ALLEGATO A – OFFERTA TECNICA DEL FORNITORE

Gara a procedura aperta per la conclusione di un accordo quadro avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

07/10/2021

ID 2296 - **LOTTO** 1

AQ SICUREZZA

accenture | FASTWEB un passo avanti | FINCANTIERI NexTech | DEAS

SOMMARIO

1 PREMESSA

L'innovazione tecnologica avvenuta nell'ultimo decennio, e le nuove necessità causate dall'avvento della pandemia iniziata nel 2020, hanno generato il bisogno di un'accelerazione nella digitalizzazione della Pubblica Amministrazione (PA). Ciò ha contribuito all'aumento del rischio di esposizione alle **minacce di tipo cibernetico**, rischio accentuato dal fatto che non tutte le organizzazioni ad oggi possiedono adeguate capacità di difesa nei confronti delle minacce emergenti.

L'**aumento della superficie di attacco** ha portato al proliferare di azioni offensive ai danni di aziende, enti pubblici e governi, perpetrate principalmente tramite campagne di phishing e ransomware, che hanno portato l'estorsione online ad un nuovo livello, trasformando in poco tempo il crimine informatico in uno dei modelli di business più redditizi e scalabile.

In questo contesto gli enti regolatori europei e nazionali hanno avviato molte iniziative volte a offrire regolamentazioni e best practice nell'ambito della sicurezza informatica, come cardine imprescindibile per la transizione digitale. In particolar modo per la PA il quadro si compone dei seguenti principali elementi:

- il **Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020–2022**, nato per guidare operativamente la trasformazione digitale della PA e che trova nella sicurezza informatica un elemento determinante;
- il **Piano Nazionale di Ripresa e Resilienza** (**PNRR**), che identifica la "digitalizzazione, innovazione e **sicurezza nella PA**" come la prima delle missioni del piano con ingenti investimenti dedicati alla sicurezza cibernetica;
- il **Perimetro di sicurezza nazionale cibernetica,** instituito con lo scopo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, dal cui malfunzionamento o interruzione possa derivare un pregiudizio per la sicurezza nazionale;
- la nascita dell'**Agenzia per la Cybersicurezza Nazionale** (**ACN**), che funzionerà da interlocutore unico per i soggetti pubblici e privati in tema di misure di sicurezza nazionali.

La presente iniziativa **Sicurezza da remoto** si inserisce all'interno di questo scenario, che sta delineando l'approccio italiano alla minaccia cibernetica, e consentirà di migliorare la **capacità di resilienza del paese**.

Il costituendo Raggruppamento Temporaneo d'Impresa (in seguito indicato dalla sigla RTI o semplicemente dall'uso della prima persona plurale) formato da Accenture S.p.A. (Accenture) in qualità di mandataria e da Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri) e Difesa e Analisi Sistemi S.p.A. (DEAS) costituisce una compagine in grado di permettere il pieno raggiungimento degli obiettivi prefissi dall'AQ, in quanto:

- **Accenture** è il più grande operatore di servizi di sicurezza al mondo; l'unità operativa dedicata Security ha più di 9.000 professionisti dedicati alla protezione dello spazio cibernetico, più di 1.000 in Italia. Opera da più di 20 anni per oltre 2.900 clienti in 67 paesi differenti; oltre ad avere un'ampia esperienza nell'erogazione dei servizi di sicurezza gestiti, sia nel privato che nel settore pubblico, è riconosciuta per la sua capacità di innovarne la modalità di erogazione, grazie alla sua rete globale di Centri di Ricerca, Sviluppo e Innovazione;
- **Fastweb** è il primo fornitore della PA in Italia di servizi avanzati di telecomunicazioni e di ICT, con più di 15 anni di esperienza, potendo vantare la presenza in una pluralità di enti della Pubblica Amministrazione Centrale (PAC) e Locale (PAL) essendo aggiudicataria di numerose Convenzioni e Accordi Quadro quali, ad esempio, SPC Cloud Lotto 2 Sicurezza, SPC 2 Connettività, SGM, Infrastrutture Condivise SPC, TF5, CT5, AQ DTO3, AQ System Management;
- **Fincantieri NexTech** è una società tecnologica, appartenente al Gruppo Fincantieri, che opera principalmente per lo sviluppo di soluzioni nei settori della sicurezza e della protezione di informazione, rappresentando il centro di competenza tecnologico del Gruppo Fincantieri, con la capacità di supportare lo sviluppo e l'integrazione sia di soluzioni "Legacy" che "innovative";
- **DEAS** è una PMI innovativa che ha scelto la Sicurezza come ambito di ricerca e sviluppo per un'offerta innovativa già apprezzata nella PAC.

I **valori** (competenze, esperienze, migliori pratiche, beni) che il nostro RTI mette a disposizione della Fornitura in oggetto possono essere classificati in relazione agli **obiettivi** che tale Fornitura si pone: **Continuità**, **Evoluzione** e **Innovazione**. La seguente tabella illustra una sintesi di tali valori, più ampiamente descritti al §3.2.

Obiettivi	Competenze e asset messi a disposizione della Fornitura
Continuità	**Fastweb** è aggiudicataria del Contratto Quadro "Servizi di Gestione delle Identità Digitali e Sicurezza Applicativa" (SPC Cloud L2) che ha permesso di sviluppare **esperienze** in numerosi progetti pubblici anche tramite una **copertura capillare delle PA**. **Accenture** è il primo fornitore di servizi in ambito sicurezza in Italia, erogandoli sia da remoto sia on-site tramite la struttura **Managed Security Services** e **il Cyber Fusion Center di Napoli**. **Fincantieri** e **DEAS** garantiscono continuità specifica nel critico **settore Difesa**.
Evoluzione	**Accenture** ha realizzato il modello **Cyber Defense Operating Model** che facilita la presa in carico dei servizi di un nuovo cliente, l'erogazione dei servizi stessi per la protezione dei sistemi informativi, il monitoraggio e miglioramento continuo per raggiungere il livello di Sicurezza auspicato. È inoltre **partner dell'anno dei maggiori vendor di tecnologia in ambito Sicurezza** senza legarsi a nessuno di essi (**technology agnostic**) e opera da **system integrator** per valorizzare le diverse tecnologie nell'interesse dei clienti. Rende, inoltre, disponibili asset distintivi descritti nel documento, tra cui: servizio di Intelligence iDefense, piattaforma di Intelligence TIS, piattaforma di Security Awareness, ecc. **Fincantieri** mette a disposizione esperienze distintive maturate nel settore militare e della **cyber security.**

	DEAS, grazie alle competenze nel settore **Difesa**, garantisce una continua **evoluzione verticale dei servizi**.
Innovazione	**Accenture** apporta ✓il contributo di una **rete globale di centri di ricerca e sviluppo** (*Cyber Labs*), di **erogazione dei servizi di sicurezza da remoto** (*Cyber Fusion Center*) e di **poligoni cibernetici** (*Cyber Range*) sia in Italia che nel resto del mondo (50+ Centri, di cui 2 in Italia) ✓il valore del **continuo investimento in acquisizioni di società specializzate** in servizi di cyber security (es. Maglan, FusionX, iDefense, Syman-tec e Contex-IS specializzata in ambito Governativo e Difesa in UK). ✓la **più grande rete globale di *threat intelligence*** con specialisti che coprono più di 39 lingue parlate e casi di successo internazionali a difesa di numerosi governi esteri. **Fastweb** mette a disposizione laboratori di sicurezza equipaggiati con **tecnologie all'avanguardia** per l'analisi di apparati embedded, strumentazioni di test e misura, centri dedicati a **collaudi e prove tecniche per la certificazione** di servizi e prodotti di sicurezza per la PA. **Fincantieri** apporta il valore della sua fitta **rete di collaborazione con le principali università e centri di ricerca** la **partecipazione a progetti di ricerca nazionali e internazionali** sui temi della sicurezza per ambienti **militari e della difesa**. **DEAS** mette a disposizione know how e strumenti per l'**applicazione dell'Intelligenza Artificiale (AI) ai Big Data** generati dall'erogazione dei servizi di Sicurezza.

Il **fattore unificante e acceleratore** della messa in opera ed erogazione dei servizi di sicurezza da remoto è il **Cyber Defense Operating Model (CDOM)**, un modello operativo proprietario messo a disposizione da Accenture per la Fornitura. Grazie alle sue componenti (Modello Operativo, Libreria di Procedure, Funzioni Fondamentali e Interfacce Chiave, Workflow, ecc.) oltre a garantire un'erogazione della **fornitura rapida, standardizzata e di qualità**, agisce come elemento omogeneizzante creando un'organizzazione di Fornitura coesa e integrata che alimenta un processo di **miglioramento incrementale continuo**. Tale modello – il cui schema di alto livello è rappresentato in Figura 1 - è basato 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); integra i requisiti normativi cogenti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al **Framework Nazionale per la Cybersecurity e la Data Protection**, che rappresenta un punto di riferimento adatto a realtà fortemente eterogenee, dalla grande PAC alla piccola PAL. Proponiamo, quindi, un approccio globale e collaborativo che non definisce solo le competenze chiave di un **Security Operation Center**, SOC (i.e. *Threat Intelligence*, *Vulnerability Management*, *Threat Monitoring*, *Threat Hunting, IIdentity Management, Application Security, Threat Response e Active Defence*) ma rappresenta anche le funzioni chiave complementari (i.e. *Breach Prevention & Readiness*, *Governance*, *Gestione prestazioni del servizio*, *Automazione e Orchestrazione, Machine Learning (ML), Miglioramento Continuo* e servizi trasversali), che sono fondamentali per un'efficace gestione dei servizi gestiti di sicurezza (MSS, Managed Security Services) oggetto di tale fornitura.

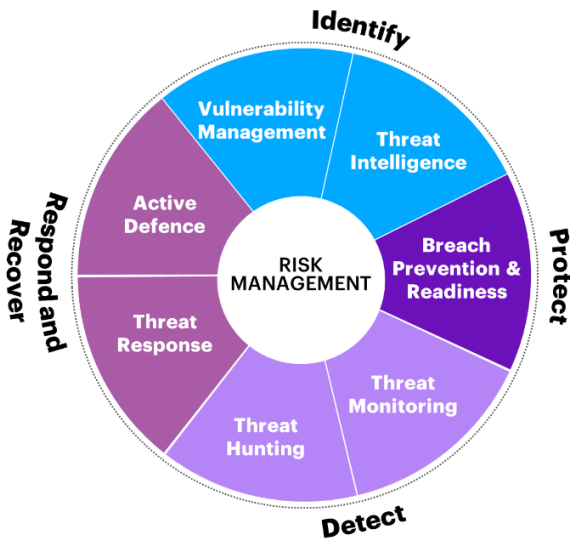


Figura 1 - Schema del CDOM

In Figura 2 mostriamo come le componenti del CDOM sono pienamente aderenti allo schema dei servizi previsti dalla presente Fornitura. Ad esempio, sotto la macrofunzione NIST Identify il CDOM prevede il dominio di sicurezza Vulnerability Management che include 4 sotto-servizi che rispondono pienamente ai requisiti del servizio L1-S4 Gestione continua delle vulnerabilità di sicurezza, facilitando la riduzione del rischio.

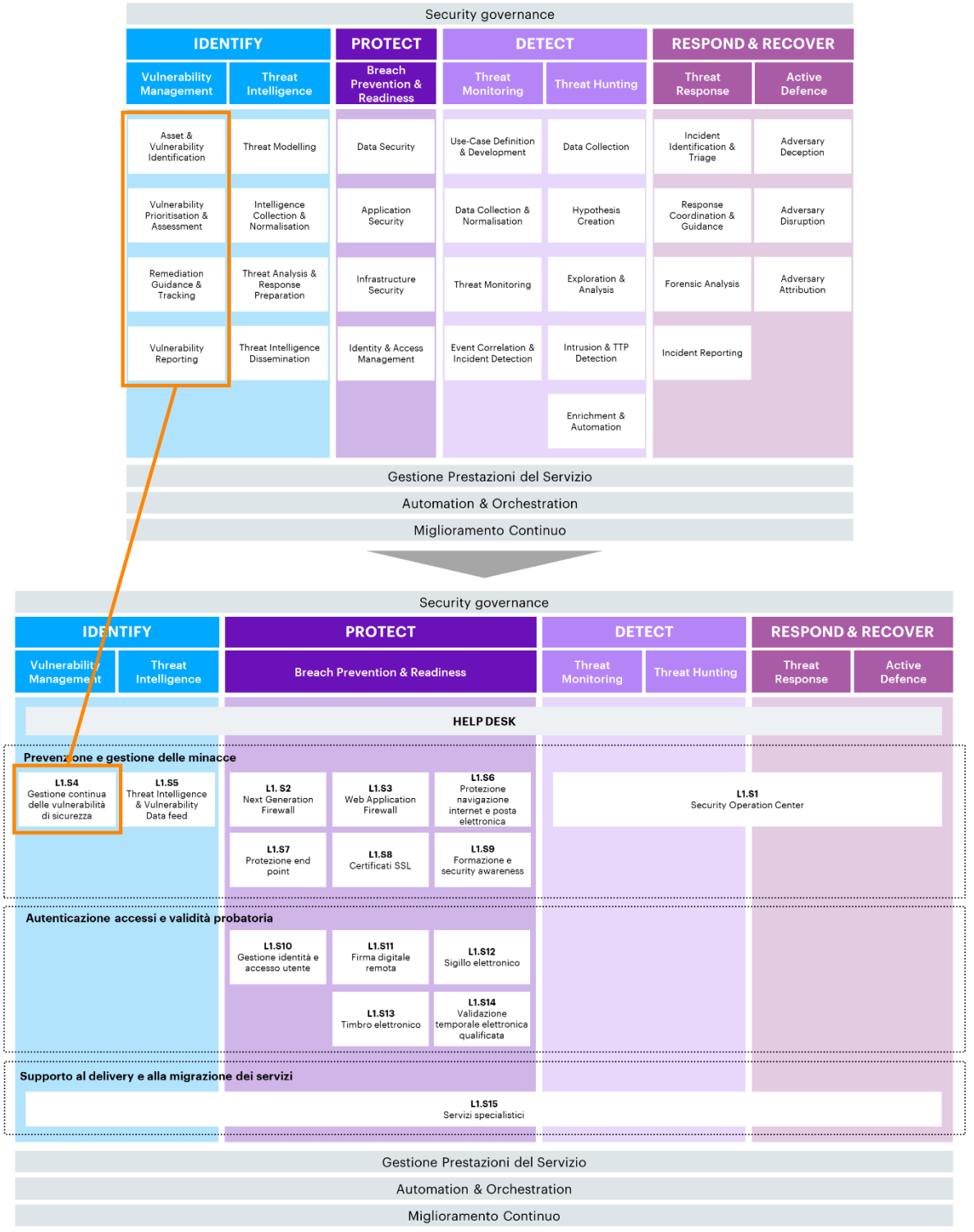


Figura 2– Aderenza tra CDOM e servizi della Fornitura

Il valore aggiunto della metodologia proposta è dato dalla disponibilità di linee guida, processi, esempi e template organizzati gerarchicamente secondo tre livelli: 1. **Framework dei servizi di sicurezza** (cfr. fig. 3): costituisce la rappresentazione di alto livello della metodologia, che esprime l'articolazione della stessa in 4 macro funzioni (es. in figura "*Identify* "), 7 domini di sicurezza, che costituiscono il focus di "Cosa" si deve fare per la metodologia in esame in riferimento a uno specifico servizio (es. "*Vulnerability Management*") e 28 sotto-servizi, che costituiscono il focus di "Come" si deve operare in riferimento a uno specifico servizio (es "*Asset & Vulnerability Identification*"); 2. **Caratteristiche dei servizi**: raccolta di Libreria di Procedure, Funzioni Fondamentali, Playbook, template di servizio, Architetture di riferimento, Knowledge Base, Workflow, KPI di servizio, frutto di esperienze e best practice, che mettono a disposizione un patrimonio informativo esaustivo e fondamentale per accelerare l'avvio e l'erogazione del servizio per ogni tipologia di PA. A titolo esemplificativo, la seguente figura illustra la "navigazione" all'interno del framework metodologico proposto relativamente al servizio di Vulnerability Management. 3. **Sviluppo di una caratteristica:** foglie terminali del framework che mostrano come le caratteristiche del servizio si sviluppano in attività da svolgere, loro sequenza e flussi di dati (ad es. la figura mostra lo sviluppo del flusso di lavoro del Processo di Gestione continua delle Vulnerabilità di sicurezza.

