Accordo quadro avente ad oggetto l'affidamento
di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

ID 2296 · **LOTTO** 1

Piano Operativo

AQ SICUREZZA

accenture | FASTWEB | FINCANTIERI | DEAS

Rev.	Data	Descrizione delle modifiche	Autore
01	18/12/2024	Prima emissione	RTI

Tabella 1 – Registro delle versioni

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

Azienda Regionale della Salute della Sardegna (di seguito anche "Amministrazione" o ARES) è l'azienda sanitaria parte integrante del sistema del Servizio Sanitario della Regione Autonoma della Sardegna e del sistema del Servizio Sanitario Nazionale, (nel seguito anche "ARES" o "Amministrazione") istituita con l'obiettivo di offrire supporto alla produzione di servizi sanitari e socio-sanitari nel rispetto del principio di efficienza, efficacia, razionalità ed economicità.
ARES si prefigura come amministrazione a supporto delle 8 Aziende Sanitarie Locali (di seguito "ASL"), delle 3 Aziende Ospedaliere (di seguito "AO") e di AREUS (Azienda Regionale per l'Emergenza e Urgenza) del territorio, caratterizzate da un grado di sviluppo delle infrastrutture digitali differente, ma che condividono l'adozione progressiva del "cloud computing" e dei nuovi paradigmi di erogazione, in ottica di miglioramento della qualità dei servizi verso cittadini, imprese e altre pubbliche amministrazioni e riduzione dei costi di esercizio. Ciò è stato accelerato nell'ultimo biennio dalla necessità di "virtualizzare" in parte o in toto i processi interni ed esterni per far fronte all'emergenza pandemica.
Questi fenomeni hanno determinato notevoli cambiamenti tecnologici ed economici, con conseguenze, dirette e indirette, di lunga durata anche sulle tattiche, tecnologie e procedure della criminalità informatica.
Le organizzazioni sanitarie operano in uno scenario in rapida evoluzione e si trovano a dover trarre vantaggio da tutte le tecnologie disponibili con l'obbiettivo di massimizzare l'efficacia dell'erogazione di cure mediche, dovendo fronteggiare al contempo una crescente complessità e vulnerabilità della propria infrastruttura.
L'ambito sanitario rappresenta infatti un ambiente disomogeneo e caratterizzato da numerosi elementi di vulnerabilità: viene impiegata un'ampia gamma di tecnologie che comprende non solo i comuni sistemi IT (information Technology), ma anche dispositivi medici che con l'adozione sempre più pervasiva dell'IoMT (Internet of Medical Things) risultano connessi ad Internet e quindi potenzialmente soggetti ad attacchi cyber provenienti dall'esterno.

1.1 Scopo

L'intervento si propone di consolidare la strategia di cybersecurity finora attuata da ARES e di coinvolgere e sensibilizzare le altre Amministrazioni (8 ASL, 3 AO e AREUS), con l'obiettivo di porre le basi per una governance della sicurezza allargata e rafforzare la resilienza al rischio cyber sul perimetro di competenza.

1.2 Ambito di Applicabilità

Il **Piano Triennale per l'informatica della Pubblica Amministrazione** è uno strumento essenziale per promuovere la trasformazione digitale dell'amministrazione italiana e del Paese e, in particolare quella della Pubblica Amministrazione (PA) italiana. Tale trasformazione dovrà avvenire nel contesto del mercato unico europeo di beni e servizi digitali, secondo una strategia che in tutta la UE si propone di migliorare l'accesso online ai beni e servizi per i consumatori e le imprese e creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi per massimizzare il potenziale di crescita dell'economia digitale europea. In tale contesto dove quindi i servizi digitali rappresentano un elemento indispensabile per il funzionamento di un Paese, la PA ne è parte fondamentale e indispensabile.

È ampiamente noto che la minaccia cibernetica è sempre più attiva e cresce continuamente in qualità e quantità minando infrastrutture critiche, processi digitali e rappresentando anche un elevato rischio di natura militare visto l'utilizzo che è sempre più diffuso verso quello che chiamiamo il perimetro di sicurezza cibernetico. In questo scenario di notevole fermento, il Piano delle Gare Strategiche ICT, concordato tra Consip e AgID, ha l'obiettivo, tra le altre cose, di mettere a disposizione delle Pubbliche Amministrazioni delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza. Il Piano mantiene l'attenzione rispetto al passato ponendosi anche il cruciale problema della protezione del dato. Questo elemento è fondamentale perché tale protezione è strettamente connessa alla sua qualità e agire correttamente consente di attuare anche gli obblighi normativi europei in materia di protezione dei dati personali (GDPR).

Il Piano si focalizza sulla **protezione degli asset critici** (ICT e apparati elettromedicali) al fine di far scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche. Le azioni stabilite nel Piano sono tutte indispensabili rispetto allo scenario possibile: danni alle infrastrutture critiche, danni economici o di immagine.

In capo ai Fornitori è la responsabilità di supportare le Amministrazioni mediante i servizi resi disponibili dalla presente iniziativa e supportare i soggetti deputati al coordinamento e controllo, secondo quanto previsto dalla documentazione di gara.

Il RTI ha basato il modello di tali servizi sul National Institute of Standards and Technology (NIST) Cyber Security Framework (principale standard di sicurezza in ambito cyber, anche il framework nazionale si basa su di esso), arricchito dai principali standard e best practice di settore (ISO 27001, NERC-CIP, MITRE ATT&CK, ISF, SANS, ITIL e COBIT), integrando i requisiti normativi co-genti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al Framework Nazionale per la Cybersecurity e la Data Protection.

In particolare, nella figura sottostante è riportata la mappatura dei servizi offerti dal Framework, al fine di illustrare come tali servizi siano funzionali a ciascuna area del Framework.

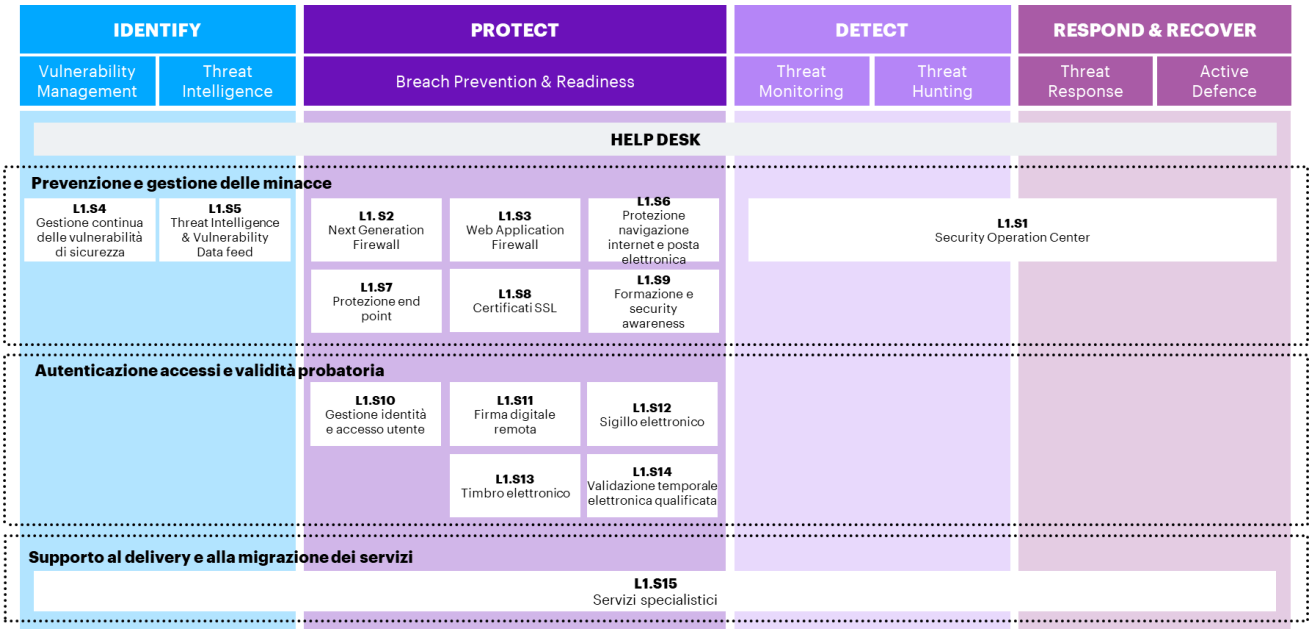

Figura 1 – Mappatura Servizi di Sicurezza e Framework NIST

In linea con le previsioni del Piano Triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, sono previste la definizione e l'implementazione di misure di governance centralizzata, anche mediante la costituzione di **Organismi di coordinamento e controllo**, orientati alla direzione strategica e alla direzione tecnica della stessa. In particolare, le attività di direzione strategica prevedono il coinvolgimento di soggetti istituzionali, mentre nell'ambito delle attività di direzione tecnica saranno coinvolti anche soggetti non istituzionali, individuati nei Fornitori Aggiudicatari della presente acquisizione. Si precisa che per "Organismi di coordinamento e controllo", si intendono i soggetti facenti capo alla Presidenza del Consiglio e/o al Ministero per l'Innovazione tecnologica e la Digitalizzazione (es: Agid, Team Digitale), che, in base alle funzioni attribuite ex lege, sono ad oggi deputati, per quanto di rispettiva competenza, al monitoraggio e al controllo delle iniziative rientranti nel Piano Triennale per l'informatica nella Pubblica Amministrazione. Nell'ambito di tali Organismi è ricompresa altresì Consip S.p.A., per i compiti di propria competenza. Rimangono salve eventuali modifiche organizzative che interverranno a livello istituzionale nel corso della durata del presente Accordo Quadro.

Gli Organismi di coordinamento e controllo saranno normati da appositi Regolamenti che, resi disponibili alla stipula dei contratti relativi alla presente iniziativa o appena possibile, definiranno gli aspetti operativi delle attività di coordinamento e controllo, sia tecnico che strategico.

I meccanismi di governance sopra introdotti e applicati anche a tutte le iniziative afferenti al Piano Triennale riguarderanno:

- i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip;
- l'inquadramento o categorizzazione degli interventi delle Amministrazioni, realizzati mediante la sottoscrizione di uno o più

contratti esecutivi afferenti alle iniziative del Piano Strategico, nel framework del Piano Triennale;

- l'individuazione, da parte delle Amministrazioni beneficiarie, secondo quanto fornito in documentazione di gara, degli indicatori di digitalizzazione con i quali gli Organismi di coordinamento e controllo analizzeranno e valuteranno gli interventi realizzati dalle Amministrazioni con i contratti afferenti alle Gare strategiche;
- la valutazione e l'attuazione della revisione dei servizi previsti dagli Accordi Quadro e/o dei relativi prezzi, per le Gare Strategiche che lo prevedono in documentazione di gara e in funzione dell'evoluzione tecnologica del mercato e/o della normativa applicabile;
- l'analisi e la verifica di coerenza, rispetto al perimetro di ogni Gara Strategica, degli interventi delle Amministrazioni realizzati mediante contratti attuativi afferenti alle Gare Strategiche;
- le modalità e le tempistiche con cui i fornitori dovranno consegnare i dati relativi ai contratti esecutivi, con particolare riferimento alla fase di chiusura degli Accordi Quadro.

L'iniziativa in oggetto si affianca alle gare strategiche previste da AgID ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese. Storicamente, il Sistema Pubblico di Connettività (SPC) ha seguito la Rete Unitaria Della Pubblica Amministrazione (RUPA), nata con l'intento di connettere le pubbliche amministrazioni, almeno quelle centrali. Il Sistema Pubblico di Connettività (SPC), è posto alla base delle infrastrutture materiali dell'architettura disegnata nel Piano Triennale l'informatica nella Pubblica Amministrazione 2017-2019 di AgID, il cosiddetto Modello Strategico. È un sistema composto da molti servizi stratificati, dalla connettività ai servizi Cloud, ed è stato aggiornato nel 2016 con nuove gare Consip SPC2, SPC Cloud ampliando il portafoglio dei servizi e delle infrastrutture.

L'iniziativa Sicurezza da remoto si pone un **duplice obiettivo**:

- quello di **garantire la continuità** e l'evoluzione dei servizi già previsti nella precedente iniziativa SPC Cloud – Lotto 2 avente ad oggetto servizi di sicurezza volti alla protezione dei sistemi informativi in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema Pubblico di Connettività;
- quello di rendere disponibili alle Amministrazioni servizi con carattere di **innovazione tecnologica** per l'attuazione del Codice dell'Amministrazione Digitale, nonché del Piano Triennale ICT della PA.

