui al Codice di Comportamento approvato con Determinazione del Direttore Generale n. 21 del 30 gennaio 2015 (aggiornata con la DT DG 26 del 31 gennaio 2024) quale dichiarazione dei valori, insieme dei diritti, dei doveri e delle responsabilità, nei confronti dei portatori di interesse (dipendenti, fornitori, utenti, ecc.), in ottemperanza a quanto previsto dall'art. 54 del D.lgs. n. 165/2001 così come sostituito dall'art. 1, comma 44 della L. 190/2012 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica Amministrazione", documento che integra e specifica il Codice di Comportamento dei dipendenti pubblici di cui al DPR n. 62/2013.

2.Le norme contenute nel Codice si applicano, per quanto compatibili, ai titolari di contratti di consulenza o collaborazione a qualsiasi titolo, anche professionale, ai titolari di organi e di incarichi negli uffici di diretta collaborazione dei vertici politici dell'amministrazione, nonché ai collaboratori a qualsiasi titolo, anche professionale, di imprese fornitrici di servizi in favore dell'Agenzia.

3.Tutti i fornitori, quali soggetti terzi sono tenuti nei rapporti con AgID, ad uniformare la loro condotta ai criteri fondati sugli aspetti etici della gestione dei contratti definiti nel Codice di Comportamento, tenendo presente che la violazione dello stesso comporterà la risoluzione di diritto del rapporto contrattuale in essere, nonché il pieno diritto di AgID di chiedere ed ottenere il risarcimento dei danni patiti per la lesione della sua immagine ed onorabilità.

Art.10.CODICE DI COMPORTAMENTO/PATTO DI INTEGRITÀ

1.I Fornitori, partecipanti e aggiudicatario, dovranno attenersi al D.P.R. 16 aprile 2013, n. 62 (Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del D.lgs. n. 30 marzo 2001, n. 165), come modificato dal D.P.R. 13 giugno 2023, n. 81, in particolare dall'art. 2, co.3, alla cui stregua le PP.AA estendono gli obblighi di condotta previsti dal codice di comportamento anche nei confronti di imprese fornitrici di beni e servizi.

2.Nel caso di violazione degli obblighi derivante dal citato codice e sue ss.mm.ii, AgID potrà procedere alla risoluzione o decadenza del rapporto contrattuale. Il Fornitore affidatario dei servizi accetta inoltre sin d'ora quanto disposto nel PNA ANAC vigente e dai seguenti Piani e Determinazioni: il Piano Integrato di attività e organizzazione (PIAO) 2024 – 2026, adottato con la DT DG n. 28/2024 del 31 gennaio 2024; la DT DG n. 26/2024 del 31 gennaio 2024 di "Aggiornamento del Piano Triennale per la Prevenzione della Corruzione e della Trasparenza (PTPCT) 2024-2026.

3.In seguito alla comunicazione di affidamento e prima della stipula del contratto, l'aggiudicatario ha l'onere di prendere visione dei predetti documenti sul sito dell'Agenzia.

4.Il Fornitore affidatario dei servizi si impegna a sottoscrivere e rispettare, infine, il Patto di integrità sottoposto da Consip e firmato in sede di abilitazione al Mercato Elettronico, nonché il Patto di integrità AgID di cui al relativo allegato.

Art.11. FORO COMPETENTE

Per tutte le controversie relative alla validità, interpretazione ed esecuzione delle clausole contrattuali e del presente documento integrativo è competente in via esclusiva il Foro di Roma.

Letto, approvato e sottoscritto

(per il Fornitore)

Ai sensi e per gli effetti dell'art. 1341 c.c. il Fornitore dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti:

Art.1 CONTESTO TECNICO, OBIETTIVI ATTESI. OGGETTO, IMPORTO, DURATA, CONTENUTI DELL'AFFIDAMENTO;

Art.4. PENALI E RISOLUZIONE;

Art.5 ATTESTAZIONE/CERTIFICATI DI REGOLARE ESECUZIONE DEI SERVIZI. TERMINI E MODALITÀ DI FATTURAZIONE E PAGAMENTO;

Art.11 FORO COMPETENTE.

(per il Fornitore)

ALLEGATO: SPECIFICHE DI DETTAGLIO DEL PACCHETTO SERVIZI DENOMINATO "IoC Phish Leak CTI"

I servizi contenuti nel pacchetto denominato "IoC Phish Leak CTI" sono:

1. Phishing Monitor;
2. Brand Monitor;
3. Data Leak/Breach Monitor
4. CTI Main Core;
5. IoC Zone;

PHISHING MONITORING

Il servizio anti-phishing deve individuare il diffondersi di frodi on-line della tipologia phishing miranti a carpire dati personali, sensibili e finanziari di utenti finali/clienti del Cliente o del personale in servizio presso il Cliente.

L'attività di monitoraggio è volta alla tempestiva individuazione dei soggetti, intesi quali computer, server e siti, coinvolti negli attacchi di phishing.