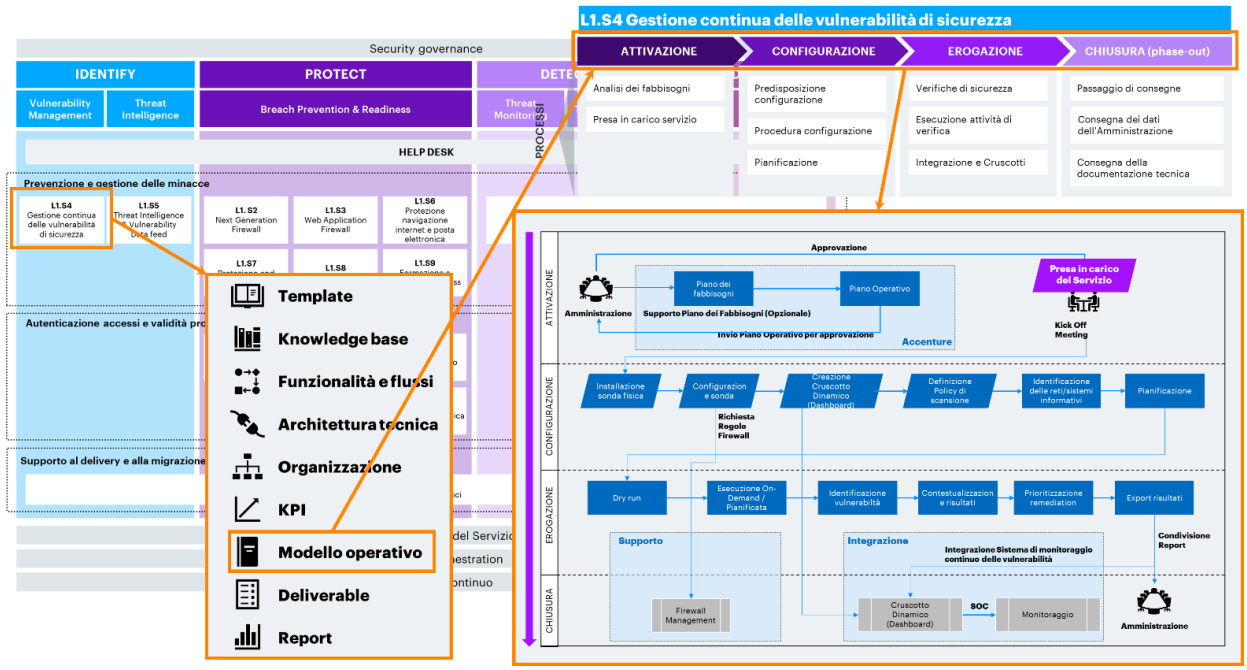


Figura 2 - Struttura e componenti del CDOM

Oltre la classificazione dei servizi, il modello CDOM fornisce una visione e guida complessiva alle interazioni tra i diversi servizi, come illustrato in figura.

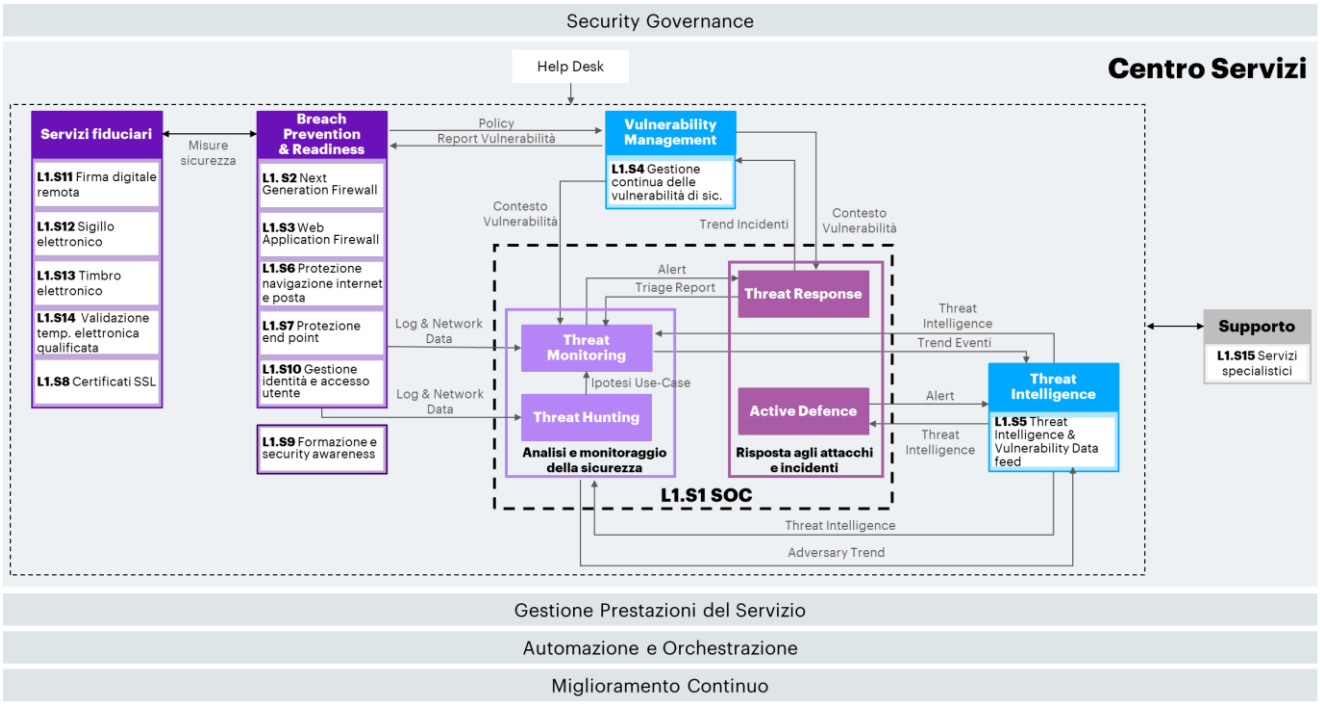


Figura 3 - CDOM - Sistema di interazioni tra i servizi

Infine, useremo il CDOM come **mappa logica di navigazione della presente relazione tecnica**, dal momento che rappresenta un utile strumento per dare evidenza degli elementi progettati a garanzia dell'omogeneità del servizio.

2 PRESENTAZIONE E DESCRIZIONE OFFERENTE

Nell'ambito dell'omonimo Gruppo internazionale, Accenture S.p.A. offre servizi di consulenza direzionale, realizzazione di sistemi e consulenza tecnologica e servizi alle imprese. Il gruppo impiega nel mondo più di 600 mila professionisti, è presente con uffici e sedi operative in più di 200 città di 51 Paesi e serve 5.000 clienti in oltre 120 Paesi nel mondo. In Italia, nell'esercizio 2020 ha sviluppato un fatturato di oltre 1,949 miliardi di Euro lavorando per oltre 300 clienti, tra i quali più di 30 clienti della Pubblica Amministrazione e gli enti di interesse pubblico (INPS, INAIL, Consip, Sogei, Ministero dell'Economia e delle Finanze, Ministero della Salute, Ministero degli Affari Esteri e della Cooperazione Internazionale, Ministero dell'Interno, Ministero dello Sviluppo Economico, AIFA, Regione Sardegna, Regione Lazio, Regione Toscana, Regione Lombardia, Roma Capitale, Poligrafico e GSE) e le più grandi aziende di tutti i settori industriali, finanziari e assicurativi (es. TIM, Vodafone, Mediaset, Unicredit, Fiat, Enel, ENI).

Accenture ritiene la Security una delle sue offerte più strategiche, sia nell'ambito dei programmi di trasformazione digitale che nell'ambito dell'erogazione dei servizi gestiti (Managed Security Services) per numerosi clienti nazionali e internazionali (es. Sogei, Senato, Min. Interno, Regione Sardegna, Comune Roma, ENEL, ENI, Intesa San Paolo, NEXI, Poste Italiane, PostePay, SNAM). L'**unità operativa Security** è la più ampia practice italiana in ambito, in grado di coprire end-to-end i servizi di sicurezza ed è riconosciuta come leader di mercato sia per i servizi di sicurezza gestiti che di consulting a livello globale e locale/europeo (Forrester, IDC). Accenture Security si avvale di:

- oltre 2.100 certificazioni professionali di processo e sicurezza (ISO27001, CISA, CISM, ISO22301, OPST, CSSLP, CRISC, CIPP, ABCP, CBCP, GCIH, GREM, GCFA, GMOB, GWAPT SSCP, CCSP, OSCP, CEH, GSEC, GCIA, GCED, GPPA, GMON, GCCC, ITIL, CISSP, etc.) e certificazioni specifiche di prodotto;
- strutture e capacità certificate in tutto il mondo (comprendenti ISO 9001, ISO 14001, ISO 20000, ISO 27001, CREST-CBEST, CMMI, CSA STAR ecc.);
- continuo investimento in acquisizioni di società specializzate in materia cybersecurity tra cui FusionX, Maglan, iDefense , Symantec, Context-IS (UK), OpenMinded (Francia) e Sentor (Svezia).

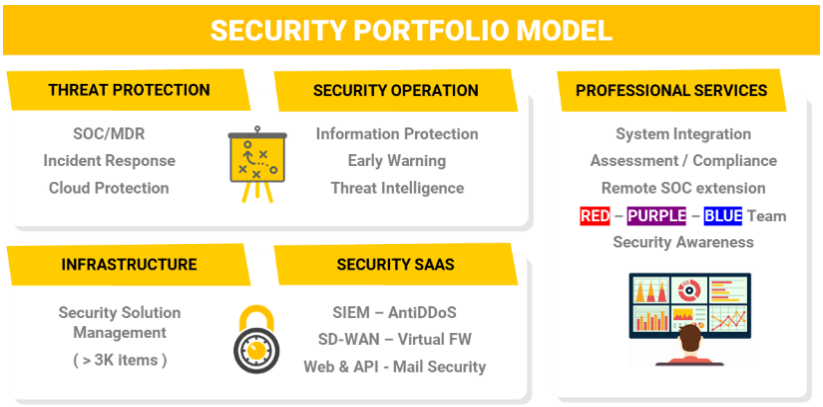
Vendor	Livello di Partnership (selezione)
Symantec	Platinum Global System Integrator
TrendMicro	Gold Reseller
Fortinet	Global Partner
CISCO	Gold Certified Cisco Channel Partner
Splunk	Elite Reseller, Managed Services, System Integrator
CyberArk	Advanced Reseller
SAP	SAP Service Partner Global VAR Platinum Level
RSA	System Integrator
IBM	IBM Platinum Business Partner
Palo Alto	Global System Integrator Partner
Microsoft	Gold Globally Recognized Partner
Oracle	Platinum Partner Global Cloud Elite
Citrix	Citrix System Integrator
ServiceNow	Global Strategic Partner
Suse	SUSE Accredited Partner
HPE	Global SI Alliance Partner
Netapp	Global System Integrator
Veritas	Veritas Platinum Tier partner

Accenture può vantare una vasta serie di alleanze e **partnership** strategiche con i principali Vendor in ambito sicurezza, volte a massimizzare la qualità dei servizi offerti pur mantenendo comunque un profilo indipendente e un insieme di asset, metodologie, framework e strumenti proprietari che consentono di garantire coerenza, uniformità ed efficacia alla gestione dell'intera Fornitura.

Fastweb, con più di 2,7 milioni di clienti (di cui 1,6 milioni collegati in tecnologie ultrabroadband, in crescita del 23% rispetto allo scorso anno), è uno dei principali operatori di telecomunicazioni in Italia. Parte del gruppo Swisscom dal settembre 2007, Fastweb offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese. Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultra-larga. Con un investimento di oltre 10 miliardi di euro, ha realizzato una rete in fibra ottica di nuova generazione che raggiunge ad oggi 55.500 km di tracciato, con oltre 4.000.000 di km di fibra (la più estesa d'Europa). Grazie all'espansione e al continuo potenziamento della rete ultra-broadband, Fastweb raggiunge oggi 22 milioni di abitazioni, di cui 8 con rete proprietaria, con velocità di collegamento fino a 1 Gigabit. La società offre inoltre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G, 4G Plus e 5G. Dall'ultimo osservatorio AGCOM, Fastweb è risultata essere leader per l'offerta di servizi con prestazioni superiori a 100 Mb/s con il 37,7% del mercato e primo operatore alternativo nel segmento dei grandi clienti pubblici e privati. Fastweb, inoltre, secondo l'indagine realizzata dall'Istituto Tedesco di Qualità e Finanza in cooperazione con l'Università Goethe di Francoforte, è il miglior operatore in Italia per il servizio di connessione in fibra ottica Ftth (Fiber to the home) ed è risultata tra le aziende "Top" anche per il servizio di connessione ADSL. Contestualmente all'infrastruttura di rete, Fastweb ha sviluppato un'infrastruttura IT di eccellenza, attraverso Data Center di proprietà distribuiti sul territorio nazionale, che permettono di erogare i più avanzati e complessi servizi a valore aggiunto. Fastweb è stata inoltre la prima Azienda in Italia a dotarsi di un Data Center certificato TIER IV dall'UpTime Institute di New York, l'ente che valuta l'affidabilità e la continuità del servizio e delle architetture di ridondanza dei Data Center in tutto il mondo. Il **nuovo Data Center** di Milano è in grado di garantire la massima sicurezza per i dati delle Aziende Clienti ed è **integrato con il SOC (Security Operation Center)**, il centro di prevenzione dagli attacchi informatici costituito interamente da personale Fastweb altamente qualificato e operante 24 ore su 24 su 365 giorni. Grazie alle proprie infrastrutture, Fastweb dispone, quindi, di una gamma completa ed integrata di servizi TLC e ICT avanzati, come l'housing, il Cloud computing, la sicurezza e la comunicazione unificata, in grado di soddisfare le esigenze di tutti i segmenti di mercato e di Aziende di tutte le dimensioni, dalle start-up alle piccole e medie imprese, dalle società di

grandi dimensioni fino al settore pubblico.

In ambito ICT, Fastweb ha recentemente acquisito Cutaway, società specializzata in progetti ICT, con l'obiettivo di rafforzare il proprio posizionamento di fornitore di servizi Cloud nel mercato Enterprise e proseguendo nella strategia di costante rafforzamento dell'offerta di Cyber Security ha acquisito una quota del 70% di 7Layers, società leader nei servizi per la sicurezza informatica inserita, dal 2017 al 2020, dal Financial Times nella classifica delle 1000 "fastest-growing companies" a livello Europeo. Nel segmento Enterprise, Fastweb è riconosciuta come fornitore d'eccellenza per affidabilità e competitività dei servizi ed è il primo fornitore della Pubblica Amministrazione in Italia, potendo vantare la presenza in una pluralità di enti della Pubblica Amministrazione Centrale e Locale essendo aggiudicataria di numerose Convenzioni e Accordi Quadro quali ad esempio, **SPC Cloud L2**, SPC 2 Connettività, SGM, Infrastrutture Condivise SPC, TF5, CT5, AQ DTO3, AQ System Management.



Fincantieri NexTech S.p.A. è una società tecnologica, appartenente al Gruppo Fincantieri, che opera principalmente per lo sviluppo di soluzioni nei settori della sicurezza e della protezione di informazione, rappresentando il **centro di competenza tecnologico del Gruppo Fincantieri**. Fincantieri NexTech, grazie alle esperienze maturate nel settore militare e della sicurezza, alle competenze specifiche nell'analisi degli scenari operativi e alla capacità di realizzare dei sistemi complessi operanti in "ambienti ostili", è in grado di supportare lo sviluppo e l'integrazione sia di soluzioni "Legacy" che di infrastrutture di campo sia su piattaforme software tradizionali (SCADA) che con l'architettura SOA (Service Oriented Architecture) ed erogare servizi di SOC, le cui competenze e la territorialità gli permettono di erogare servizi di monitoraggio di sicurezza sia da remoto sia nella sede del cliente di primo e di secondo livello. Rappresenta una realtà di eccellenza tutta italiana capace di offrire prodotti e servizi nel campo dell'elettronica, della sistemistica avanzata, dell'Information Technology e della Cyber Security.

Difesa e Analisi Sistemi S.p.A. (DEAS) è una PMI innovativa specializzata in Cyber Security e AI, in grado di fornire soluzioni tecnologiche con gli standard più alti del settore in ambito sicurezza informatica, intelligenza artificiale, GDPR, modelli di governance, soluzioni di continuità operativa. DEAS collabora con Grandi Aziende (Autostrade per l'Italia), Istituti bancari e Pubbliche Amministrazioni Centrali (Consip, Sogei, Agenzia delle Entrate, Ministero della Difesa, Camera dei Deputati, Senato della Repubblica, ISTAT, ecc.) e Locali (Regione Lazio, LazioCrea, ULSS).