Lo scenario è contestualmente caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo. Tale specializzazione si innesta in considerazione dei diversi obiettivi a cui i due Lotti rispondono.
In particolare:

- il **Lotto di servizi di Sicurezza da remoto (Lotto 1)** ha l'obiettivo di mettere a disposizione delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati;
- il **Lotto di servizi di Compliance e controllo (Lotto 2)** ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di salute della sicurezza del sistema informativo dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 nonché sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

In riferimento a quanto sopra riportato, **ARES**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

Nell'ambito di tale lotto, si riportano di seguito i **servizi fruibili**, così come previsto dall'Accordo Quadro:

- L1.S1 – Security Operation Center
- L1.S2 – Next Generation Firewall
- L1.S3 – Web Application Firewall
- L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza

- L1.S5 – Threat Intelligence & Vulnerability Data Feed
- L1.S6 – Protezione Navigazione Internet e Posta Elettronica
- L1.S7 – Protezione degli endpoint
- L1.S8 – Certificati SSL
- L1.S9 – Formazione e Security Awareness
- L1.S10 – Gestione dell'Identità e dell'accesso dell'utente
- L1.S11 – Firma digitale remota
- L1.S12 – Sigillo Elettronico
- L1.S13 – Timbro Elettronico
- L1.S14 – Validazione temporale elettronica qualificata
- L1.S15 – Servizi Specialistici

A tal fine, **ARES**, ha individuato il Raggruppamento Temporaneo di Imprese (RTI) composto da Accenture S.p.A. (Accenture, impresa mandataria), Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri), e Difesa e Analisi Sistemi S.p.A. (DEAS) , (nel seguito anche "RTI" o "Fornitore") quale aggiudicatario dell'Accordo Quadro che effettuerà la prestazione, sulla base di decisione motivata in relazione alle specifiche esigenze dell'Amministrazione e in relazione a quanto stipulato nell'Accordo Quadro di riferimento, allo scopo di beneficiare direttamente dei Servizi e di veicolarne l'erogazione agli Enti in perimetro (cifr. 1.1 Scopo) fermo restando il rispetto da parte di entrambi dei relativi oneri verso il Fornitore.

1.3 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra il ARES e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

Tabella 1 - Assunzioni

2 RIFERIMENTI

2.1 Normativa di riferimento

Trovano applicazione le normative e gli standard internazionali riportate al "Capitolato Tecnico Generale" (§ 4.6) [DA-1].

2.2 Documenti Applicabili

Rif.	Titolo
DA-1.	ALLEGATO 1 - CAPITOLATO TECNICO GENERALE - Gara a procedura aperta per la conclusione di un accordo quadro, ai sensi del d.lgs. 50/2016 e s.m.i., suddivisa in 2 lotti e avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni.
DA-2.	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
DA-3.	Accordo Quadro
DA-4.	Offerta Tecnica – Lotto 1 GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
DA-5.	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
DA-6.	Piano Dei Fabbisogni "ARES_Sardegna_AQ2296_Lotto 1_Piano dei fabbisogni_06122024_Def.pdf" inviato in data 06/12/2024

Tabella 2 - Documenti Applicabili

3 DEFINIZIONI E ACRONIMI

Definizione	Descrizione
Accordo Quadro (AQ)	L'Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A. all'esito della procedura di gara di prima fase
Aggiudicatario / Fornitore	Se non diversamente indicato vanno intesi gli aggiudicatari previsti per ciascun AQ per ciascuno dei Lotti della fornitura
Amministrazioni	Pubbliche Amministrazioni
Amministrazione Aggiudicatrice	Consip S.p.A.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato o intendono affidare un contratto esecutivo con il Fornitore per l'erogazione di uno dei servizi oggetto dell'Accordo Quadro
Capitolato Tecnico Generale	Documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa
Capitolati Tecnici Speciali	Integrano il Capitolato Tecnico Generale e definiscono i contenuti di dettaglio e i requisiti minimi in termini di quantità, qualità e livelli di servizio, relativamente al Lotto 1 avente ad oggetto i Servizi di Sicurezza da remoto e al Lotto 2 avente ad oggetto i Servizi di Compliance e controllo
Collaudo e verifica di Conformità	Effettuati dall'Amministrazione e corrispondenti alla valutazione con verifica di merito dei prodotti consegnati
Componente	Il singolo elemento della configurazione di un sistema sottoposto a monitoraggio
Contratto Esecutivo	Il Contratto avente ad oggetto Servizi di Sicurezza da remoto, di Compliance e di Controllo per le Pubbliche Amministrazioni (Lotto 1)
Piano dei Fabbisogni	Il documento inviato dall'Amministrazione al Fornitore, al quale l'Amministrazione medesima affida il singolo Contratto Esecutivo e nel quale dovranno essere riportate, tra l'altro, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore
Piano Operativo	Il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel presente documento
Prodotto della Fornitura	Tutto ciò che viene realizzato dal fornitore. Comprende tutta la documentazione contrattuale e gli artefatti come definiti nell'appendice Livelli di servizio
Modalità di erogazione da remoto	Servizio erogato - in modalità *managed* - attraverso i Centri Servizi del Fornitore
Modalità di lavoro *On-site*	Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa o in alternativa presso la sede del Fornitore
Milestone	In ingegneria del software e Project Management indica ciascun traguardo intermedio e il traguardo finale dello svolgimento del progetto. Sono i punti di controllo all'interno di ciascuna fase oppure di consegna di specifici deliverable o raggruppamenti di deliverable. Sono normalmente attività considerate convenzionalmente a durata zero che servono per isolare nella schedulazione i principali momenti di verifica e validazione. Di fatto ciascun punto di controllo serve per approvare quanto fatto a monte della milestone ed abilitare le attività previste a valle della milestone
Sistema	Per Sistema si intende la singola immagine del sistema operativo, comprensiva di tutte le periferiche fisiche e/o logiche e di tutti i prodotti e/o servizi necessari al corretto funzionamento delle applicazioni, oppure l'insieme delle componenti HW e SW inserite in un unico chassis atto alla interconnessione e l'estensione di reti TLC (ad esempio apparati che gestiscono i primi quattro livelli della pila ISO-OSI)
Centro Servizi (CS)	La/e sede/i da cui l'Aggiudicatario eroga i servizi in modalità "da remoto" di cui al presente Capitolato per lo specifico Lotto di fornitura
Perimetro di Sicurezza Nazionale Cibernetica	Ai sensi del DL. Del 21 settembre 2002 n.105, il Perimetro è composto dai sistemi informativi e dai servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali

Tabella 3 - Definizioni

Vocabolo	Titolo
AgID	Agenzia per l'Italia Digitale

Vocabolo	Titolo
AQ	Accordo Quadro
BC	Business Continuity
CE	Contratto Esecutivo
CS	Centro Servizi
CTS	Capitolato Tecnico Speciale
CVSS	Common Vulnerability Scoring System
DA	Documenti Applicabili
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
DSI	Direzione Sistemi Informativi
HSM	Hardware Security Module
HVAC	Heating, Ventilation and Air Conditioning
HW	Hardware
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LRP	Livello di Rischio Previsto
LRR	Livello di Rischio Residuo
MGMT	Management
MPLS	MultiProtocol Label Switching
NDA	Non-Disclosure Agreement
OLO	Other Licensed Operators
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PIN	Personal Identification Number
PMO	Project Management Office
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Impresa
RTO	Recovery Time Objective
SAN	Storage Area Network
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SIEM	Security Information and Event Management
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SSL	Secure Sockets Layer
SW	Software
UPS	Uninterruptible Power Supply
UTP	Unified Threat Protection
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
WNEP	Web Navigation and Email Protection

Tabella 4 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

L'approccio organizzativo che il RTI propone è volto a garantire:

- la gestione dell'Accordo Quadro (AQ) nel suo complesso, con ruoli di organizzazione, indirizzo e controllo dei diversi Contratti Esecutivi (CE) attivati (Governo dell'AQ);
- il coordinamento dei singoli CE e l'erogazione dei servizi richiesti per ciascuno di essi (Gestione dei CE);
- la capacità di adattarsi dinamicamente alle necessità della singola PA in base, ad esempio, alla maturità della stessa in ambito Cybersecurity, alle dimensioni, al contesto tecnologico, alla tipologia di dati trattati, alla distribuzione geografica e all'appartenenza del Perimetro di Sicurezza Cibernetico Nazionale.

L'organizzazione del RTI proposta per la conduzione dell'Accordo Quadro è mostrata nella figura di seguito riportata:

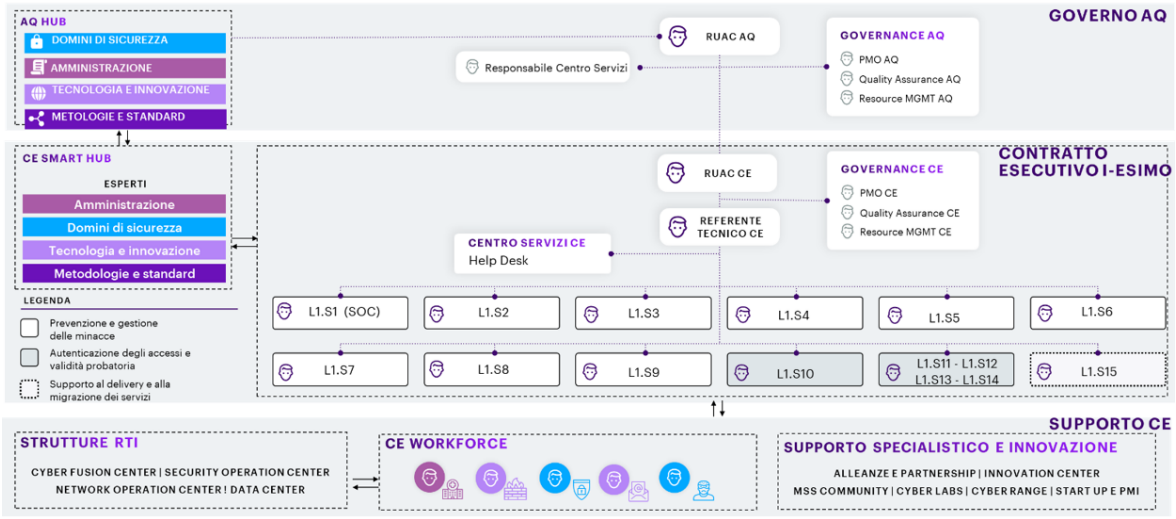

Figura 2 - Organizzazione dell'AQ proposta dal RTI

L'organigramma proposto prevede che il coordinamento delle attività del presente Accordo Quadro venga svolto dal Responsabile Unico della Attività Contrattuali dell'Accordo Quadro.

Il modello proposto si articola sui tre livelli di seguito illustrati:

- **Livello di Governo dell'AQ -** rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera Fornitura. È presieduto dal Responsabile Unico delle Attività Contrattuali dell'AQ (RUAC AQ), che svolge un'azione di indirizzo e controllo strategico in ottica di gestione unitaria dei CE. Il RUAC AQ è designato dalla mandataria, presiede il Comitato di Coordinamento del RTI composto da figure manageriali delle aziende in esso contenute e dal Responsabile del Centro Servizi, che insieme definiscono la strategia di AQ e assicurano una visione unica e integrata dell'andamento dei servizi oggetto di gara, garantendo al tempo stesso la qualità complessiva dei CE per conseguire la piena soddisfazione delle PA.
  Il RUAC AQ è il principale riferimento del RTI per Consip, rappresenta inoltre il RTI all'interno dell'Organismo Tecnico di Coordinamento e Controllo ed è quindi la principale interfaccia verso i soggetti istituzionali su tutte le tematiche contrattuali. È supportato dal team di Governance AQ che include strutture/ruoli aggiuntivi (offerti senza oneri aggiuntivi) quali: Project Management Office, Quality Assurance e Resource Management.
- **Livello dei Contratti Esecutivi -** è progettato per adattarsi alle diverse tipologie di PA che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi. A tale livello sono coordinati ed erogati i servizi previsti per ogni CE ed è prevista la presenza di:
  - ❖ un Responsabile unico delle attività contrattuali del CE (RUAC CE);
  - ❖ un Referente Tecnico CE;
  - ❖ un team di Governance CE;

- un Help Desk dedicato all'assistenza dei Referenti identificati dall'Amministrazione,
- team responsabili dell'erogazione dei servizi previsti.