Tale attività dovrà essere svolta attraverso il monitoraggio, automatizzato e non, di:

- Messaggi di posta elettronica ricevuti su caselle di posta elettronica (spamtrap);
- Database di segnalazioni on-line;
- Monitoraggio attivo mediante l'analisi di altre segnalazioni;
- Monitoraggio di Social Network;
- Passive DNS;
- Phishing Feed gratuiti ed a pagamento;
- Monitoraggio dei social network

Il monitoraggio genererà un feed di informazioni risultante quale input del sistema di AI, elaborati internamente e deputati alla detection.

Gli alert generati in tale fase dovranno essere successivamente esaminati dall'operatore al fine di:

- evitare falsi positivi;
- fornire al Cliente le informazioni necessarie per procedere in proprio con azioni di take down ed alle eventuali denunce/querele.

Il servizio risponde alle caratteristiche nel seguito elencate:

A. Svolto secondo le modalità sopra descritte;
B. Perimetro: domini e brand definiti in fase di contrattazione con il Cliente;
C. Modalità flat, senza limite al numero di segnalazioni;
D. Accessibilità ai dati: notifica via email, consultazione attraverso portale clienti e/o attraverso API;
E. Copertura temporale: h24 e 7/7 gg;
F. Periodo di erogazione: 36 mesi;
G. Azioni di contrasto non previste.

BRAND MONITOR

Monitoraggio delle diverse tecniche di typosquatting applicate ai domini istituzionali.

L'attività di Brand Monitor è deputata all'identificazione di domini di nuova registrazione aventi nomi sospetti e similari ai brand/domini del Cliente.

Il monitoraggio consta delle seguenti fasi:

- Detection automatizzata: attraverso servizi di appoggio e funzionalità sviluppate in proprio, per eseguire l'analisi di liste di nuovi domini al fine di identificare quelli con nomi palesemente simili al brand del Cliente. I servizi in uso dovranno permettere il monitoraggio dei più diffusi TLD dati con un ritardo di uno o due giorni, dipendentemente dalle tempistiche di diffusione degli stessi dai NIC di competenza o dalla distribuzione gerarchica dei DNS.
- Analisi svolta dall'operatore finalizzata ad escludere falsi positivi e a valutare la natura del dominio sospetto e del possibile impiego malevolo;

- Comunicazione: il dominio rilevato viene tempestivamente comunicato al Cliente affinché possa essere:
  - inserito nelle block list dei sistemi periferici al fine di bloccare email fraudolente dagli stessi inviate a danno della struttura aziendale;
  - Valutate possibili azioni di contrasto quali richieste take down, dispute dominio, ecc.
- Verifica periodica: in caso i domini non presentino grafica, loghi, marchi del Cliente gli stessi vengono mantenuti in monitoraggio e verificati ogni 6 ore.

Il servizio in oggetto risulta quindi idoneo a tutelare le aziende dalle azioni di phishing mirato, nelle quali i criminali fingendosi soggetti facente parte dell'organico aziendale scrivono a personale della società target facendo uso di indirizzi di posta elettronica con domini similari a quello del target al fine di richiedere l'emissione di pagamenti o inoculare software malevoli.
In un'ottica di difesa preventiva i domini individuati e ritenuti sospetti possono quindi essere inseriti nelle black list di firewall ed anti-spam affinché le mail fraudolente provenienti da essi non raggiungano mai il personale dell'organizzazione.

Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Perimetro: domini e brand definiti in fase in contrattazione con il Cliente;
C. Modalità flat, senza limite al numero di segnalazioni;
D. Accessibilità ai dati: notifica via email, consultazione attraverso portale clienti;
E. Copertura temporale: h24 e 7/7 gg;
F. Periodo di erogazione: 36 mesi;
G. Azioni di contrasto non previste.

DATA LEAK MONITOR
Segnalazione utenze / account mail compromesse relativamente dipendenti del Cliente.
L'attività è realizzata attraverso i servizi:

- Data Leak Monitor: deputato al monitoraggio degli ambienti underground al fine di rilevare il rilascio di dati estrapolati da siti web di qualsiasi dimensione in cui i dipendenti si siano registrati con l'indirizzo email aziendale, con il rischio di riutilizzo sui sistemi aziendali della medesima password;
- Recupero Email da Phishing: deputato a recuperare gli indirizzi email di coloro che cadono vittime di phishing a danno di qualsiasi tipologia di ente.

L'attività è tuttavia limitata all'acquisizione dei contenuti liberamente scaricabili. Il personale dell'Operatore Economico non dovrà opere l'acquisto di informazioni/dati messi in vendita in quanto:

- Eticamente discutibile, in quanto si favorisce il proliferare della attività criminali;
- Si configura il reato di ricettazione Art 648 C.P.;
- Tali spese non sono deducibili dalle imposte e necessiterebbero di fondi ad hoc non permessi dalla normativa vigente

Il servizio non si basa sulla consultazione limitata di servizi di terze parti, quali: Have I Been Pwned, How Safe Is Your Password? | BreachAlarm, etc, ma sull'effettiva ricerca, acquisizione ed analisi dei dati originali costituenti il dump.
Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Perimetro: domini e brand definiti in fase in contrattazione con il Cliente;
C. Modalità flat, senza limite al numero di segnalazioni;
D. Accessibilità ai dati: notifica via email, consultazione attraverso portale clienti, report pdf via email garantendo la confidenzialità delle informazioni;
E. Copertura temporale: h24 e 7/7 gg;
F. Periodo di erogazione: 36 mesi;