[redacted]

Distribuzione dei servizi/attività tra le aziende partecipanti

La tabella riporta la distribuzione dei servizi/attività tra le aziende del RTI, secondo la notazione RACI; la A di Accountable non è stata inserita in quanto per definizione è sempre in capo alla mandataria e neanche la I di Informed in quanto pervasiva su tutte le aziende/servizi. La R indica Responsabilità ed esecuzione delle attività, mentre la C designa la collaborazione.

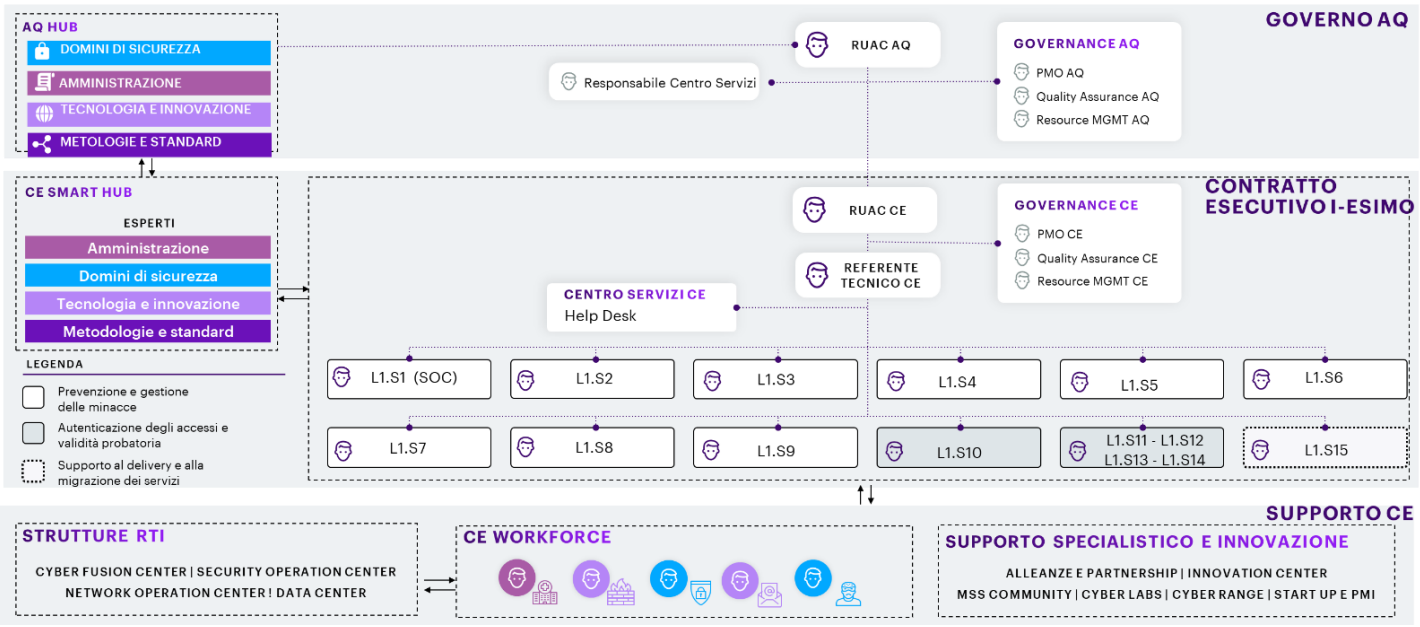
Servizi	Accenture	Fastweb	Fincantieri	DEAS
Governo della fornitura	R	C	C	C
Centri Servizi	R	R	C	C
Help Desk	R	C	C	C
Security Operation Center	R	R	C	C
Next Generation Firewall e Web Application Firewall	C	R	C	C
Gestione continua delle vulnerabilità di sicurezza	R	C	C	C
Threat Intelligence & Vulnerability Data Feed	R	C	C	C
Protezione navigazione Internet e Posta elettronica	C	R	C	C
Protezione end point	C	R	C	C
Certificati SSL e servizi di Validità Probatoria	R	C	C	C
Formazione e security awareness	R	C	C	C
Gestione dell'identità e l'accesso utente	R	C	C	C
Servizi specialistici	R	R	C	C

3 STRUTTURA ORGANIZZATIVA

La nostra proposta organizzativa è stata progettata per governare e indirizzare l'affidamento, nell'ambito del Lotto 1, dei **servizi di Sicurezza da remoto** delle PA. Si tratta di un contesto altamente critico e in continua evoluzione, rispetto al quale siamo in grado di garantire sia **continuità** dei servizi già previsti nella precedente iniziativa SPC Cloud L2 sia **approcci e tecnologie innovative** con l'obiettivo di migliorare la **resilienza delle PA contro le minacce informatiche**. L'organizzazione proposta **consolida** il meglio sia di quanto applicato per la **PA**, in particolare da Accenture e Fastweb, su altri Accordi Quadro Consip (compreso SPC Cloud L2) sia l'esperienza specifica in ambito **sicurezza** di grandi e complesse forniture realizzate per **clienti privati e infrastrutture critiche del Paese** (es. banche e servizi finanziari, telecomunicazioni, operatori energetici di produzione, trasmissione e distribuzione, infrastrutture e trasporti). L'organizzazione di seguito illustrata è reattiva e agile, e permette di gestire in maniera flessibile e scalabile l'erogazione dei servizi in base alle specifiche esigenze; è tale da 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.

3.1 Modalità Organizzative e Organigramma

Il modello proposto si articola sui tre livelli rappresentati in figura:



- **Livello di Governo dell'AQ -** rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera Fornitura. Come anticipato, Accenture e Fastweb vantano una pluriennale esperienza di successo nella gestione di Accordi e Contratti Quadro di dimensioni e complessità analoghe al presente AQ, esperienza che ha consentito di raggiungere **livelli di eccellenza** sia nella capacità di **scalare rapidamente** in funzione delle richieste delle PA sia nella **capillarità** di presenza sul territorio nazionale, come dettagliato al §3.2. Ad esempio, **Accenture** nell'ambito di AQ/CQ di cui è stata assegnataria, è giunta ad erogare **62 contratti** in parallelo (anche di grandi dimensioni) con l'impegno di circa 1400 professionisti, e **Fastweb,** nell'ambito dei diversi AQ/CQ già citati in Premessa**,** nel periodo 2017-2021 ha operato su **circa di 6.800 CE**, ripartiti tra **PAC** e **PAL**. Per gli elementi concreti in termini di infrastrutture e risorse a dimostrazione di tale scalabilità e capillarità si rimanda ai dettagli forniti al §3.2. Il livello di Governo AQ 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 nostre aziende e dal **Responsabile del Centro Servizi** (per la cui organizzazione si rimanda al §4), 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 (cfr. §3.3).
- **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, ✓supporto specialistico e innovazione. **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** (cfr. §4), 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:** comprende: ✓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, 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 si rimanda al §17.

- **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. La forza degli HUB è quella di offrire un supporto qualificato e innovativo avvalendosi del network nazionale e internazionale garantito dalle aziende del RTI. Di seguito la loro descrizione.

Competenze a disposizione dell'Accordo Quadro e del Contratto Esecutivo

Gli HUB AQ e CE forniscono il supporto di esperti per rafforzare le competenze e le metodologie possedute dai team. L'AQ HUB opera trasversalmente su tutti i CE per garantire: ✓un livello di qualità dei servizi di sicurezza erogati elevato e uniforme, ✓la diffusione dell'innovazione, ✓il corretto riuso e l'omogeneità di approccio. L'Hub è strutturato in 4 ambiti di competenza identici a livello di AQ e di CE: **Domini di Sicurezza (DS), Amministrazione (AMM), Tecnologie e Innovazione (T&I), Metodologie e Standard (M&S)** con i seguenti compiti.

Ambito	Competenze e asset messi a disposizione della Fornitura
DS	Garantire l'omogeneità di erogazione dei servizi per **dominio/servizio** oggetto dell'AQ, fornendo una guida ai team di erogazione servizi. Infatti, ciascun servizio avrà, nell'AQ HUB, un **Referente di Dominio**, individuato come la persona del RTI con maggiore esperienza sullo specifico servizio. Oltre la **garanzia di uniformità e qualità** tra i diversi CE, tali referenti hanno l'importante ruolo di contribuire al **veloce avvio dei servizi**: fin dalla definizione dei fabbisogni lavorano alla configurazione del servizio avvalendosi ✓sia degli **standard tecnologici e procedurali** del Centro Servizi (cfr. anche il ruolo del modello CDOM ai §§1 e 3.3, modello rispetto a quale i Referenti di Dominio **assicurano aderenza** in ogni CE) ✓sia dei "**Managed Security Twin**", vale a dire configurazioni di servizio già applicate in realtà analoghe (per questo "gemelle") e raccolte anche per diffondere lessons learned, best practice e conoscenza messi a punto nel corso dell'AQ. Si sottolinea in particolare che, per la rilevanza del SOC, è previsto un ruolo di **Referente del Security Operation Center** che si occuperà anche di supportare le PA, in maniera uniforme, nel processo di notifica verso le Autorità Competenti (CSIRT Italia, Garante Privacy) in caso di rilevamento di incidenti di sicurezza e per il continuo miglioramento del servizio erogato.
AMM	Ascoltare le esigenze delle PAL o PAC e degli utenti finali, facilitare il confronto tra di esse, pubblicizzare i casi di successo per stimolare l'adesione all'AQ, favorire la cooperazione e la resilienza della macchina amministrativa, analizzare i fabbisogni e garantire la realizzazione di proposte innovative. L'ambito AMM, grazie alla conoscenza di contesto, indirizza l'innovazione tecnologica dei servizi affinché tengano conto delle peculiarità delle PA (es. difesa e sicurezza pubblica, sanità, municipalità). Tra gli esperti in questo ambito sono selezionati primariamente i RUAC di CE sulla base del contesto specifico della PA richiedente. Rientrano in questo ambito, a livello di AQ, anche gli **Account Territoriali** (uno per Regione/Provincia Autonoma) che apportano consapevolezza delle specificità regionali e promuovono la conoscenza dell'AQ sul territorio.
T&I	Assicurare le **competenze tecnologiche** sui trend innovativi legati alla sicurezza informatica, alla protezione dei dati personali e alle tecnologie emergenti: es. *Zero Trust, Sicurezza del Cloud, Sicurezza dell'Internet of Things, Artificial Intelligence, Autonomus Identity*. Il **Referente Tecnologia e Innovazione**, figura con esperienza nel contesto pubblico per la definizione di strategie di trasformazione digitale e cyber resilienza, è il punto di riferimento per i team dei servizi CE, coordinandone gli interventi per garantire unitarietà di approccio. L'innovazione è altresì garantita anche da un ampio ecosistema con i player tecnologici leader per i diversi servizi di alleanze (es. *Splunk, PaloAlto, Fortinet, Tenable, Qualys, Symantec, Crowdstrike, TrendMicro, CyberGuru, Forgerock, Okta, Oracle, Microsoft, IBM, Check Point)* e di continue acquisizioni da parte delle aziende componenti il RTI (*Maglan, FusionX, iDefense, Symantec, 7layers, e-phors, ecc.*). Il Referente Tecnologia e Innovazione è promotore dei lavori della **Cyber Security Room** strumento operativo per veicolare l'innovazione a livello di AQ e CE, descritta al §17. Inoltre, come da una **best practice** di Fastweb, sviluppata nel CQ SPC Cloud L2, nei casi d'integrazione dei sistemi del Fornitore con sistemi della PA, viene individuato un **Technical Account Manager (TAM)** per interfacciare direttamente il vendor di riferimento e ottimizzare le soluzioni applicate e i tempi di risoluzione di eventuali incidenti.
M&S	Garantire le **competenze su standard e metodologie** utili a gestire il programma nella sua interezza. Gli esperti Metodologie e Standard sono espressione di due diverse attività: 1) **continuo aggiornamento e recepimento** rispetto al panorama normativo e metodologico di riferimento, 2) **contributo diretto** alla definizione di linee guida, standard e best practice a livello nazionale e internazionale. **CONTINUO AGGIORNAMENTO E RECEPIMENTO** - Le aziende del RTI seguono un **processo strutturato di Aggiornamento e Recepimento** che garantisce alle PA sia la tempestiva individuazione di novità/aggiornamenti a livello nazionale e internazionale sia la proattività del RTI nel proporre soluzioni per il recepimento. Ad esempio, il perimetro di monitoraggio comprende: ✓Metodologie di riferimento su Modelli Operativi ✓Procedure per la erogazione dei Servizi e standard di sicurezza ✓Norme e Standard di Sicurezza per l'Accesso ai Dati Personali ✓Norme e Standard di Sicurezza per i servizi essenziali. **CONTRIBUTO DIRETTO** - ✓**Accenture** contribuisce direttamente alla definizione di linee guida, standard e best practice a livello internazionale (es NERC-CIP) e nazionale (es. a supporto del CERTFin); ha inoltre attivato collaborazioni con le primarie istituzioni, enti di ricerca e osservatori italiani in ambito cyber security tra cui il Politecnico di Milano, l'Associazione Bancaria Italiana (ABI), il Ministero innovazione tecnologica e transizione digitale (MITD), l'Agenzia per l'Italia Digitale (AgID); infine partecipa attivamente **principali osservatori e forum mondiali di settore** (es. WEF, FS-ISAC, ECSO come membro fondatore, etc)

✓**Fastweb** è l'unico operatore nazionale di TLC a contribuire attivamente con le proprie analisi al rapporto annuale CLUSIT sulla Sicurezza ICT in Italia (basata su oltre 35 milioni di eventi di sicurezza individuati) e collabora con l'Osservatorio Cybersecurity & Data Protection, promosso dalla School of Management del Politecnico di Milano; ✓**Fincantieri** partecipa attivamente al programma ECHO, tra le soluzioni studiate nel progetto si possono annoverare il quadro di valutazione multisettoriale, il sistema di allarme precoce, la federazione di Cyber Ranges, le roadmap tecnologiche intersettoriali, il Cyber Skills Framework e uno schema di certificazione della sicurezza informatica.

il Raggruppamento si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, almeno nella misura del **35,01%**.

3.2 Distribuzione delle responsabilità RTI

Con il nostro RTI mettiamo a disposizione della PA una **straordinaria complementarità**, fondata su 4 pilastri di eccellenza: ✓un player di **consulenza e tecnologia** a livello nazionale e internazionale ✓un primario operatore delle telecomunicazioni, protagonista di **grandi progetti infrastrutturali** ✓il primo gruppo italiano operante nei **settori difesa e sicurezza** ✓una PMI innovativa specializzata in **Cyber Security e AI** già apprezzata nel settore pubblico. Offriamo tra queste aziende una fote **sinergia** per realizzare una proposta efficace, efficiente e di qualità dei servizi offerti attraverso le **tre direttrici** di **continuità, evoluzione e innovazione**.

Continuità

Fastweb: ✓è uno dei principali interlocutori della PA nell'ambito della Cyber-sicurezza grazie alla titolarità di convenzioni come **SPC 2 Connettività** e **Contratto Quadro SPC Cloud L2**, ✓è fornitore ufficiale della PA da ben **15 anni** (SPC1/TF3 del 2006) con più di 5000 contratti attivati, ✓ha sviluppato un'**infrastruttura IT di eccellenza**, attraverso Data Center di proprietà distribuiti sul territorio nazionale, garantendo la connettività di rete SPC richiesta dalla fornitura, nonché tutti i servizi infrastrutturali che sottendono l'erogazione da remoto dal Centro Servizi del RTI, ✓ha profonda **penetrazione nel mercato PA**. A titolo esemplificativo citiamo: ✓convenzione SGM - gestiti circa 1.000.000 di apparati e 400.000 ticket nel 2019, di cui ca. 50.000 analoghi a quelli di cui al presente AQ; ✓SPC Cloud L2 - circa 30 contratti PAC e 100 PAL; ✓SPC 2 Connettività - oltre 300 PA servite su ca. 16.000 sedi).