Il RUAC CE ha una responsabilità speculare a quella del RUAC AQ e rappresenta la principale interfaccia verso le singole PA per tutte le tematiche contrattuali, avendo allo stesso tempo compiti di raccordo tra i due livelli.
Il Referente Tecnico CE è responsabile del corretto svolgimento delle attività e dei servizi e il relativo livello di qualità di erogazione per il singolo CE ed è supportato dal team di Governance CE (PMO CE, Quality Assurance CE e Resource Management CE).
I Team responsabili dell'erogazione dei servizi, composti da professionisti di settore, hanno l'ulteriore supporto dei maggiori esperti di tematica del RTI (Subject Matter Expert) per assicurare omogeneità di metodologie e innovazione continua in base all'evoluzione del contesto.

- **Livello Supporto CE -** garantisce due tipi di supporto:
  - *Scalabilità* - La CE Workforce comprende le strutture di appartenenza delle risorse assegnate ai CE, quali Cyber Fusion Center/Security Operation Center/Network Operation Center/Data Center, la cui dimensione garantisce flessibilità e scalabilità adeguata alle esigenze (es. aumento della domanda, complessità progettuale, contesto tecnologico, sensibilità dei dati);
  - *Supporto specialistico e innovazione* - garantito da:
    - ✓ i CdC tecnologici (es. infrastruttura, rete, applicazioni, DB, S.O., sistemi di virtualizzazione e HW);
    - ✓ i Cyber Labs di Accenture, operanti a livello globale per introdurre nuove tecnologie di sicurezza tramite prove di laboratorio che ne facilitano l'integrazione sui sistemi cliente, e i centri di ricerca e sviluppo in ambito cyber di Fastweb (FDA-Fastweb Digital Academy), Fincantieri e DEAS;
    - ✓ il network di start-up e PMI innovative;
    - ✓ le partnership con i principali vendor in materia sicurezza;
    - ✓ le MSS COMMUNITY, specializzate per ambito (es. Application Security, Digital Identity, Threat Operations, Cloud Security, Continuous Risk Management), tecnologia delle soluzioni offerte e/o presenti presso le PA richiedenti, tematica (es. ambiti Difesa, Sanità);
    - ✓ i Cyber Range (Poligoni Cibernetici) di Accenture e DEAS;
    - ✓ i laboratori di test plant di Fastweb utilizzati per testare gli apparati di sicurezza, così come nella verifica della conformità dei prodotti effettuata dai CVCN (Centro di Valutazione e Certificazione Nazionale) e CV. In particolare, per la capacità del RTI di supportare Consip, le PA e gli organismi istituzionali (es. AgID, Agenzia per la Cyber Sicurezza Nazionale) in materia di Innovazione.
- **AQ HUB e CE SMART HUB -** Strutture aggiuntive composte da esperti di diversi ambiti, con il compito di stimolare e promuovere, rispettivamente a livello di AQ e di CE, l'innovazione e le competenze tecnologiche nell'erogazione dei servizi, rafforzare il livello di conoscenze nei vari domini di sicurezza e di awareness verso le PA anche rispetto alle opportunità offerte dal contratto, garantire la conformità a standard e best practice di settore.

Per quanto concerne invece i **Centri Servizi**, questi vengono coordinati da uno specifico Responsabile che opera a livello "Governo AQ" e in accordo ai seguenti criteri:

- struttura organizzativa unica che assume la responsabilità dell'erogazione del servizio per tutte le sedi operative;
- assegnazione di responsabilità specifiche centralizzate, a livello di CS e a diretto riporto del responsabile del CS, in merito alla gestione della sicurezza informatica e della continuità operativa;
- assegnazione di responsabilità specifiche distribuite, a livello di sede operativa, in merito alla sicurezza fisica e alla gestione ambientale ed energetica.

4.1 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività richieste nel Piano dei Fabbisogni saranno svolte dalle aziende del RTI secondo la ripartizione seguente:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S1 – Security Operation Center	X			
L1.S2 – Next Generation Firewall		X		
L1.S3 – Web Application Firewall		X		
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	X			
L1.S5 – Threat Intelligence & Vulnerability Data Feed	X			
L1.S9 – Formazione e Security Awareness	X			
L1.S15 – Servizi Specialistici	X	X		
TOTALE (%)	60,12 %	39,88 %	0,00%	0,00%
TOTALE (€)	10.828.666,88 €	7.183.596,00 €	0,00 €	0,00 €

Tabella 5 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

Nella tabella che segue sono riportate le principali figure di riferimento del Fornitore, i cui ruoli e responsabilità sono stati illustrati nella parte introduttiva del Capitolo:

FIGURE DI RIFERIMENTO E REFERENTI DEL FORNITORE
RUAC AQ
GOVERNANCE AQ (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
RESPONSABILE CENTRO SERVIZI
RESPONSABILE DI SICUREZZA INFORMATICA E CONTINUITÀ OPERATIVA
RESPONSABILE DI SEDE OPERATIVA
RUAC CE
GOVERNANCE CE (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
REFERENTE TECNICO CE
RESPONSABILI DELL'EROGAZIONE DEI SERVIZI

Tabella 6 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

In base alla modalità di esecuzione dei servizi, le prestazioni contrattuali saranno erogate come di seguito indicato:

- per i servizi erogati da remoto: attraverso il Centro Servizi del Fornitore;
- per i servizi on-site (per parte dei servizi specialistici e di formazione): presso le sedi dell'Amministrazione (ARES) ove specificato dall'Amministrazione stessa.

5 AMBITI E SERVIZI

5.1 Ambiti di intervento

Gli ambiti d'intervento oggetto di fornitura come di seguito elencati hanno l'obiettivo di soddisfare i requisiti della Regione Autonoma della Sardegna così come riportati nel Piano dei Fabbisogni:

- L1.S1 – Security Operation Center
- L1.S2 – Next Generation Firewall
- L1.S3 - Web Application Firewall
- L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza
- L1.S5 – Threat Intelligence & Vulnerability Data Feed
- L1.S9 – Formazione e Security Awareness
- L1.S15 – Servizi Specialistici

5.2 Servizi richiesti

SERVIZIO	FASCIA	METRICA	IMORTO/ QUANTITA' I ANNO	IMORTO/ QUANTITA' II ANNO	IMORTO/ QUANTITA' III ANNO	IPORTO/ QUANTITA' IV ANNO
L1.S1 – Security Operation Center	Fascia 5 - > 6.000 Eps	EPS (device equivalent/Anno)	859.425,00 € / 45.836 eps	859.425,00 € / 45.836 eps	859.425,00 € / 45.836 eps	859.425,00 € / 45.836 eps
L1.S2 – Next Generation Firewall	Fascia 5 – fino a 15 Gbps	NGFW Throughput/Anno	920.700,00 € /20 apparati	920.700,00 € /20 apparati	920.700,00 € /20 apparati	920.700,00 € /20 apparati
L1.S3 – Web Application Firewall	Fascia 2 – fino a 5 Gbps	Throughput HTTP/Anno	103.000,00 €/ 2 apparati	103.000,00 €/ 2 apparati	103.000,00 €/ 2 apparati	103.000,00 €/ 2 apparati
L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza	Fascia 3 - > 200 IP	Numero di IP/Anno	408.121,20 € / 29.574,00 IP	408.121,20 € / 29.574,00 IP	408.121,20 € / 29.574,00 IP	408.121,20 € / 29.574,00 IP
L1.S5 – Threat Intelligence & Vulnerability Data Feed	Fascia 3	Data-Feed /Anno	14.200,00 €/71 Feed	14.200,00 €/71 Feed	14.200,00 €/71 Feed	14.200,00 €/71 Feed
L1.S9 – Formazione e Security Awareness	gg/p Team ottimale	Numero Utenti/Anno	434.150,08 € /1754 gg/p	372.765,12 € /1506 gg/p	407.665,44 € /1647 gg/p	407.665,44 € /1647 gg/p
L1.S15 – Servizi Specialistici	gg/p Team ottimale	gg/p Team ottimale	2.908.724,00 € /11921 gg/p	1.589.172,00 € /6513 gg/p	1.335.168,00 € /5472 gg/p	1.335.168,00 € /5472 gg/p

Tabella 7 - Servizi richiesti

5.3 Indicatore di progresso

Di seguito l'indicatore di progresso (IP) identificato in questa fase per l'erogazione della fornitura, che sarà determinato come da schema seguente:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

W

Tabella 8 - Schema definizione Indicatore di Progresso

Tale indicatore sarà oggetto di revisione con l'Amministrazione a valle della fase di presa in carico. In particolare, sarà attivato uno specifico tavolo di lavoro mirato a:

- valutare il grado di maturità digitale dei servizi offerti e il grado di maturità atteso;
- consolidare l'indicatore;
- definire le misure iniziali dell'indicatore;
- stabilire i target e cioè le misure attese alla fine del contratto.

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi richiesti

Di seguito i servizi proposti in linea con le esigenze espresse da **ARES**.

6.1.1 L1.S1 - Security Operation Center

Il servizio prevede di implementare, attraverso gli strumenti tecnologici descritti di seguito, un servizio di monitoraggio e alerting degli eventi/minacce di sicurezza sia sul perimetro IT (i.e. server, apparati di rete ed endpoint), sia sul perimetro IoT (inclusi apparati elettromedicali) al fine di consentire una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle raccomandazioni relative alle azioni di contenimento e ripristino e prevenzione futura.
Il servizio SOC si baserà sui dati raccolti e correlati dal SIEM e sarà gestito anche attraverso un "Security Orchestration, Automation & Response (SOAR)". Sarà pertanto effettuata una ottimizzazione degli eventi raccolti dai sistemi ed inviati al SIEM, selezionando solo quelli significativi in termini di sicurezza e scartando tutte le righe di log non utili al sistema SIEM ed al servizio SOC, al fine di attuare i servizi previsti nell'offerta tecnica del RTI, tra cui il servizio che prevede la gestione degli incidenti di sicurezza generati, arricchimento automatico di incidenti con informazioni di interesse, correlazione tra incidenti diversi e coordinamento delle azioni di risposta tra team distribuiti.
Il servizio SOC verrà erogato in modalità remota dal Centro Servizi preposto del Fornitore e agirà in modalità strettamente coordinata con gli altri servizi oggetto della presente fornitura, beneficiando delle informazioni da essi raccolte, contribuendo in modalità proattiva al miglioramento continuo delle policy e intervenendo con azioni di inibizione/mitigazione a fronte di evidenze di incidenti o potenziali rischi in essere.
Il servizio sarà configurato in modo tale che anche il personale autorizzato dal Committente possa avere accesso alle informazioni ed agli alert prodotti dal SOC e dal SIEM, secondo le modalità previste dalla Capitolato Tecnico e dalla risposta tecnica di AQ.

il servizio sarà declinato su due aree: quella prettamente ICT (Pdl, server, device IT) quella IoT/OT e quella IoMT relativa ai dispositivi medici. Fatto salvo quanto esplicitato nel precedente paragrafo, per i dispositivi medici sono stati individuati 5000 asset a criticità elevata, che saranno oggetto di monitoraggio. Analogamente i device ICT considerati critici sono stimati in 4000 (di cui 1500 switch e 2500 stampanti) e i sistemi IoT critici (esclusi i Medical Device) sono stimati nel numero di 600. Si prevede l'on-boarding di 4 Enti al mese per i primi tre mesi di erogazione della fornitura, andando a regime dal quarto mese in poi.

Il SOC Team è perciò composto da SME (Subject Matter Expert) esperti verticali nelle varie aree di Cyber Security e, si presenta suddiviso in tre gruppi di analisti incaricati dell'analisi e gestione degli incidenti a complessità crescente: L1, L2 ed L3.

Gli SME sono esperti di Sicurezza certificati che operano all'interno di gruppi di lavoro ben definiti con chiara responsabilità e interagiscono tra loro e con l'Istituto attraverso canali di comunicazione con **massimi livelli di confidenzialità** in base alla natura delle informazioni scambiate. Di seguito si riporta una vista sintetica delle figure che compongono il 'SOC Team' con delle modifiche rispetto ai servizi standard, modificato secondo le esigenze dell'Amministrazione:

FUNZIONE-TEAM	RUOLO / PROFILO	COMPITI E RESPONSABILITÀ
Responsabile del servizio	RSOC / SP	Punto di contatto tra ISMETT e il SOC team con le responsabilità elencate nel §6.1.2 (Security Operations Governance). Possiede certificazioni quali: ISO 27001, CISSP, ITIL, CISM.
Supporto di sicurezza Livello 1	Team L1 / Jr-ISC	Effettua il monitoraggio 24x7 degli allarmi di sicurezza, verifica la priorità degli allarmi, effettua l'analisi degli eventi e la verifica, notifica gli eventi attraverso la piattaforma di ITSM fornita per tale Convenzione ed attraverso mail o chiamate al reperibile dell'Amministrazione. Possiede certificazioni quali: SSCP, CEH.