CTI MAIN CORE

L'attività di monitoraggio dei contenuti presenti sul Web nei sui diversi livelli di profondità, emerso, Deep e Dark, è svolta:

- attraverso il monitoraggio automatizzato delle piattaforme accessibili sul web emerso, attraverso connettori sviluppati ad hoc per collegare le sorgenti di informazioni alla Threat Intelligence Platform;
- la frequentazione dagli ambienti underground/cyber criminali, identificabili in Deep e Dark web, da parte dell'operatore facendo uso di profili ad hoc (sock puppets) credibili.

A seguito degli alert generati dalla TIP o dalla frequentazione in prima persona degli ambiti underground, il team di analisti esaminerà l'evidenza per determinare la sussistenza di una effettiva minaccia, nel qual caso sarà elaborato un report per il Cliente ed in caso di minaccia imminente o di elevata rilevanza si avrà un'immediata comunicazione di allerta verso il team sicurezza del committente.
Il servizio prevede inoltre l'erogazione di un report settimanale finalizzato a fornire una più completa informazione riguardo a notizie che hanno meritato l'attenzione di media generalisti e pubblicazioni del settore IT pubblica settimanalmente un approfondimento di Cyber Threat Intelligence che, in formato narrativo/discorsivo e con l'ausilio di grafici, riepiloga ogni inizio settimana gli eventi della settimana precedente.

Il report racconta complessivamente ciò che il team di analisti ha individuato e analizzato la settimana precedente, come le principali campagne di phishing, le principali campagne malware, i principali data leak e aziende compromesse da attacchi ransomware o che hanno subito attacchi DDoS ma altresì narra anche di eventi nazionali e internazionali attinenti alla Cyber Threat Intelligence.
Infine riepiloga i CVE maggiormente impattanti recentemente identificati.

Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Copertura temporale: h24 e 7/7 gg;
C. Periodo di erogazione: 36 mesi;
D. Perimetro: domini e brand definiti in fase in contrattazione con il Cliente;
E. Si richiede scambio informativo relativo ad antagonisti o elementi avversi già noti;
F. Accessibilità ai dati: consultazione attraverso portale clienti, report pdf via email garantendo la confidenzialità delle informazioni;
G. Le evidenze sono notificate al Cliente via report in formato pdf:

- Report di livello "non classificato" sono:
  - inviati via email senza protezione alcuna
  - resi disponibili attraverso il portale clienti dedicato
- Report di livello "confidenziale", "riservato" e "segreto" sono inviati via:
  - file protetto da password (pdf/zip/rar);
  - resi disponibili attraverso il portale clienti dedicato.

IOC ZONE - CONDIVISIONE INDICATORI DI COMPROMISSIONE

Il servizio è finalizzato alla condivisione di indicatori di compromissione (IoC) derivanti dall'analisi statica ed in sandbox dei malware per sistemi desktop e mobili, identificati attraverso la raccolta su apposite spamtrap gestite dall'operatore attraverso i monitoraggi web svolti con automatismi e ricerche.

Le analisi condotte consentono di estrapolare e condividere verso il Cliente tutte quelle informazioni utili a:

- Evitare che le mail spam possano essere ricevute dai dipendenti;
- Bloccare connessioni pericolose verso ulteriori malware e server C&C;
- Identificare attraverso sistemi SIEM device già compromessi presenti nelle reti interne.

La condivisione dei dati può avvenire attraverso le specifiche metodiche e strutture usualmente impiegate per tale tipologia di servizi, quali istanza MISP o formato Stix via protocollo Taxi, o con metodiche e formati specificamente customizzati per il Cliente.

A. Svolto secondo le modalità sopra descritte;
B. Modalità flat, senza limite al numero di segnalazioni;
C. Accessibilità ai dati: attraverso la metodica ed il formato concordato con il Cliente;
D. Copertura temporale: h24 7/7 gg;
E. Periodo di erogazione: 36 mesi;

COMUNICAZIONI E REPORT

Le attività sopra descritte genereranno comunicazioni secondo le modalità sotto indicate

Monitoraggio	Notifica via email	Report PDF	Dati accessibili a portale	API/Misp/ecc. .
Anti-phishing	X		X	X
Brand Monitor	X		X	
Data Leak Monitor		X	X	
CTI Main Core		X	X	
IoC Zone				X

COPERTURA TEMPORALE E SLA

I monitoraggi di Cyber Threat Intelligence descritti nel presente documento sono continui 24h/24, 365gg/ 365.

L'Operatore dovrà garantire la presa in carico e gestione delle richieste inoltrate dal Cliente:

- Nei giorni feriali: entro 6 (sei) ore dalla data/ora di inoltro richiesta da parte di personale del Cliente;
- Nei giorni festivi: entro 12 (dodici) ore di inoltro richiesta da parte di personale del Cliente.