Accenture: ✓l'unità operativa Security segue gli aspetti di sicurezza per tutti gli AQ e CQ di cui Accenture è titolare con servizi dedicati; la conoscenza riguarda più di **30 Amministrazioni Centrali** (Sogei, Min. Interno, Senato, Min. Esteri, Min. Salute, ecc.), con grande eterogeneità funzionale e dimensionale, nonché **PAL** quali Comuni di Roma e Milano, Regioni Lombardia e Sardegna; ✓è primo fornitore di servizi di sicurezza e Managed Security Services per le più importanti infrastrutture critiche del Paese, come istituti finanziari, assicurativi, operatori energetici e di telecomunicazioni operanti nel Perimetro di Sicurezza Nazionale (tra gli operatori italiani: i **6** principali istituti finanziari tra cui Intesa Sanpaolo e NEXI, i **6** principali operatori del settore energetico, oil & gas, tra cui ENI, ENEL e SNAM, **5** tra le principali aziende manufatturiere, **3** tra le principali aziende di telecomunicazioni, tra cui TIM) nonché per primari Enti della PA Centrale.

Fincantieri e **DEAS**: mettono a disposizione la loro esperienza di erogazione di servizi di Sicurezza in particolare per il **settore Difesa**.

Evoluzione

Accenture: ✓è il **più grande operatore mondiale e italiano di servizi di cyber security**, con 9.000 professionisti dedicati e oltre 1000 in Italia; ✓vanta un'offerta e una **copertura end to end in tutti i domini della sicurezza informatica**; ✓ha realizzato un modello operativo specifico per i servizi di sicurezza, il **CDOM descritto in Premessa e al §3.3**, che si **adatta perfettamente** al contesto di gara e alle esigenze delle diverse PA ✓è il **primo partner** di tutti i maggiori vendor di tecnologia in ambito Sicurezza, utili anche a valorizzare le tecnologie in uso presso le PA ✓ha **più di 500 asset proprietari**, **più di 400 brevetti** in ambito sicurezza e più di 15 acquisizioni di società specializzate in ambito cyber negli ultimi 5 anni (es. Maglan, iDefense, Symantec, FusionX), ✓opera per promuovere la security community nazionale di formazione e divulgazione per CISO, CRO e i principali stakeholder in ambito.

Fastweb: ✓è uno dei principali MSSP (Managed Security Service Provider) che eroga già servizi di sicurezza attraverso il suo Security Operation Center a numerose PA centrali e locali; ✓grazie alla sua **capillare distribuzione** sul territorio e la sua **catena logistica** consente una piena copertura delle potenziali esigenze di supporto richieste dalle PA; ✓è coadiuvato e supportato dal competence center e dall'osservatorio di sicurezza che si avvalgono di partnership consolidate con i maggiori player e vendor.

Fincantieri: ✓mette a disposizione esperienze e progetti per sviluppare la difesa cibernetica delle infrastrutture critiche nazionali (es. porti).

In particolare, ai fini dell'analisi delle minacce informatiche, garantiamo l'**accesso alle informazioni di molteplici e variegati sorgenti, di livello nazionale e internazionale**, per abilitare le successive attività di **elaborazione e correlazione** e per **proporre** alle PA le azioni di contrasto e mitigazione più opportune.

Innovazione

Vantiamo una rete di **più di 30 centri di eccellenza** - tra cui centri di Ricerca e Sviluppo (Cyber Labs e Innovation Center), Cyber Range (Poligoni Cibernetici), Delivery Center e Cyber Fusion Center - da cui vengono erogati i servizi di sicurezza gestiti (Managed Security Services) in uno spazio di lavoro immersivo e dove collaboriamo anche per sviluppare nuove soluzioni, tecniche e strumenti per prevenire e gestire le minacce informatiche. Per dettagli sulle strutture messe a disposizione per l'innovazione si rimanda al §17.

Le sinergie tra le aziende sono assicurate dal **Comitato di coordinamento del RTI**, per garantire il massimo sostegno alle iniziative dell'AQ. Il Comitato – per semplicità espositiva non riportato nella figura rappresentante la struttura organizzativa - è composto da dirigenti delegati delle aziende coinvolte, dal RUAC AQ e dai RUAC e dai Referenti Tecnici dei più rilevanti CE in corso.

La modalità operativa proposta consente al team di AQ di: ✓adattarsi alle esigenze delle diverse tipologie di PA in termini di tematiche, tecnologie, evoluzioni progettuali e dimensioni, grazie all'impiego di esperti a livello di AQ che, intercettando in anticipo i potenziali fabbisogni, di concerto con i team di Resource Management, agilmente identificano le strutture più adatte da coinvolgere per la creazione dei CE ✓valorizzare il contributo delle diverse realtà aziendali a copertura

di tutte le competenze necessarie, grazie ad un approccio proattivo che cura lo sviluppo continuo degli skill in base alle esigenze previste o espresse.

La seguente tabella mostra la **ripartizione delle responsabilità** delle Aziende in RTI, considerando che Accenture, quale mandataria del RTI, esprime il ruolo di responsabile unica del risultato per l'AQ, assicurando trasversalmente il governo, il coordinamento e la qualità dell'iniziativa; contestualmente si esalta la complementarità delle competenze, che guidano l'assegnazione dei task di servizio, assegnandone la responsabilità (R) all'azienda più esperta per quella competenza.

Servizi	Accenture SC	Accenture MSS	Fastweb DC	Fastweb CC	Fincantieri	DEAS
Governo della fornitura	R	C	C	C	C	C
Centri Servizi	C	R	R	C	C	C
Help Desk	C	R	C	C	C	C
Security Operation Center	C	R	C	R	C	C
Next Generation Firewall e Web Application Firewall	C	C	C	R	C	C
Gestione continua delle vulnerabilità di sicurezza	C	R	C	C	C	C
Threat Intelligence & Vulnerability Data Feed	C	R	C	C	C	C
Protezione navigazione Internet e Posta elettronica	C	C	C	R	C	C
Protezione end point	C	C	C	R	C	C
Certificati SSL e servizi di Validità Probatoria	C	R	C	C	C	C
Formazione e security awareness	R	C	C	C	C	C
Gestione dell'identità e l'accesso utente	C	R	C	C	C	C
Servizi specialistici	R	C	C	R	C	C

Legenda: R=Responsabile dell'attività – C=Collaboratore | Accenture SC – U.O. di Security Consulting; Accenture MSS – U.O. di Managed Security Services; Fastweb DC – U.O. responsabile dei centri servizi e dei Data Center; Fastweb CC – U.O. Centro di Competenza Security

3.3 Aderenza al contesto e coerenza generale dei ruoli, risorse e strutture aggiuntivi proposti e interazioni con l'Amministrazione

Aderenza al contesto

Garantiamo la migliore combinazione in termini di **modello operativo**, **competenze tecniche** del personale, aspetti **organizzativi** e **logistici** per rispondere completamente alle esigenze espresse nel capitolato. Il fattore unificante per l'erogazione dei servizi è il **modello operativo CDOM** (cfr. Premessa) che **copre tutti i servizi richiesti**. Il CDOM offre un linguaggio e una modalità operativa standardizzata e comune per tutto il personale di Fornitura. In figura riportiamo i domini del modello CDOM da cui i servizi attingeranno i modelli organizzativi, operativi, di reporting, i processi, i casi d'uso e la knowledge base utili per: ✓una **rapida messa in opera abilitata da veri e propri "template di servizio"**; ✓un'**erogazione uniforme in termini di qualità e standard** (per i dettagli si rimanda ai §§ da 6 a 14). Il CDOM, concepito sulla base di riconosciuti standard e best practice di settore (NIST, ISO27001, ISO22301, ISO31000, ITIL, etc.) è allineato alle normative vigenti (eIDAS, NIS, GDPR, ecc.). CDOM è stato consolidato ed evoluto nel corso del tempo sulla base delle esperienze maturate in contesti di complessità analoga a quelle delle PA future contraenti (es. Intesa Sanpaolo, Unicredit, ENI, ENEL, NEXI, SNAM) e arricchito e integrato dalle competenze verticali ed esperienze di Accenture, Fastweb, Fincantieri e DEAS nella PA (es. Mini. Interno, Stato Maggiore Difesa, Senato, Sogei, INPS, INAIL, ISTAT, Regioni Sardegna, Lombardia, Liguria, nonché Governo U.S.A, Governo U.K.).

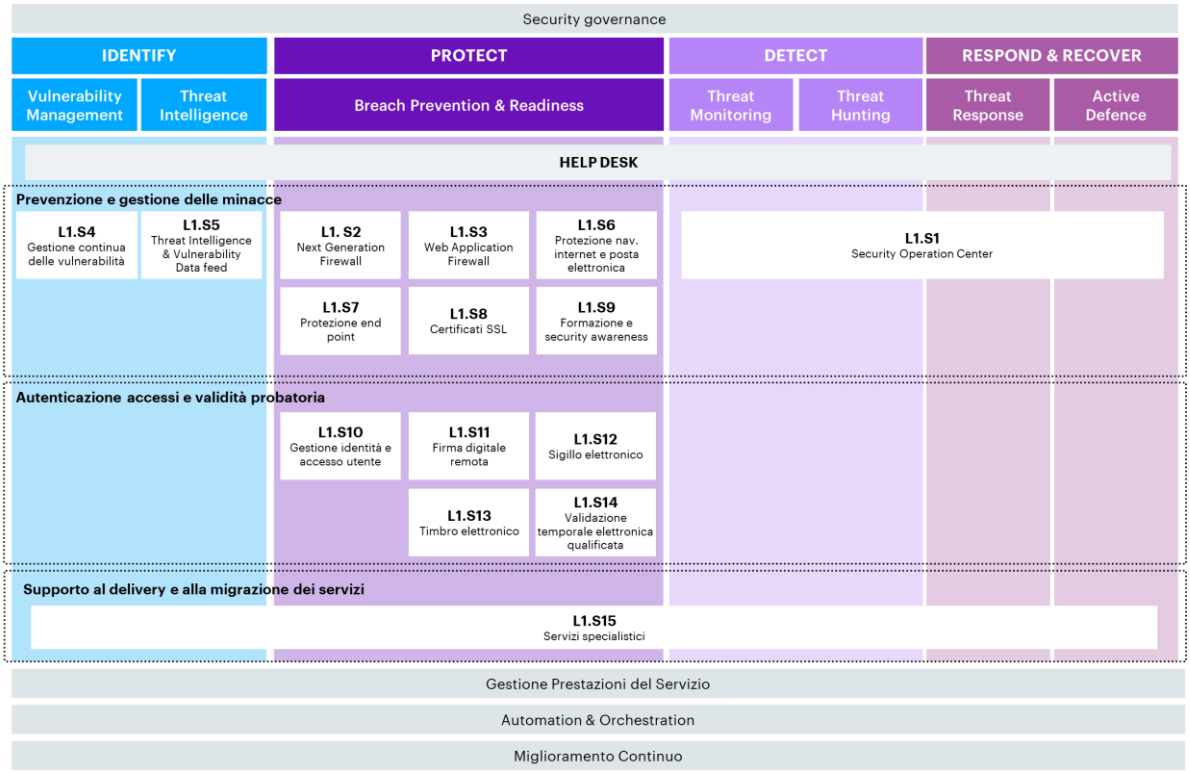
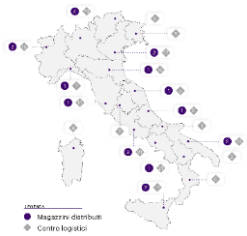


Figura 4 - CDOM

Competenze tecniche: ✓La mandataria Accenture ha nell'unità operativa Security una delle aree più strategiche della società in termini di programmi di trasformazione e servizi di sicurezza per i propri clienti in tutto il mondo; ✓Fastweb è riconosciuta come fornitore d'eccellenza per affidabilità e competitività dei servizi ed è il primo fornitore della PA in Italia; ✓Fincantieri e DEAS puntano proprio sull'innovazione tecnologica e una verticalizzazione in ambito difesa. In questo quadro le competenze tecniche sono il volano essenziale per offrire servizi di qualità; le aziende del RTI investono continuativamente in **formazione specialistica di settore** e i professionisti messi a disposizione dell'AQ hanno conseguito **più di 2.100 certificazioni** di processo e sicurezza (tra cui ISO 27001, ISO 22301, CISSP, CISM, CRISC, CEH, CSSLP, MBCP) e specifiche di prodotto (Splunk, IBM QRadar, Fortinet, PaloAlto, Oracle, FireEye, McAfee, Cisco, ecc.); inoltre DEAS dispone di un LVS (Laboratorio Valutazione Sicurezza) con **valutatori certificati** OCSI (Organismo di Certificazione della Sicurezza Informatica). Queste competenze sono poi **potenziate**

dal ricorso al ricco network di strutture del Supporto Specialistico e Innovazione, illustrato al §3.1.



Organizzazione e Logistica: garantiamo una **copertura completa** sul tutto il territorio nazionale, potendo vantare più di 40 tra **sedi** e **uffici in Italia,** e **una catena logistica con oltre 20 Centri Logistici e 168 Magazzini Distribuiti** e **personale distribuito** che consentono di fornire assistenza e servizi anche di prossimità in maniera **capillare** sia per la PAL che per la PAC (cfr. §2).

Ruoli, risorse e strutture aggiuntivi proposti per la gestione della fornitura e le modalità di interazione con l'Amministrazione

Per definire l'approccio generale di coordinamento e le modalità di interazione con le PA adottiamo l'Accenture Delivery Methods Program e Portfolio Management (ADM-PPM), il modello operativo proprietario coerente con le indicazioni del PMI, che raccoglie in una visione dinamica l'applicazione delle classiche aree di project management: ✓Strategia, Governo e Pianificazione; ✓Risorse e competenze; ✓Attività; ✓Rischio e Qualità; ✓Risultati. Di seguito, le fasi del modello con evidenza di azioni di Coordinamento e Interazione con PA e attori coinvolti.

1-PREDISPOSIZIONE/AGGIORNAMENTO RISORSE E STRUMENTI: la struttura del Resource Management, in collaborazione con l'AQ Hub, seleziona le risorse con le competenze più adeguate alle esigenze delle PA. La selezione è guidata dall'analisi del Piano dei Fabbisogni nonché dalla nostra esperienza in altri AQ/CQ. **2-PROMOZIONE AQ:** le risorse degli AQ HUB promuovono in modalità proattiva l'AQ tramite iniziative realizzate per lo più sul Portale della Fornitura, così da raggiungere il maggior numero di PA, cui si aggiungono le azioni di divulgazione della conoscenza dello strumento di AQ svolte sul territorio dai nostri Account Territoriali. **3-PREPARAZIONE CE:** la struttura del PMO AQ coordina le azioni per accompagnare le PA dal primo contatto fino alla stipula dei CE, avvalendosi anche di risorse provenienti dalle aziende del RTI per fornire consulenti esperti dei bisogni della specifica PA e in grado di anticiparne le necessità. Contattabile dal Portale, utilizza anche gli strumenti di collaboration per interagire con le PA. **4-ESECUZIONE CE:** fase operativa in cui sono erogati i servizi: ✓il Team di PMO CE coordina le attività di Project/Program Management e di Risk Management; ✓il Resource Manager e CE Smart Hub garantiscono lo staffing del CE con risorse del CE Workforce eventualmente integrate con PMI/start up/CdC; ✓i Responsabili Tecnici dei Servizi coordinano le attività richieste. **5-CONTROLLO E MONITORAGGIO:** le attività in esecuzione sono monitorate al fine di individuare criticità, attivare contromisure opportune e rendicontare ai Referenti della PA l'andamento dei servizi. In tale fase sono coinvolti i Responsabili Tecnici dei servizi nonché la struttura centrale di Governance CE, che forniscono supporto nella verifica degli SLA contrattuali e degli indicatori di digitalizzazione. **6-CHIUSURA FORMALE INTERVENTI E CE:** fase finale degli interventi/CE in cui si effettuano le verifiche formali del rispetto degli obblighi contrattuali. La struttura centrale di Governance CE aggiorna, inoltre, i dati a livello di AQ anche per consentire il controllo da parte degli Organismi di Coordinamento e Controllo. **7-CONDIVISIONE LESSONS LEARNED:** si opera per ✓condividere la conoscenza maturata sugli scenari di sicurezza delle singole PA, ✓analizzare situazioni di criticità e misure correttive adottate, ✓verificare l'opportunità di attività formative interne al RTI; protagonisti sono le strutture dell'AQ Hub e del Resource Management.

Inoltre, e come anticipato al §3.1, a livello organizzativo il **RUAC AQ** presiede il **Comitato di Coordinamento del RTI** per definire la strategia di business e assicurare omogeneità di erogazione ai CE ed è responsabile delle interazioni con Consip e gli **Organismi di Coordinamento**; in particolare con questi ultimi, l'interazione prevede uno **stato di avanzamento periodico**, almeno trimestrale, su: risultati raggiunti dalle forniture in corso, andamento dei contratti e attività di supporto alle PA. Di seguito un riepilogo di ruoli, risorse e strutture **aggiuntivi**.