Supporto di sicurezza Livello 2	Team L2 / Sr-ISC dedicato ad ARES in orario di servizio.	Fornisce report SIEM predefiniti, revisiona e analizza i report, effettua l'analisi degli allarmi e la verifica dei falsi positivi, fornisce supporto per la prima investigazione di breve periodo, effettua la qualifica di un evento in incidente di sicurezza, crea e traccia gli incidenti, monitora le performance, identifica le azioni di contenimento di breve periodo. Inoltre, interagisce con il team operativo dell'Amministrazione a supporto dell'attività di risoluzione e successivamente di chiusura del caso, che è comunque a carico della Committente ed in particolare del team operativo di competenza.
Supporto di sicurezza Livello 3	Team L3 / Sr-ISC	Supporta la risoluzione in caso di interruzione della raccolta dei log, supporta il tuning delle regole (casi d'uso), raccoglie e trasmette evidenze, valuta il post incidente per miglioramento continuo.
Legenda: SP Security Principal, Sr-ISC Senior Information Sec. Consultant, Jr-ISC Junior Information Sec.		

Di seguito si elencano quelli che saranno i prerequisiti al servizio:

- Configurazione delle sorgenti di log (eventi di sicurezza) e di rete a carico del team di competenza dell'Amministrazione, per la lettura e/o invio degli eventi utili al completamento del servizio, verso il Centro Servizi che costituisce la struttura unica abilitante per l'erogazione;
- Procedure di security incident management, escalation, Crisis Management.

6.1.1.1 Modello Operativo

Il modello operativo prevede il monitoraggio continuo delle informazioni prodotte dalle sorgenti di log (eventi di sicurezza) identificate come perimetro di monitoraggio ed in uso presso ARES e gli Enti coinvolti.

In sintesi, il servizio consentirà di:

- Controllare in maniera attiva il perimetro infrastrutturale soggetto al servizio di monitoraggio, attraverso attività di "monitoring real-time" così da anticipare per quanto possibile eventuali incidenti di sicurezza;
- Produrre specifici allarmi e reportistica per l'auditing sugli eventi raccolti;
- Identificare e comunicare verso ARES, le possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione;
- Acquisire eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente. Le evidenze digitali raccolte sono poi trasmesse al referente tecnico dell'Amministrazione ed archiviate;
- Valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza dell'Amministrazione aumentando l'efficacia del SOC team.

6.1.1.2 Modalità di erogazione

Il modello di erogazione si baserà sulla logica che prevede la raccolta degli allarmi generati dal sistema di monitoraggio del Centro Servizi che, in seguito ad incidenti di Sicurezza, apre il ticket verso il team "L1 SOC" sul sistema ITSM previsto per tale Convenzione. Il team "L1 SOC" controllerà le informazioni evidenziate dall'allarme, ed eseguirà le prime verifiche per una eventuale escalation verso il team "L2 SOC" o/e il reperibile dell'Amministrazione, nel caso di un fuori orario di servizio.

Successivamente alla conferma di un possibile incidente, il SOC Team procederà con le necessarie azioni, elencate di seguito solo a scopo esemplificativo:

- drill down sugli eventi aggregati che hanno generato l'evidenza/alert;
- verifica dei falsi positivi;
- investigazione/deep analysis del caso;

- escalation verso team di Sicurezza ed il team operativo di pertinenza dell'Amministrazione per segnalare/supportare azioni di remediation;
- verifica di chiusura del caso segnalato, da parte del team operativo dell'Amministrazione.

6.1.2 L1.S2 –Next Generation Firewall

L'idea architetturale, perseguita dall'Amministrazione, prevede l'installazione di N.10 cluster NGFW in alta affidabilità, fino a 15 GB fascia 5, il servizio sarà erogato con apparati installati, previo accordo con l'Amministrazione, presso le sedi dell'Amministrazione (on-premise) ed in linea con le proprie esigenze.
La soluzione prevede anche una prima fase di analisi dell'architettura di rete esistente, degli asset e delle configurazioni presenti sui firewall perimetrali, attualmente in esercizio presso l'Amministrazione, e successivamente recepisce le indicazioni di configurazione riportate a seguire:

· routing
· segregazione con reti overlay e attivazione funzionalità Firewall Statefull Layer 7, Application Control, URL Filtering e Network Antivirus
· ambienti segregati (VDOM)

6.1.3 L1.S3 –Web Application Firewall

Il servizio di "Web Application Firewall" consentirà di filtrare, monitorare e bloccare il traffico HTTP da e verso un servizio Web, esaminando il traffico, utilizzando regole, analisi e firme per rilevare attacchi e quindi proteggendo l'amministrazione dagli attac-chi incorporati nei dati trasmessi dalle applicazioni web. Nell'ambito del servizio di Web Application Firewall saranno garantite almeno le seguenti funzionalità:

- Protezione dagli attacchi più critici alle applicazioni web, quali ad esempio Iniezioni SQL, Cross-site scripting (XSS), inclusione di file e configurazioni di sistema impropri, dirottamento di sessioni, buffer overflow;
- Capacità evoluta di filtraggio del traffico con possibilità di configurare l'utilizzo di whitelist e blacklist;
- Funzionalità di apprendimento automatico che consentano di individuare un modello di comportamento dell'utente per identificare il traffico benigno e dannoso delle applicazioni;
- Rilevamento automatico della natura dei contenuti e rilevazione di attacchi che comportino la manomissione di cookie, sessioni o parametri;
- Funzionalità di ispezione del traffico SSL criptato per tutti i tipi di minacce integrate;
- Capacità di identificare/bloccare gli allegati XML che nascondono contenuti dannosi e di convalidare gli schemi per i messaggi SOAP;
- Protezione di Api e web services di qualsiasi natura;
- Supporto per le regole di controllo degli accessi a livello di rete e componente basate sulla firma per rilevare le minacce note;
- Trasmissione di eventi e log alla funzionalità di SIEM del servizio SOC oggetto di fornitura o ad altro strumento di raccolta log, ove disponibile, dell'Amministrazione;
- Produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.

Per l'Amministrazione il RTI ha pensato di erogare il servizio WAF con appliance fisici, 1 cluster in alta affidabilità (i.e. 2 web application firewall), a servizio di tutti gli enti inclusi nel perimetro, con una banda fino a 5 Gbps.

6.1.4 L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza

Il servizio proposto utilizzando una piattaforma che consente la gestione del patrimonio infrastrutturale degli Enti in perimetro, alla quale accede esclusivamente personale altamente qualificato e certificato (SANS, GEVA/GXPN, OSCP, OSCE, CEH, OPST, etc.) permetterà il censimento, la classificazione, la gestione delle vulnerabilità e la manutenzione dei device (IT, Medicali e IoT) individuati nella fase di assessment.
Nello specifico, il servizio consentirà di avere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i sistemi informatici oggetto del servizio. Esso prevede:

- Rilevazione delle vulnerabilità presenti in sistemi, apparati di rete, applicazioni (web, mobile, client-server, etc.), dispositivi ad uso professionale e personale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MI-TRE kill-chain, etc.) capaci di sfruttarle; la fase di ricerca delle vulnerabilità agevola peraltro la ri-

costruzione (ove non presente) di un 'Asset Inventory' (con CCE e CPE) del patrimonio informativo di **ARES** ai fini della successiva misura del livello di esposizione alla minaccia cyber associato ai singoli cespiti IT; inoltre, l'integrazione con le piattaforme di Cyber Threat Intelligence (es. TIS e iDefense) rende più profonda la ricerca di nuove vulnerabilità sulla base delle evidenze predittive prodotte degli analisti (artifact, IoC, IoA, etc.) anche se non note alla community (es. CVE);

- Categorizzazione, classificazione e misura del potenziale impatto delle vulnerabilità rilevate, sulla base della misura del rischio ponderato con il livello di criticità associato all'asset e derivante dalla rilevanza dei processi di **ARES** che l'asset abilita, dalla sensibilità dei dati trattati e delle interdipendenze (con altre funzioni e/o sistemi), unitamente alle indicazioni sulle modalità tecniche, organizzative e procedurali di risoluzione (o mitigazione) delle problematiche riscontrate;
- Supporto per la Pianificazione, su base priorità (stante la misura del rischio residuo corrente), delle azioni di risoluzione o mitigazione delle problematiche di sicurezza individuate e delle fasi di controllo orientate al rientro dalle non conformità e al miglioramento continuo;
- Supporto tecnico-organizzativo e tecnico-funzionale;
- Reportistica relativa alle scansioni con un alto grado di personalizzazione di elementi quali la superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

I volumi identificati per il servizio di Vulnerability scanning sarà equivalente a 29.574 IP.

L'architettura della piattaforma che abilita il servizio è composta dalle seguenti componenti principali:

- Una sonda fisica o virtuale, da installare da parte dell'Amministrazione nella propria infrastruttura qualora necessaria per raggiungere gli asset target, per l'esecuzione delle scansioni verso gli apparati di rete, gli host, i server, le applicazioni web, i database e tutti i dispositivi dotati di un indirizzo IP presenti nelle reti in perimetro; se necessario il RTI connetterà la sonda alla rete dell'Amministrazione e quest'ultimo abiliterà la comunicazione verso tutte le porte TCP e UDP dei i sistemi informativi presenti nelle reti in perimetro per eseguire le scansioni.
- Una console di gestione, installata presso il Centro Servizi, da cui è possibile pianificare le analisi infrastrutturali e applicative, visualizzare i risultati e gestire la reportistica per mantenere una visione complessiva dello stato di esposizione del contraente; la console di gestione comunica con le sonde tramite una connessione VPN.
- Una console per il dashboarding avanzato e l'automazione, installata presso il Centro Servizi, per la configurazione e la gestione remota delle sonde; la console di gestione comunica con le sonde tramite una connessione VPN.
- Un modulo di supporto con acceleratori e strumenti di diagnostica per l'esecuzione delle scansioni manuali, le analisi delle evidenze e la rappresentazione dei risultati.
- Un modulo di monitoraggio del rischio calcolato sui processi.
- Una knowledge base contestualizzata e aperta all'information sharing.

Qualora i suddetti assesment vengano svolti in ambienti di produzione, l'Amministrazione e/o i singoli Enti Sanitari Locali che usufruiscano del servizio approveranno formalmente l'esecuzione di questi test, manlevando il Fornitore nel caso in cui l'esecuzione dei test approvati provochi degli impatti e/o danni, , eccetto nei casi di negligenza o dolo.
Resta inteso che il Fornitore segnalerà all'Amministrazione e/o ai singoli Enti Sanitari Locali, tramite comunicazione formale, il perimetro che sarà interessato dall'attività di analisi e di test, la tipologia e la descrizione dei controlli da effettuare e la valutazione dell'impatto potenziale.
In ogni caso, prima di eseguire test che richiedano l'accesso ai sistemi, l'Amministrazione e/o i singoli Enti Sanitari Locali, dovranno fornire specifica autorizzazione in tal senso, pertanto, qualora tale autorizzazione non venga fornita il Fornitore non potrà procedere.
Fermo restando quanto sopra, l'Amministrazione si impegna a verificare che siano resi al Fornitore tutti i consensi, le autorizzazioni e le manleve suddette e necessarie

6.1.5 L1.S5 – *Threat Intelligence &Vulnerability Datafeed (Ti&Vdf)*

Il servizio in oggetto è erogato dal Centro Servizi avvalendosi della piattaforma di Threat Intelligence ATIP, sviluppata e gestita da Accenture che prevede l'accesso tramite interfaccia e API alle informazioni di intelligence che coprono le vulnerabilità di oltre 1.000 vendor, strumenti e tecniche malware, Indicatori di Compromissione, organizzazioni target, threat actor e loro motivazioni, campagne di phishing e minacce pertinenti l'organizzazione aziendale.
Per ulteriori dettagli sui servizi L1.S5 e l'utilizzo della piattaforma ATIP di Accenture si rimanda all'"Annex A" in fondo al presente documento.