Ruoli, risorse e strutture aggiuntivi	Descrizione
HUB di AQ e CE SMART HUB	Si rimanda per la descrizione al §3.1
Project Management Office di AQ (PMO AQ) e di CE (PMO CE)	Assicura un costante monitoraggio dell'avanzamento dell'AQ e dei CE, gestendo centralmente aspetti quali la pianificazione delle attività della fornitura e delle risorse, (Program Management) e la gestione della conoscenza (Knowledge Management)
Quality Assurance AQ e CE	Assicura il rispetto dei livelli di qualità richiesti durante la fornitura (Quality Assurance) e incentiva l'utilizzo di standard e metodologie uniformi in ottica di riuso e razionalizzazione
Resource Management AQ e CE	Valuta gli skill delle nostre risorse da dedicare all'erogazione dei servizi, sotto il profilo delle competenze tematiche, funzionali, metodologiche e tecnologiche.

Per i **ruoli aggiuntivi**: **Responsabile del Centro Servizi, Referenti di Dominio, Referente del Security Operation Center, Referente Tecnologia e Innovazione, Technical Account Manager, Account Territoriali** si rimanda alle descrizioni fornite al §3.1.

4 PROPOSTA PROGETTUALE PER I "CENTRI SERVIZI"

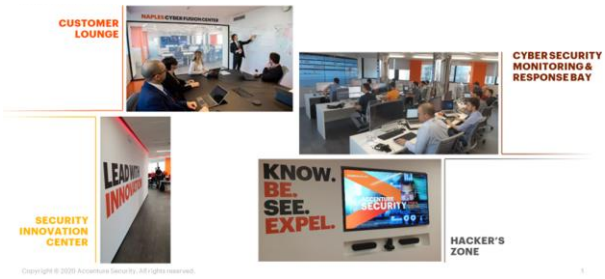
4.1 Descrizione del Centro Servizi

Il RTI eroga i servizi richiesti tramite il **Centro Servizi** che costituisce la struttura unica abilitante i servizi di fornitura e che tramite il servizio di Help Desk fornisce un punto unico di contatto alle PA. Il Centro Servizi (CS) si compone delle singole sedi operative appartenenti alle nostre Aziende che, operando in **modalità federata** e adottando **processi operativi univoci**, garantiscono l'erogazione di servizi (**Delivery Center**) e di gestione dei sistemi informatici (**Data Center**) secondo un modello disegnato per garantire scalabilità, performance e resilienza ad uso delle PA. Le singole sedi possono essere utilizzate da personale appartenente a ciascun componente del RTI così da rendere disponibili le migliori competenze necessarie all'erogazione dei servizi. Di seguito le sedi operative che costituiscono il CS.

Sede operativa	Tipologia	Indirizzo
Accenture Cyber Fusion Center Napoli (ACFC-N)	Delivery Center	Via Porzio, 6, 80143 Napoli (NA)
Accenture Assago (AAS)	Delivery Center	Strada 4, 4, 20089 Assago (MI)
Fastweb Caracciolo (FWCA)	Delivery Center & Data Center	Via Caracciolo, 51, 20155 Milano (MI)

Fastweb Bernina (FWB)	Data Center	Via Bernina, 6, 20158 Milano (MI)
Fastweb Omodeo (FWO)	Delivery Center	Via Adolfo Omodeo, 49, 70125 (BA)
Fastweb Polo Tiburtino (FWPT)	Data Center (Sito di Disaster Recovery)	Via Giacomo Peroni, 292, 00143 Roma (RM)

✓La sede **Accenture di Napoli** ospita il Cyber Fusion Center ovvero la struttura Accenture che concentra le attività di gestione, monitoraggio e innovazione in ambito Cyber Security. La struttura è operativa in modalità 24x7, conta su oltre 100 dipendenti specializzati e certificati sulle tecnologie da utilizzare per l'erogazione dei servizi e gestisce servizi per oltre 40 Clienti italiani ed europei. Il Cyber Fusion Center si inserisce in un network di centri presenti in tutto il mondo, dove vengono combinati servizi di sicurezza gestiti, tecnologie di automazione intelligenti e servizi integrati di difesa informatica per aiutare le organizzazioni a innovarsi e combattere il cyber-crime. Consente quindi di offrire ai nostri clienti un accesso diretto ai servizi più avanzati a livello mondiale, e allo stesso tempo, un punto di riferimento locale per la protezione del proprio business digitale. Il centro si sviluppa su una superficie di oltre 600mq e monitora oltre **224 miliardi di log** di sicurezza al giorno, gestisce **8.000 eventi** di sicurezza e oltre **200 incidenti** al giorno con grande potenziale di scalabilità. Inoltre il Centro riunisce le nostre capacità di gestione della sicurezza end-to-end, consentendo ai clienti di eseguire il monitoraggio degli eventi di sicurezza, fornisce assistenza dedicata per un'efficace gestione delle crisi attraverso l'adozione di azioni appropriate per rispondere a frodi e incidenti di sicurezza e lavora a stretto contatto con il Cliente, inviando avvisi tempestivi in caso di problemi di sicurezza e segnalando periodicamente lo stato dei servizi monitorati ✓La sede **Accenture di Assago** costituisce uno dei principali siti di delivery di Accenture a livello nazionale e ospita oltre 400 dipendenti specializzati nell'implementazione e gestione di tecnologie di sicurezza per clienti italiani ed europei. ✓La sede **Fastweb Caracciolo**, che impiega 420 dipendenti specializzati, ospita il Data Center che costituisce il sito primario di erogazione dei servizi di sicurezza grazie alla possibilità di ospitare i sistemi di elaborazione, connettività e storage in un **ambiente certificato** "**Tier IV – Constructed Facility**" dal Uptime Institute. Il Data Center è stato costruito e viene gestito con l'obiettivo di garantire il massimo livello di disponibilità dei servizi di elaborazione e connettività (garantita al 99,997%) grazie alla totale ridondanza delle infrastrutture di supporto. La sede ospita inoltre il SOC Enterprise di Fastweb, operativo in modalità 24x7 e disegnato per garantire la fornitura di Servizi Gestiti di Sicurezza alle grandi realtà Aziendali e Organizzazioni nazionali ed internazionali. ✓La sede **Fastweb Bernina** costituisce il secondo sito di erogazione dei servizi informativi ospitando i sistemi in ambienti certificati Tier III in grado di garantire una disponibilità dei servizi di elaborazione e connettività al 99,98%. ✓La sede **Fastweb Omodeo** ospita una ulteriore unità organizzativa adibita a Security Operation Center, che fornisce un presidio in h24 e costituisce un ulteriore back up alla sede Accenture di Napoli e Fastweb Caracciolo. ✓La sede **Fastweb Polo Tiburtino** costituisce il sito di Disaster Recovery per i servizi informatici, ospitando la terza copia dei dati di produzione (in aggiunta a quelle presenti a Caracciolo e Bernina) e le infrastrutture di connettività e di elaborazione necessarie alla loro messa in opera in caso di emergenza.



Il CS e, in particolare le relative sedi operative, utilizzano **servizi di connettività** garantiti da Fastweb assicurando i massimi livelli di servizio grazie a un'architettura di rete di backbone gerarchica, costantemente monitorata per verificare lo stato di occupazione di tutti i link. I collegamenti sono adeguati dinamicamente al superamento di valori di soglia rimodulati nel tempo. La **scalabilità dell'infrastruttura è stata confermata** in occasione del recente lockdown nazionale in cui Fastweb ha assorbito picchi di incremento del traffico sulla rete fino al 40% non pregiudicando la qualità del servizio erogata ai clienti sia Enterprise che Privati.

La **continuità operativa** dei servizi di elaborazione e connettività del CS è garantita dai **due Data Center Fastweb di Milano** (Caracciolo e Bernina) da cui erogare servizi basandosi sui paradigmi della virtualizzazione estesa e del Cloud Computing che, in perdita della disponibilità del sito primario, assicurano tempi di RTO e RPO prossimi allo zero. La robustezza della soluzione è ampiamente collaudata, essendo in uso da anni sui due Data Center Fastweb per l'erogazione di servizi verso enti pubblici e grandi aziende private. La soluzione proposta prevede, inoltre, il sito di **Disaster Recovery presso il Data Center Fastweb di Roma** (Polo Tiburtino) tale da garantire l'erogazione dei servizi anche a fronte di eventi catastrofici estesi che rendano indisponibili i 2 data center di Milano.

Il CS è in grado di erogare servizi in modalità sinergica tra le varie sedi operative, che già oggi operano con SLA superiori alla media di mercato e prevede, in aggiunta alla ridondanza garantita per i servizi elaborazione e connettività, anche la disponibilità di soluzioni per garantire l'operatività delle risorse in caso di **indisponibilità/inaccessibilità delle sedi operative adibite a Delivery Center**, ivi incluso il Cyber Fusion Center di Napoli. In tal senso, ogni sede è dotata di sistemi di connettività e alimentazione ridondati e ogni servizio viene erogato da almeno 2 sedi distinte come riportato in tabella.

A ulteriore garanzia del livello di sicurezza e di qualità del CS si riportano di

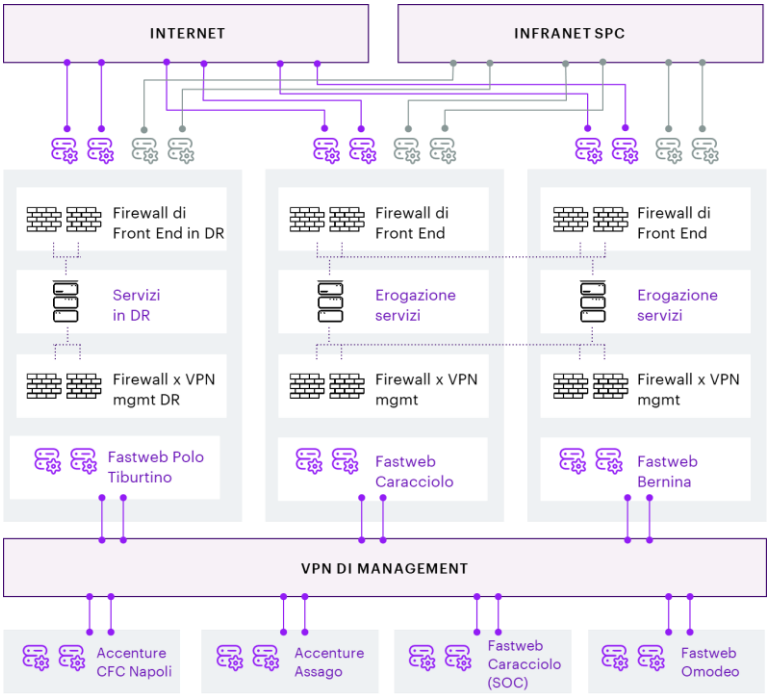


Figura 5 - Architettura tecnica del Centro Servizi

SERVIZIO	SOP	SOS
Help Desk	ACFC-N	AAS
L1.S1 – Security Operation Center	ACFC-N	FWCA
L1.S1 – Next Generation Firewall	FWCA	ACFC-N
L1.S3 – Web Application Firewall	FWCA	ACFC-N
L1.S4 – Gestione continua delle vulnerabilità	FWCA	ACFC-N
L1.S5 – Threat intelligence & vulnerability data feed	ACFC-N	FWO
L1.S6 – Protezione nav. internet e posta elettronica	FWCA	ACFC-N

seguito le relative **certificazioni di riferimento**: ✓CMMI - Capability Maturity Model Integration for System Development (DEV) and Service Management (SVC) ✓ISO 9001- Quality Management System ✓ISO 14001 - Environmental Management System ✓ISO 20000 - IT Service Management ✓ISO 27001 - Information Security Management System ✓ISO 27701 - Privacy Information Management System ✓ISO 22301 Business Continuity Management System ✓ISO 45001 - Occupational Health and Safety Management System ✓Tier IV – Constructed Facility dal Uptime Institute (Data Center Caracciolo) ✓CREST Cyber security incident response (CSIR). Per quanto concerne l'erogazione dei servizi fiduciari, l'architettura è costituita da un layer di front end costituito dal software applicativo da cui le PA possono richiedere i servizi e da un layer di back end che comprende gli HSM e altri sistemi funzionali all'erogazione dei servizi.

L1.S7 – Protezione end point	FWCA	ACFC-N
L1.S8 – Certificati SSL	ACFC-N	FWCA
L1.S9 – Formazione e security awareness	ACFC-N	FWO
L.1.S10 – Gestione identità e accesso utente	ACFC-N	FWCA
L.1.S11 – Firma digitale remota	ACFC-N	FWCA
L1.S12 – Sigillo elettronico	ACFC-N	FWCA
L1.S13 – Timbro elettronico	ACFC-N	FWCA
L1.S14 – Valid. temporale elettronica qualificata	ACFC-N	FWCA
L1.S15 - Servizi specialistici	ACFC-N	FWCA
Legenda: **SOP** *Sede operativa primaria,* **SOS** *Sede operativa secondaria*		

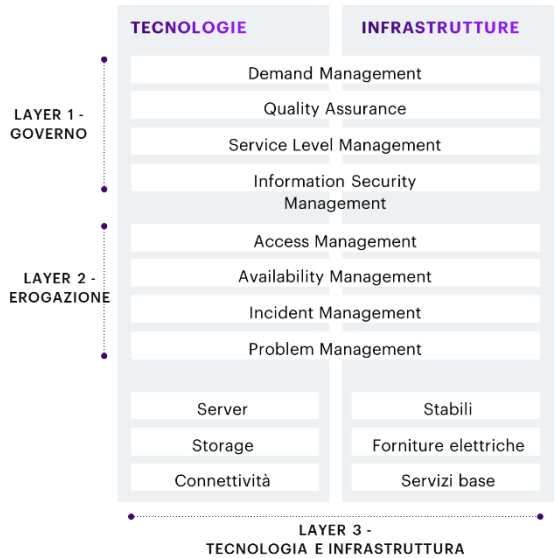
4.2 Modello organizzativo

Il CS viene coordinato da uno specifico Responsabile che opera a livello "Governo AQ" in accordo all'organigramma riportato al §3.1 secondo un modello definito, 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. Di seguito le principali responsabilità.

Figura	Principali responsabilità
Responsabile del Centro Servizi	✓Gestisce l'erogazione complessiva dei servizi verso le PA ✓Rende disponibili alle strutture operative le risorse umane, tecnologiche ed economiche per l'erogazione dei servizi in funzione delle necessità manifestate dalle PA ✓Governa complessivamente gli aspetti di conformità normativa, gestione dei rischi e tutti gli adempimenti necessari al funzionamento della macchina operativa ✓Costituisce l'interfaccia verso le nostre aziende in RTI
Responsabile di sicurezza informatica e continuità operativa	✓Analizza i rischi relativi ai servizi da erogare e ai dati/informazioni gestite ✓Definisce e manutiene il Piano per la sicurezza delle informazioni e il Piano di continuità operativa ✓Sviluppa e implementa gli strumenti di controllo di efficacia delle soluzioni implementate ✓Pianifica ed esegue test di verifica di efficacia delle stesse soluzioni ✓Rendiconta ai Vertici del RTI in merito allo stato della sicurezza informatica e della continuità operativa ✓Gestisce le certificazioni di sicurezza del CS
Responsabile di sede operativa (include la gestione della sicurezza fisica e ambientale ed energetica)	✓Gestisce le infrastrutture e i servizi logistici pertinenti il sito di riferimento ✓Supervisiona l'operatività delle risorse presenti nel sito ✓Interagisce con i responsabili dei servizi che vengono erogati nel sito ✓Implementa e gestisce gli apprestamenti di sicurezza fisica ✓Implementa e gestisce le necessità in ambito energy management ✓Effettua le valutazioni dei rischi sulle strutture e risorse del sito ✓Rendiconta i vertici del RTI su eventuali criticità pertinenti il sito di riferimento

4.3 Modello di funzionamento

Il modello di funzionamento è stato disegnato in accordo alle migliori pratiche internazionali in ambito IT Service Management ed è basato su processi operativi unici da applicare a tutte le sedi operative e ai singoli servizi garantendone **l'interoperabilità completa**. Il modello si articola su 3 livelli:



- **Layer 1 – Governo del CS**. Include i processi unici comuni a tutte le sedi operative, necessari a garantire la corretta implementazione ed erogazione dei servizi tra i quali si evidenziano: ✓**Demand management** dedicato alla gestione delle richieste delle singole PA che vengono raccolte tramite portale e indirizzate sui singoli servizi in modo automatizzato per le richieste standard e a seguito di analisi specialistica per eventuali richieste a maggiore complessità; ✓**Quality assurance** finalizzato a monitorare nel continuo il rispetto dei più elevati standard di erogazione dei servizi nel tempo e ad indirizzare eventuali azioni di rafforzamento che si dovessero rendere necessarie; ✓**Service level management** finalizzato alla gestione dei livelli di servizio al fine di garantirne un monitoraggio e una rendicontazione continuativa, nonché ad abilitare l'esecuzione di eventuali azioni di miglioramento che si rendessero necessarie; ✓**Information security management**, gestito dal responsabile della sicurezza informatica, per garantire la corretta implementazione dello Information Security Management System (ISMS).
- **Layer 2 – Erogazione dei servizi**. Include i processi necessari a garantire l'erogazione sicura e continuativa dei servizi in modalità univoca e sinergica tra tutte le sedi operative tra i quali si evidenziano: ✓**Access management** per poter garantire l'accesso ai servizi informativi agli utenti delle PA in modalità sicura; ✓**Availability management** finalizzato a garantire la continuità dell'erogazione dei servizi secondo gli standard contrattualizzati; ✓**Incident management** finalizzato alla gestione degli incidenti che possono impattare le dimensioni di riservatezza, integrità dei dati e di disponibilità dei servizi; ✓**Problem management** per l'analisi di eventuali problematiche che si dovessero riscontrare nell'erogazione e l'identificazione delle relative iniziative di adeguamento. In tale ambito sono incluse anche le attività di knowledge transfer verso le PA necessarie a garantirne l'autonomia operative.
- **Layer 3 – Tecnologia e infrastruttura**. Include tutte le componenti fisiche di natura **informatica e infrastrutturale** necessarie all'erogazione dei servizi. Per i Data Center include le dotazioni delle sale adibite a ospitare i sistemi operativi, di connettività e di storage; per i Delivery Center include tutti gli asset per

l'accesso delle risorse nonché gli apprestamenti di sicurezza fisica e per la sicurezza sul lavoro del personale. È gestito dal responsabile di sito tramite presidi locali necessari a garantire un costante adeguamento e manutenzione degli stessi.

4.4 I requisiti di sicurezza delle informazioni

Il CS è dotato di misure di sicurezza delle informazioni atte alla protezione di dati, informazioni e servizi erogati alle PA e, in particolare, a garantire: ✓la **riservatezza** dei dati e delle informazioni gestite permettendo l'accesso solo a chi è autorizzato; ✓l'**Integrità** dei dati e delle informazioni gestite impedendo modifiche non autorizzate o manomissioni; ✓la **Disponibilità** dei servizi erogati grazie a soluzioni di protezione e ridondanza dei dati e delle infrastrutture. La soluzione proposta prevede l'implementazione, per le sedi operative, di contromisure di sicurezza logica secondo il principio di "difesa in profondità" e "zero trust" strutturato secondo livelli che comprendono più strati di protezione, in conformità dello **standard ISO 27001**. Viene quindi definito il **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** ovvero lo strumento che permette di controllare in modo sistematico e continuativo i processi che riguardano la sicurezza di tutto il patrimonio informativo coinvolto nell'erogazione dei servizi.

Tra le misure di sicurezza implementate in accordo a tale standard si evidenziano: ✓controllo degli accessi per utenti finali, utenti interni e personale con privilegi amministrativi (cd access control) ✓crittografia per la gestione dei segreti aziendali e delle chiavi di cifratura ✓protezione delle postazioni di lavoro tramite antivirus, EDR, Data Loss Prevention, e-mail security ✓protezione dei server tramite antivirus, EDR, FIM ✓protezione delle basi dati tramite soluzioni di mascheramento e di controllo delle operazioni ✓protezione da minacce cyber tramite security monitoring e della threat intelligence ✓protezione delle applicazioni tramite controllo del codice sorgente e la protezione delle applicazioni esposte su internet ✓protezione della rete tramite sistemi perimetrali, di monitoraggio del traffico e di segregazione / segmentazione ✓processi continuativi di vulnerability management, di patching e l'applicazione di standard di hardening.

Il CS è dotato di un proprio **Piano per la sicurezza delle informazioni** redatto secondo i principi del Client Data Protection Program, sviluppato e adottato da Accenture per garantire la tutela delle informazioni dei Clienti e certificato ISO27001. Il Piano è soggetto a revisione continua e ad approvazione da parte del RTI.

4.5 I requisiti di sicurezza fisica

Tutte le sedi operative sono dotate di soluzioni volte alla protezione nei confronti di danni dovuti ad eventi esterni (incendi, inondazioni, esplosioni, disastri naturali) o causati dall'uomo tramite accessi non autorizzati mirati a danneggiare sistemi e dati (manomissione e furto delle informazioni e degli apparati IT, impedimento allo svolgimento dei servizi e dei processi IT, manomissioni e interruzioni delle attività). Per ogni sede operativa è previsto un **piano per la sicurezza fisica** e ambientale e l'assegnazione della responsabilità della sicurezza fisica al responsabile di sede.

Le contromisure di sicurezza fisica sono strutturate secondo **livelli di protezione progressivi** e includono: ✓Sistemi di protezione fisica perimetrale tramite barriere fisiche arricchite da sensori di rilevamento presenze e sensori anti-intrusione; ✓Sistemi di controllo accessi tramite barriere di protezione (bussole o tornelli) e sistemi di autenticazione a due fattori (inclusi elementi di biometria); ✓Sistemi di videosorveglianza arricchiti da soluzioni che si basano sull'AI per identificare anomalie in corrispondenza degli accessi critici; ✓Sala di monitoraggio operativa 24x7 in grado di gestire eventi allarmi e di allertare servizi di ronda/vigilanza a chiamata; ✓Presidio fisico tramite personale di presidio 24x7 per gli accessi alle aree ad alta criticità; ✓Collegamento con le forze dell'ordine per gestire interventi di emergenza; ✓Integrazione con il servizio Security Operation Center in grado di collegare anomalie sui sistemi di accesso fisico e logico.

Con particolare riferimento agli stabili adibiti a **Data Center** sono previste misure di sicurezza specifiche, stante la criticità dei dati e dei servizi gestiti. Queste sedi sono dotate, tra le altre misure, di impianti e sistemi di sicurezza controllati e monitorati 24x7 da personale Fastweb specializzato e certificato e sono gestiti dal sistema di supervisione GEMSS (GEneral Manager for Security Systems). Sono installati sistemi di videosorveglianza ad alta definizione e ad alte prestazioni con funzionalità di Motion Detection e, in particolare in sala dati, sono presenti telecamere dedicate ad ogni fila di rack (43 Telecamere, in media 1 cam ogni 10mq). Sono installate sbarre o cancelli di protezione azionati dalla postazione di guardiania per regolamentare l'accesso dei veicoli, laddove ritenuto necessario.

Tutte le aree del Data Center, sala dati e locali esterni, sono protette da un sistema di rilevazione fumi e, per un maggior grado di sicurezza, è presente anche un sistema di rivelazione fumi a campionamento d'aria HSSD nella sala dati e nei locali UPS e batterie. Tutte le aree del DC sono protette con un sistema di spegnimento automatico a gas tipo IG-01 (Argon), oltre che da sensori di rilevamento del calore, sensori di fumo, sistema di estinzione incendi, estintori portatili. La protezione dal fuoco è effettuata tramite compartimentazione e isolamento dei locali impianti. La resistenza è garantita fino a 120 minuti (REI 120 / F 120) tramite utilizzo di materiali da costruzione ignifughi e autoestinguenti.

Il processo di accesso al Data Center prevede l'adozione di procedure di autenticazione via web, riconoscimento puntuale, abilitazione e consegna di un badge e successivamente l'accesso tramite una bussola classificata "antirapina".

È presente un sistema ridondato di rilevamento dello spandimento dei liquidi a protezione della sala dati e dei locali con trasformatori, UPS e batterie, e centrali idrauliche. Gli allarmi di perdite provocano la chiusura delle valvole di linea e InRow del tratto interessato.

4.6 Continuità Operativa

Il CS è disegnato in modo tale da poter erogare i servizi con requisiti di continuità operativa definiti in accordo alle indicazioni definite dallo standard ISO 22031. Tali requisiti sono implementati per garantire la continuità: ✓**dei servizi informatici** secondo l'architettura dei Data Center di Fastweb descritta in precedenza che prevede 2 siti di erogazione (Caracciolo e Bernina) e 1 sito di Disaster Recovery (Polo Tiburtino) e ✓**dei servizi erogati dai centri di delivery** di Accenture e di Fastweb tramite la ridondanza di tutti i servizi di connettività e di alimentazione e la possibilità di spostare l'operatività presso altri centri di delivery. Questo consente la **copertura completa degli scenari di rischio** definiti dalle più stringenti normative applicabili in Italia, tra cui: ✓Indisponibilità dei sistemi e dei servizi informatici (erogati dai Data Center); ✓Indisponibilità della sede operativa di riferimento per l'erogazione di un servizio; ✓Indisponibilità del personale; ✓Indisponibilità dei servizi; ✓infrastrutturali (tlc ed energia); ✓Indisponibilità di dati e della documentazione essenziale; ✓Indisponibilità delle terze parti coinvolte.

Le soluzioni previste garantiscono requisiti di ripristino elevati che prevedono un **RTO e un RPO prossimi allo 0** per eventi che coinvolgono i Data Center e/o i Delivery Center (es. incendio/allagamento/terremoto). Solo nel caso in cui si rendesse necessario il ricorso al sito di Disaster Recovery e alla relativa terza copia di dati (indisponibilità contemporanea di entrambi i Data Center di Milano) è previsto un RTO di 4 ore e un RPO prossimo allo 0.

Con riferimento **ai servizi informatici**, nell'ambito dell'architettura sopra presentata, i Data Center sono serviti da 2 reti pubbliche di distribuzione e sottostazioni

separate ciascuna delle quali può tenere il pieno carico del sito. Sono presenti 2 gruppi di 2 x 800 KVA UPS con autonomia a pieno carico di 15 minuti (ogni gruppo ha 2 linee di alimentazione separate (A e B) e un sistema aggiuntivo di Inertial Water Storage da 26 m^3 e generatori di standby costituiti da 2 Gruppi Elettrogeni per una potenza complessiva di 4,2 MW e 2 serbatoi addizionali e separati da 16.000l.

La soluzione è abilitata da specifiche dotazioni e configurazioni che includono: ✓Link di interconnessione tra i datacenter in fibra ottica di tipo L2 e percorsi geografici affatto diversificati che rendono possibili allineamenti sincroni delle SAN ✓Adeguato dimensionamento della banda di rete tra i datacenter e basse latenze ✓Opportune apparecchiature di rete e relative configurazioni di WAN geografiche ✓Tecniche di stretch clustering che consentono di estendere il concetto di cluster di risorse su scala geografica ✓Due nodi SAN storage con replica sincrona per la disponibilità continua dei dati su entrambi i siti di erogazione in BC ✓Suite di virtualizzazione VMWare in grado di garantire ambienti speculari sui due siti e potenza elaborativa resa disponibile in modo immediato e automatico.

In **aggiunta** evidenziamo l'applicazione di soluzioni per **isolare le seconde e terze copie** dei dati da eventuali compromissioni delle copie primarie a seguito di attacco informatico (es. ransomware). La disponibilità di un back-up basato su versioning continuativo consente di ripristinare i dati immediatamente, rendendo disponibili le ultime versioni prima dell'attacco identificato.

In riferimento **ai servizi erogati dai centri di delivery**, sono previste soluzioni atte a garantire l'erogazione dei servizi tramite: ✓Formazione di risorse di back up e disponibilità di unità operative gemelle presso altre sedi operative ✓Possibilità di erogare i servizi in modalità "smart working" in situazione di emergenza in conformità alla normativa vigente ✓Ridondanza delle infrastrutture di connettività dei siti di Delivery relativamente alle telecomunicazioni (doppie connessioni alla connettività esterna) e all'approvvigionamento energetico (doppie cabine di connessione al provider di energia) ✓Virtualizzazione della documentazione e sua gestione secondo le configurazioni di continuità dei Data Center ✓Clausole contrattuali di salvaguardia e sulle terze parti e ricorso altri fornitori pre-identificati.

Tutte le soluzioni sono formalizzate all'interno del **Piano di Continuità Operativa** del CS, sono soggette a revisione costante e ad attività di test periodico con cadenza almeno annuale. A garanzia della responsabilizzazione su tale tematica è prevista la nomina formale di un Responsabile della Continuità Operativa cui sono assegnate risorse economiche adeguate ad adempiere ai propri compiti.

4.7 Impatto ambientale ed energetico

Tutte le sedi operative (Data Center e Delivery Center) sono dotate di soluzioni tecnologiche che consentono una **drastica riduzione dell'impatto ambientale** attraverso l'abbattimento delle emissioni di CO_2 e la minimizzazione dei consumi energetici, secondo un percorso iniziato da tempo verso la Green Company da tutti i componenti del RTI, sia nella erogazione dei servizi ai clienti che nella gestione di procedure interne atte a migliorare gli impatti sull'ambiente (uso carta "ecolabel", uso di energia proveniente da fonti rinnovabili, ecc.).

In particolare, il **Data Center Caracciolo** è stato progettato adottando criteri orientati alla sostenibilità ambientale ("green building"), come dimostrato dalla certificazione **LEED Platinum** dell'edificio. La sede è provvista di un impianto fotovoltaico per l'auto generazione di energia elettrica e di un sistema di climatizzazione di ultima generazione, permettendo in questo modo di ridurre i consumi energetici. Fastweb ha ottenuto nel 2013 la certificazione ISO 14001, rinnovata nel 2016 con la **certificazione ISO 14001:2015**, confermando il suo impegno nel mantenere attivo un sistema di gestione ambientale secondo i requisiti della norma per garantire il controllo, la riduzione e la prevenzione degli impatti ambientali, reali e potenziali, connessi alla propria attività. Tra le soluzioni tecnologiche adottate per la **riduzione delle emissioni di CO_2 e la minimizzazione dei consumi energetici** si evidenziano: ✓Impianti di illuminazione progettati e realizzati con tecnologie e materiali a basso consumo energetico e con dissipazione di calore prossima allo zero ✓Dispositivi di monitoraggio e attuatori che consentono il controllo e lo spegnimento automatico dei dispositivi non necessari all'operatività ✓PDU (Power Distribution Unit) intelligenti ad alta efficienza che minimizzano gli overload e quindi la dissipazione di calore ✓Alimentatori degli apparati IT a singola fase e dotati di regolatori di tensione a bassa dispersione ✓Sistemi di raffreddamento dei rack a elevato rendimento ✓Sistemi UPS ad alto rendimento con fattori di potenza estremamente elevati e che minimizzano le perdite di potenza attiva ✓Server a elevata densità ad alte prestazioni per ridurre il numero di macchine fisiche necessarie a parità di capacità computazionale ✓Meccanismi di CPU Scaling per gestire la potenza elaborativa in funzione del carico applicativo e permettere la modulazione del consumo energetico delle CPU ✓Sistema DCIM (Data Center Infrastructure Management) che autoregola i valori di potenza e raffreddamento in tempo reale ✓Sistema per ottimizzare il funzionamento dei gruppi frigo.

Le soluzioni definite consentono di attestare i Data Center su un **valore di PUE (Power Usage Effectiveness) medio pari 1,55** inferiore al valore di 1,6 previsto come obiettivo dalle "Linee Guida per il Consolidamento dei Datacenter della Pubblica Amministrazione" di AgID. In particolare, il Data Center Caracciolo rappresenta l'**eccellenza nello scenario nazionale** con un valore di PUE pari 1,25.

4.8 Descrizione del servizio di Help Desk

Il servizio di Help Desk erogato dal CS ha l'obiettivo di fornire un unico punto di contatto per le PA tramite l'adozione di sistemi multicanale che abilitano l'accesso degli utenti secondo le più moderne **logiche di multicanalità integrata**. In tal senso, vengono resi disponibili una grande varietà di canali di accesso che operano in modalità integrata, rendendo possibile per gli operatori passare da uno strumento ad un altro per garantire la migliore esperienza utente. La soluzione proposta si basa su un'istanza **ServiceNow** installata all'interno del CS. Metteremo a disposizione **SPARK** (ServiceNow Powered by Accenture Resources & Knowledge), toolkit definito da Accenture che abilita su ServiceNow un'implementazione rapida dei processi ITIL4 con numerosi modelli e acceleratori pre-compilati.