Funzioni offerte
Il servizio TI&VDF consente di elaborare ed estrarre le informazioni necessarie attraverso le funzionalità offerte, articolate nei livelli riportati nella seguente figura:

Figura 3-Livelli Funzionalità

Tali livelli comprendono tutte le funzionalità previste nel capitolato dell'AQ Sicurezza e ne aggiungono alcune migliorative, come di seguito descritto:

- **Accesso web** - la piattaforma integra l'interfaccia che si basa su un modello di rappresentazione dei dati che consente agli analisti di mettere in relazione nodi di informazioni su threat actor, malware, vulnerabilità, campagne, target, domini, e-mail di phishing, ecc. Tale struttura di dati consente un accesso più rapido ai dati rilevanti e la capacità di visualizzare le relazioni tra i diversi dati;
- **Personalizzazione delle informazioni -** la piattaforma consente di personalizzare le informazioni richieste dalla Amministrazione in funzione dei sistemi adottati. Tramite l'interfaccia è possibile consultare i bollettini predisposti dal team di Threat Intelligence (TI) e generare report personalizzati; nello specifico saranno predisposti report contenenti:
  - IOCs, specifici per i sistemi gestiti dall' Amministrazione;
  - notizie di interesse per l'Amministrazione e con lo scopo di mantenere l'Amministrazione allineata su possibili eventi di interesse, fintanto che questi non si traducano in una minaccia fattuale;
  - sintesi delle segnalazioni effettuate nel periodo di riferimento e la loro classificazione sia per tipologia che per severity (mensile).
- **Intelligence -** la piattaforma è gestita da un team specialistico di intelligence che ha l'obiettivo di arricchire le informazioni e contestualizzarle rispetto al contesto operativo della Amministrazione;
- **Analisi / Prioritizzazione** - la piattaforma dispone di funzionalità atte a filtrare le informazioni in funzione delle necessità dell'Amministrazione secondo meccanismi dinamici e continuativi che consentono di focalizzare l'attenzione sui fenomeni più rilevanti.

Feed di Threat Intelligence
I feed utilizzati per l'erogazione del servizio TI&VDF saranno gli outcome:

- di prodotti di Vendor di riferimento;
- di analisi effettuate da ricercatori di sicurezza;
- del network Accenture costituito da tutti Centri di Competenza a livello Globale progressivamente acquisiti negli anni.

Tali Feed, contengono informazioni affidabili, aggiornate e dettagliate sulle vulnerabilità di sicurezza. Ove possibile, i feed provengono dalle fonti primarie dei dati di intelligence in modo da ridurre la ridondanza delle informazioni raccolte e ottimizzarne l'utilizzo.
Di seguito vengono rappresentate le caratteristiche, in termini di descrizione e informazioni fornite, dei feed utilizzati raggruppati per Tipologia.

TIPOLOGIA - Vulnerability data feed	NUMEROSITÀ - 2 feed
Descrizione	Feed costituiti da informazioni sulle vulnerabilità che impattano i prodotti di interesse, provenienti dal National Vulnerability Database (NVD) e dal database di vulnerabilità CVE Details
Informazioni	Descrizione della vulnerabilità, CPE impattate, score CVSS, classificazione CWE, data pubblicazione e ultimo aggiornamento, link ai bollettini di sicurezza rilasciati dal vendor, sfruttamento della vulnerabilità in campagne di attacco.

Tabella 9- Vulnerability data feed

TIPOLOGIA - Vulnerability Intelligence Data Feed	NUMEROSITÀ - 6 feed
Descrizione	Feed costituiti da informazioni sulle vulnerabilità provenienti da diverse fonti tra cui la piattaforma proprietaria Accenture ATIP e i database di exploit per lo sfruttamento delle vulnerabilità disponibili in rete.
Informazioni	Descrizione della vulnerabilità, CPE impattate, score CVSS, classificazione CWE, data pubblicazione e ultimo aggiornamento, link ai bollettini di sicurezza rilasciati dal vendor, sfruttamento della vulnerabilità in campagne di attacco.

Tabella 10-Vulnerability Intelligence data feed

TIPOLOGIA - Threat Advisory Data Feed	NUMEROSITÀ - 2 feed
Descrizione	Bollettini riguardanti le minacce che impattano il contesto italiano e il settore dei Servizi Pubblici, redatti dal team di Cyber Threat Intelligence (CTI) del RTI
Informazioni	Descrizione di minacce, informazioni di contesto approfondite con un focus sulla PA, IoC aggiornati, azioni di mitigazione consigliate.

Tabella 11-Threat Advisory data feed

TIPOLOGIA - Threat Intelligence Data Feed	NUMEROSITÀ - 19 feed
Descrizione	Feed riguardanti il panorama globale delle minacce, inviati automaticamente dai vendor e dai provider di Intelligence.
Informazioni	Informazioni sulle minacce esistenti a livello globale, eventuali informazioni di contesto disponibili, IoC.

Tabella 12- Threat Intelligence data feed

TIPOLOGIA - Threat Indicators Data Feed	NUMEROSITÀ - 42 feed
Descrizione	Feed costituiti da Indicatori di Compromissione (IoC) relativi alle minacce che impattano il settore dei Servizi Pubblici in Italia.
Informazioni	IoC aggiornati relativi alle minacce di interesse per la PA contraente relativi a: domini sospetti, URL dannosi, elenchi di hash malware noti, indirizzi IP associati ad attività dannose.

Tabella 13-Threat Indicators data feed

I volumi indicati nel Piano dei Fabbisogni di ARES corrispondono alla quantità di 71 Feed i quali saranno configurati secondo le necessità dell'Amministrazione.

6.1.6 L1.S9 – Formazione e Security Awareness

L'efficacia della gestione del rischio cyber risiede nella stretta collaborazione tra le strutture che pianificano ed esercitano le Security Operation a vario titolo. Questo è particolarmente vero in quelle situazioni "ibride" nelle quali i ruoli e i compiti delle Security Operation sono ripartiti tra personale interno ed esterno all'Amministrazione con vari gradi di competenze specialistiche. A questo si aggiunga il generalizzato *skill shortage* nei ruoli della cybersecurity segnalato dall'Agenzia per la cybersicurezza dell'Unione europea (ENISA) e dai principali operatori del settore (https://www.guerredirete.it/cybersicurezza-italia-perche-non-si-trovano-candidati/). Questa debolezza strutturale richiede l'attuazione di percorsi di formazione/aggiornamento del

personale IT dell'Amministrazione sui temi della cybersicurezza e dell'integrazione tra Security Operation residenti ed erogate da remoto, formazione che verterà sulla costruzione di un lessico comune, sulla natura delle minacce e le modalità di attacco che queste utilizzano (TTP - Tactics, Tecniques and Procedures), sulle procedure di gestione degli attacchi cyber. La formazione dovrà essere corredata da esercitazioni che prevedano la simulazione di attacchi cyber per la verifica delle procedure di gestione e dell'Incident Response Plan.
In linea con quanto richiesto dall'Amministrazione nel Piano dei Fabbisogni, il servizio sarà erogato da remoto ed on-site.
I contenuti di sicurezza informatica trasmessi ai discenti saranno mirati a fornire gli strumenti propedeutici affinché ci sia, a valle della chiusura del contratto, una piena consapevolezza sui temi di cybersecurity strettamente legati alle tecnologie adottate da parte dell'Amministrazione ed un sostanziale aumento delle competenze dei singoli partecipanti.
Per soddisfare le esigenze dell'Amministrazione e degli Enti afferenti saranno strutturate due macro-iniziative:

- Servizi di Formazione specifica
- Servizi di Formazione diffusa/Security Awareness

Servizi di Formazione specifica

Tale macro iniziativa prevede l'erogazione di corsi di formazione/Workshop su tematiche di Cybersecurity principalmente per figure apicali e referenti ICT, da erogarsi in modalità sincrona o asincrona, in presenza o da remoto in base agli accordi con l'Amministrazione, nonché attività volte alla definizione delle esigenze formative e a monitorarne l'efficacia. In particolare, verranno svolte le seguenti attività:

- Presentazione delle iniziative formative a singolo Ente aderente
- Erogazione di un assessment per verificare il livello di consapevolezza delle figure apicali e dei referenti ICT su tematiche di cyber sicurezza per singolo ente aderente
- Condivisione delle esigenze e delle iniziative proposte con singolo ente aderente
- Produzione dei contenuti e materiale didattico di ciascuna iniziativa proposta
- Erogazione dell'iniziativa
- Produzione di reportistica inerente gli esiti di ogni singola iniziativa erogata e dell'attività di formazione destinata alle fi-gure apicali e ai referenti ICT nel suo complesso, per singolo Ente e, qualora richiesta, con una vista complessiva circa il totale delle iniziative erogate.

Tali iniziative potranno includere, a titolo esemplificativo e non esaustivo:

- Corsi da remoto tramite personale specializzato
- Corsi in aula tramite personale specializzato
- Workshop e sessioni di confronto con gli Stakeholders sui temi della Sicurezza informatica
- Condivisione del materiale necessario all'erogazione del corso e/o alla produzione di moduli multimediali che saranno in carico all' Amministrazione
- Condivisione dei contenuti di newsletter in ambito cyber security
- Predisposizione ed erogazione di attività di simulazioni di tipo "table-top" relativi alla gestione degli incidenti di sicurezza.
- eventuale attivazione di percorsi di supporto a certificazioni in materia di Cybersecurity per i referenti ICT degli Enti aderenti

Gli interventi formativi verranno calendarizzati in accordo con l'Amministrazione e verranno erogati nelle fasce orarie previste dal Capitolato Tecnico dell'Accordo Quadro.

Le attività fanno riferimento ai punti 1 e 3 del Piano dei fabbisogni nel paragrafo relativo alla formazione:

- *<u>Formazione specifica per le strutture tecniche degli enti:</u> due sessioni formative per personale tecnico IT (per 15 discenti a sessione per AREUS, AOU Sassari, AOU Cagliari e AO Brotzu e 150 discenti per ARES) aventi oggetto tematiche di cyber Security da concordare con le Amministrazioni e da erogare nel primo anno di vita contrattuale.*
- *<u>Formazione specifica per il top management:</u> attività formativa annuale (per un totale di 4 anni) specifica per Top Management (circa 8 discenti ad Ente), finalizzata al miglioramento della cultura della sicurezza informatica e con lo scopo di fornire ai dirigenti le conoscenze necessarie per comprendere i rischi informatici, valutare le minacce e adottare le misure di sicurezza più efficaci*

Servizi di Formazione diffusa/Security Awareness

Tale macro iniziativa prevede l'erogazione di corsi di formazione e awareness destinati ad un pubblico più ampio ed eterogeno, con particolare attenzione alla consapevolezza diffusa per tutto il personale aziendale sulle tematiche di cybersecurity.
Sono previsti corsi da remoto e/o on site su tematiche quali, principali veicoli di attacco, riconoscimento di eventi sospetti, comunicazione alle parti interessate per la gestione dell'evento, simulazioni di phishing, ecc. ecc. a cui seguiranno check point di verifica dell'apprendimento e reportistica.

Questa attività mira a soddisfare la richiesta dell'Amministrazione al punto 2 del Piano dei fabbisogni nel paragrafo relativo alla formazione

- *Formazione per la popolazione aziendale: attività formativa annuale (per un totale di 4 anni) per accrescere la consapevolezza degli utenti/dipendenti di ARES e dei 12 Enti in perimetro (circa 11.000 utenti).*

6.1.7 L1.S15 – Servizi Specialistici

A completamento delle linee di servizio sopra citate, saranno erogati servizi specialistici a supporto al fine di aumentare il livello di sicurezza ed integrarli alle strategie di cybersecurity dell'Amministrazione attività di coordinamento ARES ed Enti, tra cui:

- raccolta requisiti
- supporto tecnico al servizio
- review processi impattati per compliance e per le organizzazioni interessate
- Project Management
- Program Management

Di seguito si riportano i progetti a corpo, identificati come Servizi Specialistici, ad integrazione di ciascuno dei servizi selezionati di **ARES**, tra quelli previsti dall'Accordo Quadro.