L'Help Desk, erogato secondo gli orari ed i livelli di servizio previsti nella documentazione di gara, garantisce quindi accessibilità e fruibilità con molteplici modalità quali: ✓utilizzo del **numero verde unico**, appoggiato su di una infrastruttura VOIP ad alta affidabilità; ✓**interfaccia web** e **mobile** che operano in modalità integrata al portale disponibile alle PA; ✓**Chat / SMS / Social** che abilitano forme di contatto alternative alle tradizionali in base alle differenti esigenze delle PA; ✓**e-mail** per la gestione delle comunicazioni scritte con le PA. A titolo esemplificativo, l'ingaggio da parte della PA può essere iniziato tramite contatto telefonico, proseguire con un una chat ed essere rendicontato tramite interfaccia web o mobile. L'Help Desk costituisce, inoltre, il principale punto di ingaggio del Security Operation Center in modalità 24x7 per tutte le problematiche relative alla gestione di eventi / incidenti di sicurezza.

Tra i principali elementi innovativi introdotti si evidenziano: ✓Applicazione di tecnologie basate sull'**AI** per poter indirizzare al meglio i ticket e proporre all'operatore soluzioni alle necessità della PA. ✓Adozione di **soluzioni automatizzate (BOT)** per la risoluzione di casi standard e a bassa complessità. ✓Costante **misura del livello di soddisfazione** della PA così da indirizzare al meglio eventuali criticità e problematiche. ✓**Accesso facilitato** e comune ai quesiti provenienti da tutti i canali disponibili alle PA (web e mobile).

Di particolare importanza è inoltre la **piattaforma di Knowledge Management integrata in ServiceNow c**he consente di gestire e rendere fruibile la base di conoscenza condivisa con il Portale (cfr. §16) e che consente di accedere ai dettagli operativi dei servizi erogati e delle tecnologie di supporto tramite la costituzione di un patrimonio informativo specifico. La piattaforma consente di accedere alla Knowledge Base per cercare le informazioni, filtrando i contenuti per tipologia e ordinando per aggiornamento più recente, per numero di visualizzazioni o per il livello di valutazione definito dagli utenti. L'applicazione consente agli utenti di iscriversi a specifici Knowledge articles e di ricevere notifiche su nuovi articoli e revisioni o commenti. Gli utenti possono commentare i Knowledge articles in vari modi: ✓segnalare un articolo come errato o inappropriato; ✓fornire una valutazione sull'articolo; ✓indicare l'articolo come utile o non utile; ✓visualizzare i commenti, aggiungere un nuovo commento o rispondere ai commenti esistenti.

Il servizio di Help Desk è governato da un **Help Desk Manager** che ha la responsabilità complessiva dell'erogazione del servizio e si occupa del monitoraggio continuativo del livello di servizio, ne esegue la rendicontazione e definisce e implementa le eventuali azioni di miglioramento che si dovessero rendere necessarie. Dal punto di vista operativo, il servizio viene erogato tramite: ✓**una struttura di 1° livello** costituita da team composti da analisti e coordinati da supervisori esperti. Questo livello gestisce le richieste standard secondo playbook predefiniti (stimate intorno allo 80% dei casi totali); ✓**una struttura di 2° livello** costituta da specialisti dei singoli servizi, distinti per tipologia di PA servita, che si occupano di gestire i casi a maggiore complessità o comunque che esulano dalle richieste standard (stimati intorno al 20% dei casi totali). È inoltre prevista la figura del **Customer Assistant** ovvero di risorse dedicate a seguire PA che hanno attivato molteplici servizi. Il Personal Assistant è una risorsa dotata di elevata esperienza che consente di facilitare la presa in carico e l'evasione delle richieste di tali PA.

I processi operativi del servizio sono supportati da uno strumento di **case management** avanzato che sarà opportunamente implementato per gestire le casistiche di eventi legate a tutti i servizi oggetto di erogazione.

Il servizio prevede un'organizzazione basata su turnistica frutto di un **processo continuo di analisi e pianificazione**, che tiene conto delle **statistiche** acquisite quotidianamente sulle chiamate ricevute per tipologia e durata. Il **dimensionamento è quindi flessibile e adattativo**, in conseguenza dei volumi di traffico e del numero di ticket stimato e sarà progettato sulla base di pregresse esperienze consolidate e utilizzando strumenti di analisi in base a tutte le variabili di servizio a disposizione (volumi, tempi di risposta/intervento, incremento di attività su base oraria, SLA, etc.) si calcola con precisione il numero di risorse necessarie.

Elemento fondamentale del servizio sono le risorse umane allocate sulle attività che sono oggetto di **interventi di formazione continuativi** finalizzati a: ✓Garantire la conoscenza dei servizi erogati, tramite affiancamento alle risorse che si occupano dell'erogazione dei servizi affinché possano avere esperienza diretta del contenuto degli stessi e delle problematiche che si possono riscontrare, ✓Gestire la relazione con le PA. Si procederà quindi ad interventi di formazione specifici per poter interloquire in modalità efficace con le PA e poter dare un riscontro corretto e tempestivo alle relative esigenze; ✓Indirizzare problemi complessi in funzione della relativa esperienza lavorativa. Sono previsti **meccanismi di crescita professionale** che consentono di assumere progressivamente un ruolo di riferimento per la gestione delle problematiche a maggiore complessità.

5 PROPOSTA PROGETTUALE PER IL SERVIZIO "SECURITY OPERATION CENTER (SOC)"

5.1 Soluzione proposta

Il modello **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di 'Security Operations Center (SOC) nel dominio: ✓"Threat Monitoring" e "Threat Hunting", riconducibili alla Funzione NIST "Detect" ✓"Threat Response" e "Active Defence", riconducibili alla Funzione NIST "Respond & Recover".

La ventennale esperienza di Accenture, unitamente a quella di Fastweb nell'ambito della PA, ha permesso di consolidare e far evolvere un modello di servizio ponendo a fattor comune esperienze analoghe nella realizzazione ed erogazione di servizi di Security Operation Center per istituzioni governative nazionali ed internazionali. Si è giunti alla definizione ed ingegnerizzazione di un modello di "**Next Generation Security Operation Center (NG-SOC)**" basato sulla piattaforma tecnologica di Accenture denominata "**Advanced Security Monitoring & Detection (ASMD)**", la quale sfrutta un'architettura modulare flessibile e multi-cliente, che permette di scalare a seconda del numero e livello di integrazione delle amministrazioni in ambito di gara. La soluzione ASMD di Accenture abilita ad un servizio di Managed Detection & Response (MDR), per offrire alle Amministrazioni aderenti servizi gestiti SIEM **segregati e integrati** con la piattaforma centralizzata SOAR, nel seguito descritte. La soluzione opera in modalità 24x7x365 e viene erogata dai *SOC* di Napoli e Milano, operanti all'interno dei Centri Servizi in ambito di gara (cfr. §4). Accenture ha selezionato e integrato nella piattaforma *ASMD* la tecnologia **Splunk** per la parte di *"Security Information & Event Management (SIEM)"* e **PaloAlto Cortex XSOAR** per la parte di "*Security Orchestration, Automation & Response (SOAR)"*, entrambi leader di mercato secondo fonti affermate di analisti di settore quali Gartner e Forrester e partner decennali a livello globale delle Aziende del RTI.

La natura del *Security Operations Center* proposto (SOC) fa sì che **assuma un ruolo centrale** nella proposta del RTI per **tutti i servizi, inclusa la gestione delle funzionalità di sicurezza afferenti alla rete, ai sistemi, ai dati e alle applicazioni, *On-Site* e non**, delle PA. Questo include la possibilità di estendere il monitoraggio ad eventi e specifici casi d'uso provenienti da sorgenti non squisitamente IT (si pensi ad esempio alla possibilità di importare i log prodotti dai dispositivi IoT/OT connessi nelle Smart-City per individuare minacce in grado di minare la sicurezza fisica dei cittadini). Attraverso un continuo **scambio informativo bidirezionale**, in particolare con i Servizi da L1.S2 a L1.S7 e L1.S10, **il SOC aumenta la propria efficacia e accuratezza** tramite un processo automatico di **arricchimento** degli eventi di sicurezza ingegnerizzato dal RTI e basato su un processo di *datamining, ML e deep learning;* sfruttando le funzionalità offerte dalle soluzioni tecnologiche in uso presso il SOC per lo sviluppo di modelli di identificazione delle anomalie e clustering dinamico per gli use case di detection, incrementa la produttività della gestione degli incidenti mediante ✓attribuzione automatica della ownership ✓sviluppo assistito di playbook di risposta ✓inferenza di azioni di risposta applicabili. Il servizio proposto di SOC ha l'obiettivo di **individuare nel minor tempo possibile** gli attacchi ai danni dell'Integrità, Confidenzialità e/o Disponibilità del patrimonio informativo delle Amministrazioni siano esse Locali o Centrali. A fronte della rilevazione e della convalida dell'incidente, **viene innescato il processo di Incident Management supportato dalle informazioni di dettaglio fornite dal Servizio SOC, contestualizzate e arricchite** da ulteriori ambiti oggetto della presente proposta quali ad esempio il 'Servizio di Gestione continua delle Vulnerabilità di Sicurezza' - per assegnare in fase di Triage la corretta priorità all'incidente - e il 'Servizio di Threat Intelligence & Vulnerability Data Feed' - per correlare informazioni sugli Indicatori di Compromissione (IOC) e Tactics Techniques and Procedure (TTP) del MITRE ATT&CK relative al potenziale Threat Actor. Questo permette di offrire alla Amministrazioni servizi avanzati di **Monitoraggio di Sicurezza in "real-time"** per identificare le minacce in modalità proattiva e automatizzata, comprimere i tempi di analisi e presa in carico degli incidenti, incrementare la capacità di

individuazione e rimozione dei falsi positivi, e **attivare in maniera tempestiva il processo di 'Risposta agli attacchi e agli incidenti'** supportato dalle informazioni di dettaglio necessarie all'efficace contenimento ed eradicazione dell'incidente stesso, rendendo la risposta agli eventi di sicurezza molto più veloce rispetto ai servizi SOC tradizionali, con un incremento di efficienza misurato di circa il 60%. L'efficacia e la qualità del servizio sono frutto dell'esperienza maturata dai nostri pluricertificati CyberSecurity Analyst in due decadi di servizio nel settore pubblico e privato, nella costante gestione operativa end-2-end della piattaforma ASMD ivi inclusi gli ambienti del SIEM segregati e integrati con la soluzione di orchestrazione e automazione centralizzata (SOAR), e su un insieme di oltre cinquanta procedure consolidate che sono evolute nel tempo raggiungendo oggi un **livello di maturità riconosciuto** non solo dai clienti ma anche dagli analisti di mercato come nei report *"Forrester Wave European Managed Security Services Providers 2020"* e "*IDC Marketscape Worldwide Managed Security Services 2020*".

BEST PRACTICE - ASMD - La piattaforma ASMD attualmente in Italia è in uso presso oltre 20 clienti, portando **standardizzazione** nella gestione degli incidenti di Sicurezza tramite i propri playbook e **riducendo** la manualità delle operazioni ripetitive, con conseguente maggiore spazio operativo per attività a maggiore valore aggiunto (più approfondita analisi delle cause e miglioramento nella caccia delle minacce). L'analisi dei KPI interni ha evidenziato un **notevole abbassamento nei tempi di risposta degli incidenti di sicurezza.**

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: circa 30, tra cui Roma Capitale e SACE

Private: Intesa Sanpaolo, NEXI, A2A, ISAB, Poste Italiane e Poste Mobile, primario operatore finanziario

Descrizione di un caso di successo - Intesa Sanpaolo →Esigenza - Team di presidio in ambito cybersecurity che eroghi servizi di SOC insieme al team di cybersecurity del cliente **→Soluzione** - Accenture ha erogato servizi SOC 24 x7, tramite un team MSS presso il cliente e ricorrendo al Cyber Fusion Center per servizi extra orario di lavoro. Gestione degli incidenti, malware, analisi di phishing e spam, valutazione delle vulnerabilità ed esecuzione di test di penetrazione, early warning, caccia alle minacce e supporto di Digital Forensics **→Benefici** - Efficace gestione della cybersecurity e contenimento del rischio a livelli richiesti dal cliente.

5.1.1 Funzioni Offerte

Il servizio prevede: un livello di **Interfaccia** utile all'interazione con il servizio, un livello di **Erogazione** in cui sono espletate le funzioni principali del servizio, un livello di **Automazione** (intelligent layer) che aggiunge funzioni avanzate, un livello **Interazioni** per le relazioni con gli altri servizi. I livelli comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative**, descritte di seguito:

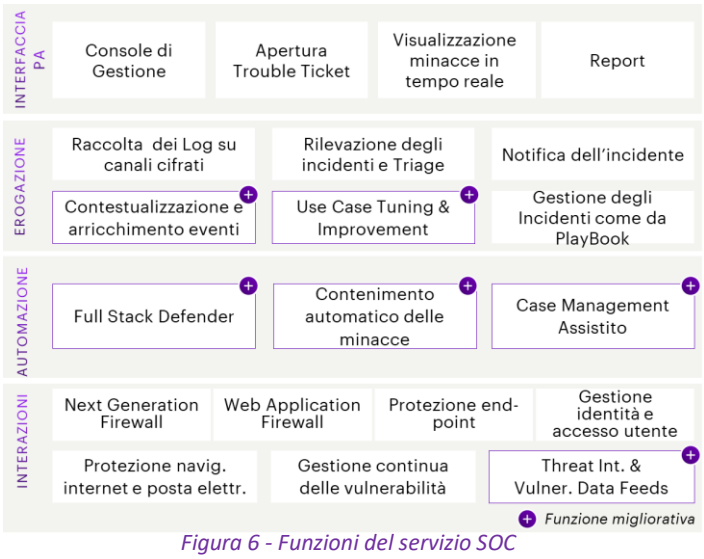


Figura 6 - Funzioni del servizio SOC

- **Contestualizzazione e arricchimento eventi:** Tutti gli eventi di sicurezza raccolti dal servizio SOC sono correlati e arricchiti con le informazioni fornite dagli altri servizi integrati attivi sulla singola PA, in modo da calare i dati raccolti e gli alert identificati sullo specifico contesto e velocizzare le attività degli analisti.
- **Use case Tuning & Improvement:** L'esperienza maturata sui casi/incidenti gestiti sulle singole PA viene utilizzata per migliorare continuamente la libreria di use case sviluppati dal servizio SOC, minimizzando il numero di falsi positivi, migliorando l'efficienza dei team di analisti ed eventualmente inferendo soglie di alert o use case aggiuntivi rilevanti tramite ML/deep learning.
- **Full Stack Defender:** Il nostro modello NG-SOC permette di superare i limiti di efficacia nella detection delle moderne soluzioni SIEM e SOAR, offrendo un controllo real-time dello stato di sicurezza delle amministrazioni, e correlando le informazioni di monitoraggio con interrogazioni dirette ai dati delle altre soluzioni tecnologiche in ambito di gara per sfruttare il pieno potenziale di visibilità sugli asset su cui sono installati. Mette inoltre a disposizione playbook sviluppati per agevolare le interrogazioni degli analisti sui tool e dedicare il tempo di analisi sulle attività di valore.
- **Contenimento automatico delle minacce:** Il servizio SOAR implementato dal SOC è integrato con le soluzioni di sicurezza in ambito di gara in modo da offrire una risposta automatica efficace di primo intervento sulle piattaforme tecnologiche relative ai servizi attivi sulle singole PA, permettendo di ridurre sensibilmente i tempi di intervento.
- **Case Management Assistito:** Il servizio SOC utilizza le più moderne tecnologie SOAR per supportare gli analisti nella gestione degli incidenti e analisi degli eventi di sicurezza rilevanti, tramite l'implementazione di playbook di automazione che permettono di arricchire automaticamente le informazioni collezionate con le fonti di Intelligence oppure assegnare la priorità ai case aperti.
- **Threat Intelligence & Vulnerability Data feed:** Le soluzioni di Threat Intelligence e Vulnerability Data feed sono utilizzate internamente dal SOC come fonte di arricchimento degli eventi di sicurezza raccolti in relazione al contesto del panorama delle minacce globale di interesse per le PA.

5.1.2 Architettura tecnologica

La piattaforma ASMD proposta prevede l'integrazione di una componente SIEM - segregata per la specifica PA e basata su tecnologia Splunk - con la piattaforma SOAR centralizzata del RTI basata su tecnologia PaloAlto Cortex XSOAR.