6.1.7.1 Integrazione servizi di sicurezza per L1.S1 - Security Operation Center

I Servizi Specialistici a supporto del Servizio SOC, prevedono l'utilizzo di personale specializzato in logica di progetto, finalizzati al controllo imparziale della corretta esecuzione del servizio, nel supportare ed evolvere il processo di monitoraggio e gestione degli incidenti di sicurezza. Gli obiettivi indicati per tale servizio specialistico aggiuntivo sono i seguenti e saranno oggetto di pianificazione:

- assessment del contesto tecnologico degli Enti
- raccolta requisiti
- installazione e configurazione di sonde e log collector
- supporto alla configurazione delle log sources
- impostazione connessione al SOC
- classificazione degli incidenti e configurazione del processo di crisis management
- supporto nella "remediation" degli incidenti di sicurezza
- identificazione e realizzazione di nuovi use-case a supporto del processo di detection al fine di migliorare continuamente la libreria di casi dedicati
- identificazione e realizzazione di nuovi playbook dedicati, con lo scopo di contestualizzare il monitoraggio e la risposta alla violazione
- supporto alla investigazione di possibili attacchi informatici o "data breach"
- review processi impattati per compliance e per le organizzazioni interessate
- project management
- attività di coordinamento ARES ed Enti
- supporto tecnico al servizio
- Supporto specialistico erogata come presidio On Site dedicato alle strutture dell'organizzazione, garantendo una protezione avanzata e personalizzata delle infrastrutture IT (i.e. server, apparati di rete. Endpoint);

Il servizio potrà essere erogato sia in modalità da remoto che on-site.

6.1.7.2 Integrazione servizi di sicurezza per L1.S2 – Next Generation Firewall

I Servizi Specialistici a supporto del Servizio NGFW, prevedono l'utilizzo di personale specializzato in logica di progetto, finalizzati al controllo imparziale della corretta esecuzione del servizio, nel supportare ed evolvere il processo di monitoraggio e gestione degli incidenti di sicurezza. Gli obiettivi indicati per tale servizio specialistico aggiuntivo sono i seguenti e saranno oggetto di pianificazione:

- Supporto per l'on-boarding degli Enti con modalità progressiva con pianificazione di on-boarding di 4 enti al mese.
- Supporto nell'implementazione della segregazione e dell'hardening delle reti.
- Supporto per la progettazione di un servizio di accesso sicuro in MFA per gli utenti e gli amministratori di sistema.
- Supporto per le attività di monitoraggio e per la protezione basata su DNS, al fine di bloccare gli accessi a siti malevoli.

Il servizio potrà essere erogato sia in modalità da remoto che on-site.

6.1.7.3 Integrazione servizi di sicurezza per L1.S3 – Web Application Firewall

I Servizi Specialistici a supporto del Servizio WAF, prevedono l'utilizzo di personale specializzato in logica di progetto, finalizzati al controllo imparziale della corretta esecuzione del servizio, nel supportare ed evolvere il processo di monitoraggio e gestione degli incidenti di sicurezza. Gli obiettivi indicati per tale servizio specialistico aggiuntivo sono i seguenti e saranno oggetto di pianificazione:

- Supporto nella "remediation" degli incidenti di sicurezza;
- Supporto nell'implementazione di regole custom per la protezione applicativa dei siti web esposti.

Il servizio potrà essere erogato sia in modalità da remoto che on-site.

6.1.7.4 Integrazione servizi di sicurezza per L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza

Il servizio prevede, un supporto specialistico per la consegna del report delle vulnerabilità periodico sui sistemi e una assistenza all'Amministrazione nella valutazione delle vulnerabilità per identificare un piano di rientro in base alle priorità dettate dall'Amministrazione e dai suoi team tecnici/operativi, che avranno l'onere di valutare la fattibilità e i tempi per loro competenza.
I Servizi saranno forniti all'Amministrazione per un supporto tecnico connesso all'attivazione dei servizi da remoto oggetto di fornitura e in particolare:

- supporto nella definizione, configurazione ed erogazione del servizio di monitoraggio continuo delle vulnerabilità di sicurezza con particolare riferimento all'analisi dei deliverable raccolti a seguito dell'esecuzione da parte del fornitore delle sessioni di vulnerability assessment previsto nel servizio
- supporto nelle analisi delle vulnerabilità
- supporto alle attività di asset intelligence e discovery
- supporto alle attività di asset management
- supporto nella definizione del piano di rientro per Ente e supporto tecnico al servizio
- supporto nella revisione dei processi impattati

Il servizio potrà essere erogato sia in modalità da remoto che on-site.

6.1.7.5 Integrazione servizi di sicurezza per L1.S5 – Threat Intelligence & Vulnerability Data Feed

I servizi specialistici saranno quindi erogati al fine di integrare il servizio standard con ulteriori moduli che consentiranno all'Amministrazione di avere un quadro più dettagliato delle minacce che possono impattare il proprio dominio.
Di seguito una descrizione dei moduli che saranno integrati:

- Domain and Phishing Monitoring: Il modulo **Domain and Phishing Monitoring** monitora la registrazione di nuovi domini e permette di identificare quelli che contengono riferimenti a siti web, brand o termini di ricerca legittimi del perimetro del Cliente. Il modulo consente, attraverso la raccolta di feed di phishing, di verificare la presenza di eventi di phishing relativi al marchio del Cliente, segnalando proattivamente potenziali abusi. Il modulo permette inoltre di valutare il takedown delle risorse. Per il presente modulo è previsto un limite di volume di 10 domini Web e di 1 brand.

- Data and Credential Leakage: Il modulo **Data and Credential Leakage** è progettato per identificare e segnalare tempestivamente l'esposizione non autorizzata o la fuga di dati aziendali sensibili, inclusi documenti riservati, violazioni delle credenziali dei clienti, a seguito di attacchi informatici che potrebbero portare a modifica, perdita, distruzione, divulgazione impropria o accesso non autorizzato ai dati. Il rilevamento di dati e credenziali trapelati si basa sull'uso di diversi feed OSINT e privati, raccolti e analizzati per mitigare il potenziale abuso da parte di attori criminali. Per il presente modulo è previsto un limite di volume di 10 domini web e 1 brand.

- Dark Web Monitoring: Il modulo **Dark Web Monitoring** è specializzato nel monitoraggio di vari forum e marketplace del cybercrime accessibili ad Accenture su fonti del Deep e Dark Web, per comprendere le intenzioni dei threat actor, come ad esempio le discussioni tra threat actor e insider malintenzionati, le vulnerabilità e i punti deboli nei processi aziendali. Il modulo monitora i siti di "Malware as a Service", i marketplace e i forum sulla Darknet e le piattaforme di messaggistica per rilevare fughe di notizie o menzioni al Cliente e ai suoi fornitori, partner e peer. Per il presente modulo è previsto un limite di volume di 10 domini web e 1 brand.

- Vulnerability Advisory: Il modulo **Vulnerability Advisory** fornisce notifiche di nuove vulnerabilità per individuare quelle che potrebbero avere un impatto sulle CPE (Common Platform Enumeration) relative agli asset monitorati. Il servizio monitora la pubblicazione di nuove vulnerabilità o aggiornamenti del National Vulnerability Database (NVD), le vulnerabilità precedentemente sconosciute (zero-day) pubblicate da fonti CLOSINT e HUMINT e la pubblicazione di exploit code (Proof Of Concept) relativi a vulnerabilità che hanno un impatto sull'ambiente del Cliente. Per il presente modulo è previsto un limite di volume di 50 Tecnologie.

- External Asset Monitoring: Il modulo **External Asset Monitoring** esamina la superficie di attacco del Cliente attraverso l'integrazione di servizi open-source non invasivi per identificare le informazioni pubblicamente disponibili e indesiderate sui sistemi esterni. Il servizio comprende il rilevamento di configurazioni errate e di problemi di sicurezza che riguardano l'infrastruttura di rete, come porte aperte, esposizione a vulnerabilità note (CVE) e protocolli non configurati correttamente nei sistemi rivolti a Internet. Per il presente modulo è previsto un limite di volume di 10 domini web.

- Intelligence Warning: Il modulo **Intelligence Warning** fornisce una visione approfondita delle minacce attuali ed emergenti attraverso la collezione, l'analisi e la condivisione di informazioni sul panorama globale delle minacce, raccolte da fonti OSINT, dal Clear, Deep e Dark Web e da numerosi feed specializzati per identificare e comprendere la natura delle minacce informatiche. Il modulo fornisce *Alert* tempestivi sulle minacce che impattano direttamente l'organizzazione e *Advisory* informativi con lo scopo di anticipare e prevedere rischi e incidenti potenziali.

- Social Monitoring: Il modulo **Social Monitoring** monitora i principali social media per identificare eventi, minacce o situazioni che possono avere un impatto negativo sul Cliente, sui suoi asset e sul suo brand. Il monitoraggio viene condotto su pagine, gruppi e post dei social media indicizzati pubblicamente dai motori di ricerca per individuare menzioni al Cliente che indichino profili social, pagine, canali, gruppi, bot o contenuti falsi che potrebbero essere utilizzati per perpetrare frodi o riutilizzi non autorizzati di loghi o marchi del Cliente e altre attività dannose. Per il presente modulo è previsto un limite di volume di 1 brand.

- Rogue Mobile App: Il modulo **Rogue Mobile App** si basa sul monitoraggio dei principali marketplace ufficiali e non ufficiali per identificare applicazioni mobili fraudolente che tentano di emulare le app ufficiali del Cliente, o applicazioni sviluppate da terze parti non autorizzate i cui loghi o marchi imitano quelli ufficiali del Cliente. Inoltre, il modulo rileva la presenza delle applicazioni mobili del Cliente all'interno di elenchi di obiettivi contenuti nel codice di applicazioni

dannose, che potrebbero esfiltrare dati sovrapponendosi alle applicazioni target legittime. Per il presente modulo è previsto un limite di volume di 3 mobile app e 1 brand.

- VIP Monitoring: Il modulo **VIP Monitoring** è progettato per rilevare la distribuzione e l'uso fraudolento di informazioni sensibili e private relative a figure VIP dell'organizzazione del cliente, tra cui credenziali di account, numeri di telefono, e-mail esposte nel Clear, Deep e Dark Web, e per monitorare le menzioni che minacciano i VIP. L'identificazione precoce di attività digitali fraudolente, come l'impersonificazione dell'identità di un dirigente da parte di un threat actor, limita i danni alla reputazione dello stakeholder e protegge l'integrità del brand. Per il presente modulo è previsto un limite di volume di 5 utenti.

6.1.7.6 Integrazione servizi di sicurezza per L1.S15 – Ulteriori attività

- Supporto nella revisione dell'impianto documentale di sicurezza che viene impattato dalla messa in esercizio dei servizi gestiti (procedure di gestione degli incidenti, patch management, asset management, ecc., ecc.);
- Attività di project management e program management; generazione dei report personalizzati rispetto ai report e relazioni standard forniti dai servizi a Catalogo (output).

6.1.7.7 Dettaglio servizi specialistici

Codice servizio collegato	Descrizione	METRICA	IMPORTO/ QUANTITA' I ANNO	IMPORTO/ QUANTITA' II ANNO	IMPORTO/ QUANTITA' III ANNO	IMPORTO/ QUANTITA' IV ANNO
L1.S1 SOC	On-boarding Enti e integrazione con infrastrutture Enti	gg/p Team ottimale	1.110.200,00 €/ 4550,0 gg/p	400.160,00 €/ 1640,0 gg/p	400.160,00 €/ 1640,0 gg/p	400.160,00 €/ 1640,0 gg/p
L1.S1 SOC	Supporto on-site per protezione infrastruttura	gg/p Team ottimale	595.360,00 €/ 2440,0 gg/p	488.000,00 €/ 2000,0 gg/p	488.000,00 €/ 2000,0 gg/p	488.000,00 €/ 2000,0 gg/p
L1.S2 NGFW	SetUp NGFW e Integrazione con infrastrutture Enti	gg/p Team ottimale	18.056,00 €/ 74,0 gg/p	0,0	0,0	0,0
L1.S2 NGFW	Secure Access	gg/p Team ottimale	329.400,00 €/ 1350,0 gg/p	101.992,00 €/ 418,0 gg/p	101.992,00 €/ 418,0 gg/p	101.992,00 €/ 418,0 gg/p
L1.S2 NGFW	Protezione DNS	gg/p Team ottimale	0,0	254.004,00 €/ 1041,0 gg/p	0,0	0,0
L1.S3 WAF	SetUp WAF	gg/p Team ottimale	48.800,00 €/ 200,0 gg/p	24.400,00 €/ 100,0 gg/p	24.400,00 €/ 100,0 gg/p	24.400,00 €/ 100,0 gg/p
L1.S4 VM	Progetto Asset Intelligence	gg/p Team ottimale	479.948,00 €/ 1967,0 gg/p	0,0	0,0	0,0
L1.S5	TI moduli aggiuntivi	gg/p Team ottimale	113.948,00 €/ 467,0 gg/p	107.604,00 € 441,0 gg/p	107.604,00 € 441,0 gg/p	107.604,00 € 441,0 gg/p
L1.S15 SS	Servizi di Governance e PMO	gg/p Team ottimale	213.012,00 €/ 873,0 gg/p	213.012,00 €/ 873,0 gg/p	213.012,00 €/ 873,0 gg/p	213.012,00 €/ 873,0 gg/p

6.2 Utenza interessata / coinvolta

Personale dell'Amministrazione e degli Enti in perimetro (cifr. 1.1 Scopo).

6.3 Eventuali riferimenti / vincoli normativi

N.A.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 48 mesi, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), avrà durata come indicato nella seguente tabella:

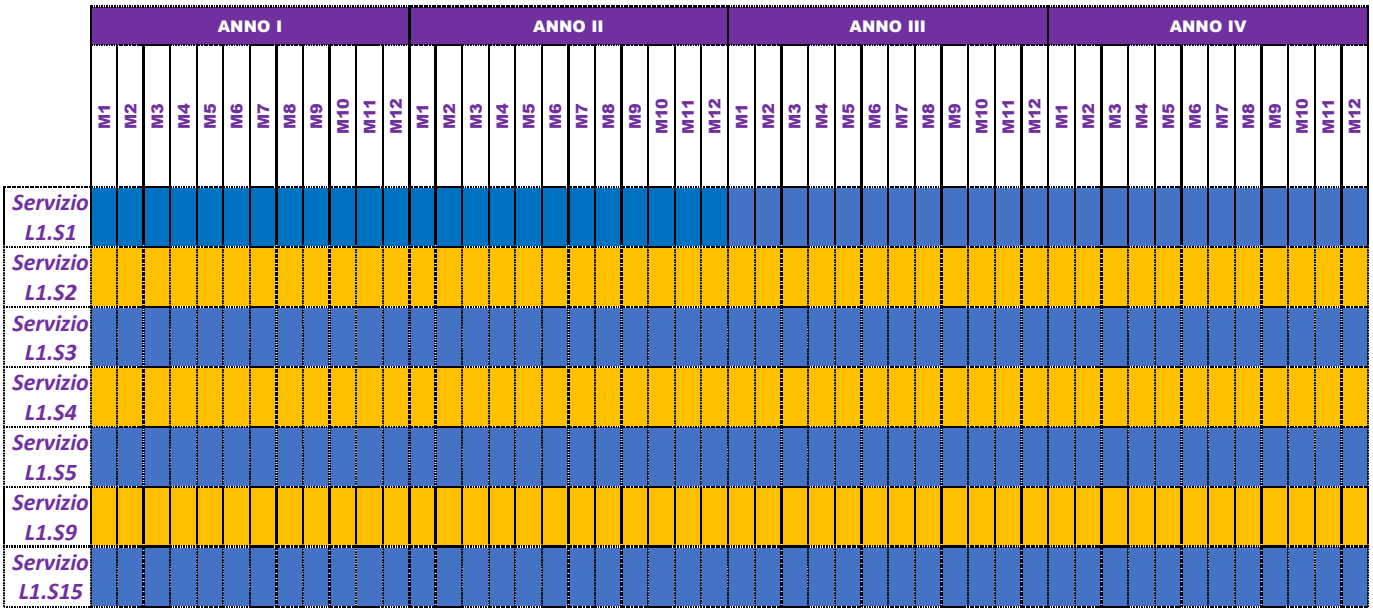

Tabella 14 – Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo dispiegherà i suoi effetti dalla data di stipula e avrà una durata di 48 mesi decorrenti dalla data di conclusione dell'attività di presa in carico.

7.3 Gruppo di Lavoro

L'approccio organizzativo individuato e descritto all'interno del Capitolo 4 consente di predisporre team e organizzazioni del lavoro secondo condizioni ad hoc per ogni progetto, secondo i carichi di lavoro previsti nella progettualità condivisa ma facilmente scalabili, qualora in corso d'opera maturassero condizioni tali da richiedere una modifica al numero dei team, delle risorse o del perimetro d'intervento. Una volta individuate le peculiarità dell'Amministrazione contraente, la selezione del gruppo di lavoro avviene analizzando il contesto della stessa sia dal punto di vista tecnologico, individuando il personale maggiormente qualificato sulle tecnologie e sui prodotti già in uso o attese, che tematico, andando ad identificare le figure professionali con esperienze e competenze nel settore pubblico.

7.4 Modalità di esecuzione dei Servizi

Per la modalità di esecuzione dei servizi è possibile far riferimento al Capitolo 8 del Capitolato Tecnico Speciale. In generale, a partire dal Piano di Lavoro Generale, l'Amministrazione richiederà la stima ed il Piano di Lavoro del singolo stream progettuale (obiettivo), fornendo la documentazione di supporto ed i macro-requisiti per poter effettuare una stima dell'obiettivo.
Di seguito si riporta una tabella di sintesi con le principali milestone per ogni servizio:

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	**Amministrazione**
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	**RTI**
Collaudo	Esecuzione del collaudo dei servizi per cui è stato richiesto	**RTI**
Attivazione	Individuazione del ciclo di vita ed avvio del fornitore a procedere con le attività sul servizio. Al momento dell'attivazione saranno noti elementi caratteristici ai quali si associa una valutazione di complessità	**Amministrazione**
Consegna	Rilascio degli artefatti previsti dal piano di lavoro, sia intermedi che finali	**RTI**
Approvazione e Verifica di Conformità	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto	**Amministrazione**
Accettazione e Verifica di Conformità	Verifica e validazione dei prodotti intermedi di servizio, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione	**Amministrazione**
Valutazione difettosità all'avvio e Verifica di Conformità	Verifica della piena fruizione delle funzionalità e dei servizi da parte dell'utente (cittadino/ impresa/ operatore amministrativo/ decisore/ fruitore) tramite l'esame della quantità e della tipologia di malfunzionamenti e non conformità rilevati durante il periodo di avvio in esercizio. Certificazione della corretta esecuzione del servizio	**Amministrazione**

Tabella 15 - Descrizione milestone per obiettivo

Per il Governo della Fornitura, si propone l'adozione delle pratiche di seguito descritte:

- **Stato avanzamenti lavori – tecnico.** Con cadenza mensile (o su richiesta dell'Amministrazione) per le attività progettuali e mensile (o su richiesta dell'Amministrazione) per quelle continuative, verrà prodotto un report di sintesi che sarà discusso nel corso di un meeting ad hoc con l'Amministrazione. Il report riporterà, a livello di progetto e a livello di obiettivo: i) avanzamento e scostamenti rispetto al piano di lavoro; ii) attività svolte e attività previste; iii) rischi e problematiche operative; iv) punti aperti; v) azioni da intraprendere per il corretto svolgimento delle attività.

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

La quota massima di attività subappaltabile – o concedibile in cottimo – da parte del RTI è pari al 50% dell'importo complessivo previsto dal contratto. Di seguito è riportato l'elenco delle attività / prestazioni per parti delle quali il RTI intende ricorrere al subappalto:

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S1 – Security Operation Center **L1.S4 – Gestione Continua delle Vulnerabilità di Sicurezza** **L1.S5 – Threat Intelligence & Vulnerability Data Feed** **L1.S9 – Formazione e Security Awareness** **L1.S15 – Servizi Specialistici**	**Accenture**	**50%**
L1.S2 – Next Generation Firewall **L1.S3 – Web Application Firewall** **L1.S15 – Servizi Specialistici**	**Fastweb**	**50%**

Tabella 16 - Modalità di ricorso al Subappalto da parte del Fornitore

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

Di seguito sono riportate per ogni servizio le metriche di misura e le modalità di erogazione e consuntivazione.

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ ANNO	VALORE ECONOMICO (totale su 4 anni)
L1.S1	Per Device equivalenti	Da remoto	A canone	Mensile	18,75 €	45836	3.437.700,00 €
L1.S2	Throughput	Da remoto	A canone	Mensile	46.035,00 €	20 FW	3.682.800,00 €
L1.S3	Throughput	Da remoto	A canone	Mensile	51.500,00 €	2 WAF	412.000,00 €
L1.S4	Numero IP	Da remoto	A Canone	Mensile	13,80 €	29574	1.632.484,80 €
L1.S5	Numero datafeed	Da remoto	A Canone	Mensile	200,00 €	71	56.800,00 €
L1.S9	gg/p Team ottimale	Da remoto /on site	Progettuale – a corpo	Mensile	247,52 €	1754 il primo anno, 1506 il secondo anno, 1647 per ogni anno successivo	1.622.246,08 €
L1.S15	gg/p Team ottimale	Da remoto /on site	Progettuale – a corpo	Mensile	244,00 €	29378 (n°11921 primo anno, n°6513 secondo anno, 5472 terzo e quarto anno)	7.168.232,00 €

Tabella 17 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **18.012.262,88 € iva esclusa.**

A seguire si riporta la mappatura dei fondi disponibili, come indicato nella sezione 2. Contesto, del Piano dei Fabbisogni e la loro distribuzione negli anni:

Lotto	Servizio	2025				2026				2027				2028			
		Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex
Lotto 1	Security Operation Center (SOC)		617.000		1.379.217	107.125			752.300	859.425				859.425			
Lotto 1	Next Generation Firewall (NGFW)		22.000		392.535	38.350			214.110	920.700				920.700			
Lotto 1	Web Application Firewall (WAF)		38.000		20.533	89.116			11.200	103.000				103.000			
Lotto 1	Gestione continua delle vulnerabilità di sicurezza (Vulnerability Management)		165.000		416.919	199.251			208.870	408.121				408.121			
Lotto 1	Threat Intelligence & Vulnerability Data Feed (TI)		14.000		26.033				14.200	14.200				14.200			
Lotto 1	Formazione e Security Awareness		82.689	5.603	209.120	342.568				342.568				342.568			
Lotto 1	Servizi specialistici per SOC			1.058.661	5.603	96.951		791.209		888.160				888.160			
Lotto 1	Servizi specialistici per NGFW			345.808		249.846		106.150		101.992				101.992			
Lotto 1	Servizi specialistici per WAF			49.654				27.084		24.400				24.400			
Lotto 1	Servizi specialistici per VM			1.238.056													
Lotto 1	Servizi specialistici per TI					107.604				107.604				107.604			
Lotto 1	Servizi specialistici di Governance e PMO				390.522				213.012	213.012				213.012			
Lotto 1	Servizi specialistici per migrazione on cloud in sicurezza																
Totale NON IVATO		-	938.689	2.697.782	2.840.482	1.230.810	-	924.443	1.413.692	3.983.182	-	-	-	3.983.182	-	-	-
Totale IVATO		-	1.145.201	3.291.294	3.465.388	1.501.588	-	1.127.821	1.724.704	4.859.482	-	-	-	4.859.482	-	-	-

Tabella 18 – Mappatura fondi disponibili

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

La fatturazione sarà eseguita in accordo con quanto previsto nello Schema di Contratto Esecutivo. Per quanto concerne i termini di pagamento si fa riferimento a quanto previsto nell'Accordo Quadro.

9 ALLEGATI

9.1 Piano di Lavoro Generale

Per il piano di lavoro generale si rimanda all'allegato Piano di Lavoro Generale.

9.2 Piano di Presa in Carico

Come riportato nel Piano dei Fabbisogni, una prima pianificazione di queste attività, è riportato nell'allegato Piano di Presa in Carico. Il RTI si impegna a garantire l'esecuzione dei collaudi nelle modalità e con riferimento ai servizi per i quali è richiesto come sarà concordato con l'Amministrazione durante il periodo di Presa in Carico.
.

9.3 Piano della Qualità Specifico

Per il piano di qualità specifico si rimanda al documento denominato Piano della Qualità Specifico.

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE e del Responsabile di CE.

9.5 Misure di Sicurezza poste in essere

Per le misure di sicurezza poste in essere si rimanda al Piano di Sicurezza del Centro Servizi.

9.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH)

Si allega la documentazione trasmessa a Consip tramite pec in data 11/11/2022, relativa al principio "Do No Significant Harm" (DNSH).

ANNEX A - Servizi di Threat Intelligence & Vulnerability Data Feed - Condizioni d'uso per la Piattaforma ATIP di Accenture

SERVIZI

1.1 Accenture, come dettagliato nel presente Piano Operativo, fornirà i servizi di **L1.S5 Threat Intelligence & Vulnerability Data Feed** (nel seguito del presente documento il "Servizio" o i "Servizi"), tramite la piattaforma ATIP (la "Piattaforma ATIP" o la "Piattaforma").

1.2 **Piattaforma ATIP.** La Piattaforma ATIP raccoglie, normalizza ed organizza le informazioni raccolte nell'ambito dei Servizi. La Piattaforma ha tre componenti operative principali:

• *Acquisizione di informazioni:* la Piattaforma acquisisce informazioni per eseguire i Servizi. Le fonti di queste informazioni includono feed "OSINT" di intelligence open source.

• *Analisi dell'intelligence:* Accenture utilizza una combinazione di metodi automatizzati e manuali per analizzare le informazioni all'interno della Piattaforma.

• *Reporting delle informazioni:* la Piattaforma produce degli alert. Tali alert includono dettagli sugli eventi, correlazione con eventi noti, cause degli attacchi, metodi utilizzati e soluzioni consigliate per la risoluzione o la prevenzione della minaccia. Gli alert, accessibili in modalità di sola lettura, informano tempestivamente l'Amministrazione sugli eventi individuati dal Servizio. La Piattaforma può essere configurata per inviare gli alert sotto forma di feed di posta elettronica ad una mailing list personalizzata, che tenga conto di flussi diversi per livello di intelligence (strategico, operativo e tattico). Una volta avvisata tramite e-mail, l'Amministrazione può accedere ad una sezione dedicata della Piattaforma contenente un bollettino dettagliato sulle minacce ("Bollettino delle Minacce"), archivio dei risultati contestualizzati per l'Amministrazione stessa.

1.3 **Data Feed.** Il Servizio prevede l'abilitazione dei feed di dati sulle minacce e sulle vulnerabilità sulla Piattaforma allo scopo di migliorare il flusso di dati relativi alle minacce di sicurezza e alle vulnerabilità. In linea con il Piano Operativo di cui al Contratto, il Cliente richiede 71 Data Feed tra quelli di seguito elencati:

Feed	Tipologia
abuse.ch	Indicator
Alienvault	Indicator
Alienvault	Report
Blocklist	Indicator
Greensnow	Indicator
Emerging Threats	Indicator
CERT-FR	Indicator
CERT-FR	Report
ci-badguys	Indicator
CIRCL OSINT Feed	Indicator
CIRCL OSINT Feed	Report
CyberCrime	Indicator
CyberCure	Indicator
DiamondFox	Indicator
DigitalSide	Indicator
DigitalSide	Report
DataPlane DNS	Indicator
Feodo IP Blocklist	Indicator

Feed	Tipologia
sipregistration	Indicator
SMTP data	Indicator
sshpwauth	Indicator
Honeynet Telnet Brute-force Ips	Indicator
DataPlane TELNET login	Indicator
The Botvrij.eu Data	Indicator
The Botvrij.eu Data	Report
ZeroDot1	Indicator
Threatfox	Indicator
Threatfox	Report
dan.me.uk TOR	Indicator
Honeynet honeypots urls	Indicator
URLHaus	Indicator
URLHaus	Report
VNC RFB	Indicator
VXvault	Indicator
Accenture Cyber Threat Intelligence - Actively exploited vulnerabilities	Indicator
Accenture Cyber Threat In-	Indicator

firehol_level1	Indicator
IP protocol 41	Indicator
IP Blocklist SNORT	Indicator
ipspamlist	Indicator
IPsum	Indicator
malshare	Indicator
malsilo	Indicator
Malware Bazaar	Indicator
MalwareBazaar	Report
Metasploit	Vulnerability
mirai.security.gives	Indicator
OpenPhish	Indicator
Panels Tracker	Indicator
PhishScore	Indicator
Phishtank	Indicator
pop3gropers	Indicator
sipinvitation	Indicator
sipquery	Indicator

telligence - Public sector-targeting	
Accenture Cyber Threat Intelligence - Italy-targeting	Indicator
Accenture Cyber Threat Intelligence - Actively exploited vulnerabilities	Report
Accenture Cyber Threat Intelligence - Public sector-targeting	Report
Accenture Cyber Threat Intelligence - Italy-targeting	Report
Accenture Cyber Threat Intelligence	Malware
Accenture Cyber Threat Intelligence	Threat Actor
CISA Cybersecurities Alert & Advisories	Report
CISA Blog & News	Report
ACTI Data Feed	Indicator
ACTI Data Feed	Vulnerability
CSIRT-ITA	Report
MITRE	Malware
MITRE	Attack Pattern
MITRE	Tool
MITRE	Intrusion Set
MITRE	Course of Action
NIST	Vulnerability

IMPEGNI

2.1. L'Amministrazione dovrà:

(a) Nominare gli utenti autorizzati ad accedere alla Piattaforma ATIP (ivi inclusi gli accessi tramite modalità API) nonché a ricevere gli alert e garantire che detti utenti mantengano riservati nome utente e password. Nel caso in cui uno o più utenti non necessitino più dei suddetti accessi e/o qualora lascino l'Amministrazione, la stessa dovrà informare tempestivamente Accenture per la relativa rimozione. Si precisa che per "utenti autorizzati" si intendono i dipendenti dell'Amministrazione e/o i dipendenti di fornitori terzi dell'Amministrazione che sono autorizzati ad accedere alla Piattaforma ATIP dall'Amministrazione stessa. Qualora gli utenti autorizzati siano dipendenti di fornitori terzi dell'Amministrazione, l'Amministrazione (con esclusione dei competitors) si impegna a far sottoscrivere anche al fornitore interessato le presenti condizioni e a darne evidenza ad Accenture.

(b) Assicurarsi che tutte le azioni degli utenti autorizzati siano in linea con il presente accordo ed il corretto uso delle proprie connessioni al sistema Accenture.

(c) Fornire tempestivamente ad Accenture tutte le informazioni necessarie per la fase di acquisizione delle informazioni;

(d) Determinare se i Servizi soddisfino i requisiti dell'Amministrazione e siano conformi alle leggi, regolamenti, policy o guide a cui l'Amministrazione è soggetta.

(e) Determinare se intraprendere azioni sulla base dei risultati dei Servizi e/o se implementare eventuali modifiche alle politiche interne, ai sistemi o alle misure di sicurezza. Resta inteso che quanto fornito da Accenture durante l'erogazione dei Servizi non costituisce mai in alcun modo consulenza, opinione o raccomandazione legale.

(f) Garantire l'utilizzo del Contenuto, come sotto definito, qualsiasi azione o della mancata azione, in risposta al Contenuto.

(g) Al termine dei Servizi, cessare immediatamente di utilizzare la Piattaforma ATIP; a tale data i diritti di utilizzo della stessa cesseranno immediatamente, fermo restando, tuttavia, che l'Amministrazione avrà il diritto di continuare ad utilizzare il Contenuto (come di seguito definito) in suo possesso anche dopo tale termine e sempre in conformità al presente Accordo.

2.2**. Proprietà intellettuale di Accenture**. Allo scopo di fornire i Servizi, Accenture utilizzerà contenuti di Threat Intelligence generati su misura per la Piattaforma ATIP ("**Contenuto**"), che sono e resteranno di sua proprietà e ne conserva tutti i diritti, i titoli e gli interessi relativi alle opere di Accenture, che consistono in: (a) informazioni sulle vulnerabilità zero day pubbliche e non pubbliche derivanti da molteplici fonti pubbliche e ricerche interne; (b) flussi di indicatori di minaccia atti a rilevare gli attacchi informatici; e (c) altre informazioni di cyber intelligence, avvisi, strumenti analitici e visualizzazioni interattive. L'Amministrazione è consapevole che il Contenuto costituisce knowhow di Accenture e che pertanto può utilizzare tale Contenuto solo così come gli viene fornito (secondo i principi di "*as is*", "*where is*" e "*as available*") e solo ed esclusivamente allo scopo di gestione e protezione della propria rete, sistemi e risorse. L'Amministrazione, consapevole che il Contenuto costituisce Informazioni Riservate di Accenture, non trasferirà nè distribuirà il Contenuto o qualsiasi parte di esso a terzi e non dovrà: (a) tentare di copiare la Piattaforma ATIP e il Contenuto nonchè creare un servizio o un prodotto sostitutivo attraverso l'uso della Piattaforma ATIP; (b) consentire l'uso diretto o indiretto del Servizio avente ad oggetto il Contenuto da parte di terzi, fatti salvi gli utenti autorizzati;(c) utilizzare il Contenuto per fornire servizi a terzi; (e) rimuovere qualsiasi riservatezza, diritto d'autore o altri segni distintivi dal Contenuto o da qualsiasi opera Accenture visualizzata o copiata in conformità al presente accordo; (f) creare opere derivate del Contenuto; o (g) modificare, disassemblare, decompilare, decodificare o effettuare qualsiasi altro tentativo di scoprire o ottenere la proprietà intellettuale che fornisce il Servizio relativo alla Piattaforma ATIP.

TERMINI E CONDIZIONI AGGIUNTIVE

3.1 L'Amministrazione riconosce che il Servizio si basa sulla disponibilità di intelligence open source e di informazioni disponibili al pubblico e accetta che Accenture non può garantire che i Servizi eseguiti:

- nè i report di Accenture o le raccomandazioni rese nel corso dei Servizi saranno prive di errori, complete o legalmente perseguibili;
- rileveranno o individueranno tutte le vulnerabilità, le minacce alla sicurezza, le intrusioni e i danni alla rete, alle strutture, agli asset e alle proprietà della stessa;
- Resta inteso inoltre che qualunque eventuale report fornito in seguito alla esecuzione dei Servizi non si intende realizzato per essere utilizzato (i) al fine di ottenere certificazioni, (ii) nell'ambito di procedimenti contenziosi o a fini di (iii) auditing.

Il Servizio, il Contenuto e i singoli componenti del Servizio, nonché le API per accedervi, costituiscono Informazioni riservate di Accenture o dei suoi concessori di licenza terzi e saranno trattati come tali in conformità al presente Accordo. L'Amministrazione è responsabile di mantenere riservato il Contenuto, di utilizzarlo solo internamente all'interno della propria attività allo scopo di proteggere le proprie reti e di proteggere il Contenuto dalla divulgazione a terzi. L'Amministrazione deve informare tempestivamente Accenture dopo essere venuta a conoscenza di qualsiasi accesso, acquisizione, divulgazione, perdita o utilizzo non autorizzato del Servizio e del Contenuto.

3.2 Se Accenture determina, che il report fornito contiene errori, o è, o potrebbe essere, soggetto a un reclamo secondo cui viola qualsiasi diritto di qualsiasi persona o entità, l'Amministrazione si impegna ad eliminare, correggere o rendere inaccessibili tale Contenuto su richiesta di Accenture.

3.3 **Metadati.** L'Amministrazione autorizza Accenture a conservare per i propri scopi aziendali eventuali indicatori di compromissione, malware, vulnerabilità, anomalie o altri metadati rilevati come parte o correlati alla prestazione dei Servizi ("Metadati"). Accenture quindi potrà analizzare, copiare, archiviare e utilizzare tali metadati per scopi di miglioramento della sicurezza, compreso lo sviluppo di risorse di intelligence sulle minacce.

3.4 **Segnalazione**. L'Amministrazione resta responsabile della segnalazione di eventuali data breach. Qualora Accenture sia tenuta a segnalare qualsiasi informazione dell'Amministrazione alle forze dell'ordine o alle autorità di regolamentazione, Accenture farà tutto il possibile per avvisare l'Amministrazione stessa prima di rispondere e, se possibile, consentire alla stessa di sollevare obiezioni presso tali autorità. Fatto salvo quanto sopra, l'Amministrazione consente ad Accenture di conformarsi ai requisiti delle autorità preposte all'applicazione della legge o delle autorità di regolamentazione in relazione ai Servizi.

3.5. **Trattamento Dati.** Il trattamento dei dati effettuato all'interno della Piattaforma ATIP, si intenderà regolato dall'atto di nomina che verrà sottoscritto tra le parti prima dell'avvio dei servizi. Si precisa che nelle categorie di interessati si intendono con il presente atto inclusi anche (i) i nomi e gli indirizzi e-mail aziendali degli utenti autorizzati ad accedere alla Piattaforma A-TIP, come comunicati ad Accenture dall'Amministrazione, al fine di fornire le credenziali di accesso. (ii) qualsiasi dato personale con cui Accenture potrebbe, nel corso del Servizio, entrare in contatto e quindi condividere con l'Amministrazione, inclusi indirizzi e-mail aziendali, password o altri dati personali simili del personale, dei fornitori o dei clienti dell'Amministrazione, nonché di qualsiasi altro individuo i cui dati vengono restituiti a seguito di ricerche in base ai nomi/dati sulle parole chiave forniti dall'Amministrazione (dati personali ai sensi di (i) e (ii) collettivamente, nel contesto dei Servizi).