La soluzione **Splunk** ci ha permesso di superare i limiti delle soluzioni SIEM convenzionali, tramite un **deploy scalabile** che rende

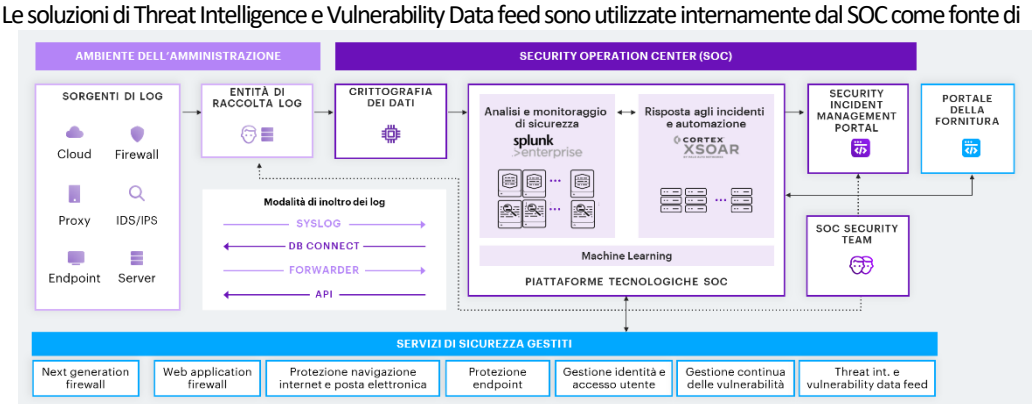


Figura 7 - Architettura tecnologica SOC

possibile l'integrazione con ogni tipo di sorgente di dati senza alcuna limitazione di schema. La piattaforma garantisce **piena visibilità sugli eventi di sicurezza**, riducendo sensibilmente il tempo di identificazione delle minacce, e offrendo non solo funzionalità di ricerca, correlazione dei dati e creazione di cruscotti, ma anche strumenti avanzati di analytics, ML e analisi comportamentale. L'utilizzo di un **approccio basato sul rischio** e il supporto nativo alle tecnologie in ambito di gara, permette inoltre di prioritizzare gli interventi e minimizzare i tempi di investigazione in caso di incidente.

Come soluzione SOAR è stato identificato **PaloAlto Cortex XSOAR:** l'utilizzo in ASDM ha permesso un **abbattimento del tempo di risposta agli incidenti**, riducendo sensibilmente il volume degli allarmi generati dagli strumenti di sicurezza. Cortex XSOAR ci ha permesso di integrare nel servizio funzionalità avanzate di deep learning per fornire raccomandazioni, accelerare lo sviluppo di playbook e migliorare i modelli di risposta sulla base di incidenti e azioni precedenti.

La soluzione tecnologica proposta mira a ridurre sensibilmente il tempo speso dagli analisti su task operativi ricorrenti, in modo da soffermarsi su **attività a maggior valore** quali approfondimento delle analisi, ricerca proattiva e miglioramento continuo. Il disegno proposto permette inoltre di segregare i contesti delle singole PA, e di creare viste personalizzate per ognuna di esse, in modo da avere sempre chiaro il livello di sicurezza dei singoli asset integrati in relazioni a tutti i servizi di sicurezza attivi. L'integrazione con i servizi attivi sulle PA permette inoltre di correlare e arricchire le informazioni raccolte dal SIEM, permettendo di offrire una *detection* olistica dell'ecosistema delle singole PA.

Nel corso della fornitura per l'erogazione dei servizi, al fine di indirizzare le diverse esigenze di cluster di PA diverse, in ottica multivendor, potremo utilizzare piattaforme tecnologiche diverse da quella descritta o anche una combinazione di più prodotti di mercato. Questa considerazione vale per tutti i servizi di fornitura.

5.1.3 Next Generation SOC (NG-SOC): caratteristiche tecnologiche e prestazionali migliorative e innovative

Il servizio NG-SOC nasce con l'obiettivo di rilevare e interrompere il processo di attacco il prima possibile, in modo da minimizzare gli impatti sulle singole PA. Con il suo approccio innovativo, basato sulla forte coesione tra strumenti di monitoraggio avanzati e meccanismi di automazione delle analisi, nonché su un modello pienamente gestito (Managed Security Services) che libera le PA dagli oneri di gestione delle infrastrutture a supporto. Il servizio di *NG-SOC* basato sulla piattaforma *Advanced Security Monitoring & Detection (ASMD)* è stato ingegnerizzato da Accenture avendo come obiettivo principale l'abbattimento del lasso di tempo che intercorre tra l'ingestione da parte del *SIEM* dei *log* contenenti i dati grezzi dell'attacco, e l'identificazione dell'incidente da parte del team preposto. **Si raggiunge quindi la minimizzazione degli impatti sulle singole Amministrazioni** attraverso un processo accelerato e consapevole di risposta all'incidente. Per conseguire tale obiettivo è stata posta particolare attenzione all'integrazione nativa tra soluzione SIEM Splunk e SOAR PaloAlto con fonti di Threat Intelligence e i servizi di sicurezza in ambito delle PA. L'arricchimento automatico ottenuto tramite la standardizzazione da parte del RTI di feed normalizzati fornisce alle PA piena visibilità sullo stato di sicurezza dei sistemi monitorati, sia dal punto di vista degli attaccanti sia per quanto concerne l'impatto sull'organizzazione stessa. Il modello si fonda inoltre su un paradigma di miglioramento continuo che, a partire dalle evidenze raccolte dalla funzione di controllo qualità (cfr. § 5.3.2), identifica e implementa le azioni migliorative applicabili al servizio per fornire sempre un **livello di sicurezza competitivo e rilevante** rispetto al contesto delle minacce cyber a livello globale.

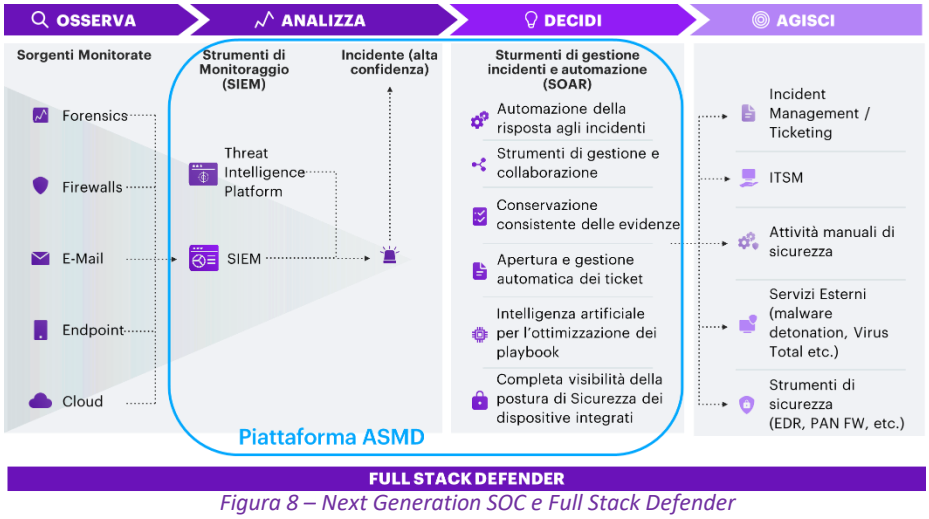


Figura 8 – Next Generation SOC e Full Stack Defender

Il modello NG-SOC proposto utilizza un approccio innovativo denominato "**Full Stack Defender**", il quale permette di superare i limiti di efficacia nella detection delle moderne soluzioni SIEM e SOAR. Tramite integrazione con le soluzioni tecnologiche proposte dai servizi di gara, questo modello offre un pannello centralizzato per il controllo real-time della postura di sicurezza delle amministrazioni, correlando e arricchendo le informazioni del SIEM con interrogazioni dirette ai dati delle altre soluzioni, sfruttandone così il pieno potenziale di visibilità sugli asset su cui sono installati. Permette inoltre di semplificare la complessità di ricerca e analisi delle cause sui sistemi, mettendo a disposizione degli analisti del SOC playbook di sicurezza sviluppati per agevolare le interrogazioni, delegando ad ASDM la complessità legata all'ottenimento dei dati, e abilitando gli analisti a focalizzarsi solo su temi significativi e compromissioni non note.

5.1.4 SIEM: Caratteristiche tecniche della soluzione

Un elemento cardine della piattaforma ASMD è il SIEM basato sulla soluzione ***Splunk***, le cui caratteristiche sono elencate nel §5.1.2. Il RTI ha maturato una lunga esperienza nell'integrazione e onboarding di log custom da un'ampia varietà di Clienti e tecnologie, che ha permesso la strutturazione di un **processo efficiente, flessibile e facilmente adattabile** ad ogni tipo di esigenza. La soluzione Splunk è stata selezionata proprio per la capacità del sistema di poter eseguire l'ingestione del *log* con diverse modalità, che includono, ad esempio, sia l'utilizzo del protocollo ***Syslog***, sia componenti per l'integrazione diretta come il ***DB-Connect*** oppure Agent quali ***Universal/Heavy Forwarder*** per collezionare, comprimere, pre-elaborare e inoltrare i dati in maniera sicura tramite canali cifrati. Inoltre, sono disponibili anche le ***API*** per l'implementazione delle chiamate alle interfacce offerte dai dispositivi da integrare al fine di raccogliere e correlare gli eventi di sicurezza prodotti. Il modello proposto sfrutta la normalizzazione e mapping dei logs tramite lo **Splunk Common Information Model** per garantire una rapida e uniforme fruizione attraverso gli use-case. La soluzione proposta permette di segregare i contesti delle singole PA, e di creare viste personalizzate per ognuna di esse, in modo da avere sempre chiaro il livello di sicurezza dei singoli asset integrati in relazione a tutti i servizi di sicurezza attivi.

Abbiamo inoltre sviluppato negli anni un'ampia libreria di *use-case*, basata sulle tipologie di attacchi osservati nei diversi settori e sulle tecniche identificate dal framework MITRE ATT&CK. Gli use-case vengono ottimizzati e integrati regolarmente attraverso un processo consolidato e un modello di sviluppo agile, a fronte dell'evoluzione delle minacce e sulla base dei feedback da parte degli analisti SOC e dei team coinvolti nella gestione degli incidenti. In aggiunta alle regole fornite dalla libreria, il servizio può sviluppare **regole personalizzate** sulle necessità e fonti dati specifiche dei clienti, attraverso un processo di identificazione e analisi dei requisiti, progettazione, sviluppo, test, messa in produzione e tuning degli *Use Case*.

5.1.5 Automazione e case management: caratteristiche tecniche della soluzione

Accenture ha progettato la piattaforma *ASMD* attorno al *SOAR* prendendo in input le esperienze maturate su altri progetti analoghi su svariate istituzioni governative in particolare italiane, inglesi, americane e dei paesi del nord Europa che hanno indirizzato gli investimenti dell'azienda dedicati allo sviluppo. Si è quindi giunti alla definizione di una libreria proprietaria di oltre 50 playbook capaci di introdurre un livello di **automazione** che partendo dalla *Knowledge Base* condivisa dai SOC di Accenture, porta alla riduzione dei tempi di identificazione, classificazione, notifica e risposta degli incidenti. Si ottiene così l'abbattimento dei falsi positivi e degli eventi duplicati consentendo agli specialisti *SOC* di concentrarsi su indagini di dettaglio e sul miglioramento continuo della qualità del servizio, con un incremento di efficienza misurato di circa il 60%. Quest'ultimo beneficia inoltre di processi strutturati, documentati e tracciabili che garantiscono consistenza nei risultati e relativa misurazione di efficacia rispetto ai KPI. Le **integrazioni** e i **playbook** implementati da Accenture e messi a disposizione della piattaforma ASDM proposto, mettono a disposizione una serie di valori aggiunti in termini di **efficacia di monitoraggio e risposta** alle Amministrazioni, tra cui:

- ***Case Management assistito*:** raccolta degli incidenti sulla base di filtri rilevanti, gestione assistita degli incidenti, arricchimento automatico di incidenti con informazioni di interesse, correlazione tra incidenti diversi e coordinamento delle azioni di risposta tra team distribuiti.
- **Gestione accessi:** blocco degli *account*, *reset password*, attivazione automatica di meccanismi di autenticazione a più fattori.
- **Arricchimento e *Threat Intelligence*:** ricerca automatica di indicatori di compromissione, ricerca e analisi dei risultati di scansioni precedenti, arricchimento delle informazioni raccolte, definizione di uno score complessivo, eventuale *whitelisting/blacklisting* dell'indicatore su base score.
- ***E-mail Gateway*:** download della mail e relativi allegati, blocco/rilascio automatico di mittenti e *URL*, codifica/decodifica degli *URL* nei messaggi, eventuale rilascio di un messaggio in quarantena.
- ***Forensics* e *Malware Analysis***: detonazione automatica di *URL*/allegati, ricerca di esiti per analisi passate, raccolta automatica del traffico di rete e di snapshot delle componenti potenzialmente malevole.
- ***Endpoint Protection e contenimento minacce*:** contenimento automatico di file e servizi, isolamento e contenimento automatico degli endpoint, raccolta di eventi rilevanti per uno specifico *host*, propagazione degli indicatori di compromissione sulle soluzioni di sicurezza installate, verifica della presenza di indicatori di compromissione su altri *host* diversi da quello compromesso.
- ***Firewall, IDPS, Web Gateway*:** raccolta automatica dei flussi di rete, raccolta dei log di rete e correlazione con quelli relativi agli strumenti di sicurezza degli endpoint, creazione/gestione/rimozione di regole e *policy*, aggiornamento delle firme degli strumenti di sicurezza, *blacklist* indirizzi IP/ FQDN.
- ***Vulnerability Management*:** raccolta di informazioni sulle vulnerabilità e correlazione automatica con le informazioni degli altri servizi attivi; è quindi possibile gestire un *triage* dinamico dell'incidente.

Inoltre, l'esperienza pluriennale delle aziende componenti il **RTI** nella ***SOC Automation,*** unita alla relazione di partnership strategica a livello globale con i principali player del settore tra cui *Palo Alto Networks* e *Splunk,* fornisce alle PA contraenti il beneficio del **continuo sviluppo di integrazioni, *use case* e *playbook*** che permettono di indirizzare le minacce emergenti. Accenture rappresenta un partner strategico per Splunk e, insieme a Fastweb, di PaloAlto Networks, con cui condivide l'esperienza accumulata sui Clienti e investe capitali significativi nello sviluppo di capability, asset e metodologie di delivery dal 2016; con oltre 3500 persone certificate su scala globale sulle tecnologie di entrambi i vendor, Accenture è stata riconosciuta da Splunk come *"Solution Partner of the Year"* nel 2019, *"Global Solution Partner of the Year"* nel 2020 e *"Global Sales Partner of the Year"* nel 2021, nonché da PaloAlto Neworks come *"Partner of the Year"* per il 2017, 2018 e 2019. Anche Fastweb vanta una forte collaborazione con Palo Alto Networks, certificata dal livello massimo di partnership "Diamond", ed è stata riconosciuta "Enterprise Service Provider of the Year 2021 – Italia". Un esempio di questo è rappresentato dal ***playbook* di *Threat Hunting*** per effettuare la ricerca proattiva di Indicatori di Compromissione (*IoC*) su larga scala per garantire una rapida identificazione e risposta delle minacce emergenti. Ogni qualvolta le fonti di *Threat Intelligence* identificano nuovi *IoC* rilevanti, quali indirizzi IP, *URL* o *hash* di codici malevoli, il *Playbook* ne esegue in parallelo la ricerca su tutte le istanze delle PA integrate con il servizio SOC nell'arco degli ultimi 90 giorni. Questo permette di industrializzare il processo di ricerca delle minacce, rendendolo continuo e immediato, riducendo la finestra di esposizione al rischio delle Amministrazioni.

5.2 Organizzazione

5.2.1 Strutture coinvolte

Il servizio *SOC* è erogato da un unico gruppo di lavoro *(SOC Team)* con base nel *Centro Servizi*, che risponde a un **Responsabile del Servizio SOC** (RSOC, vale a dire il Service Manager) il quale rappresenta il punto di contatto con il Referente tecnico dell'Amministrazione; il SOC Team è supportato da uno o più *SME* (*Subject Matter Expert*), esperti verticali nelle varie aree di *Cyber Security*. Al suo interno, il SOC Team presenta **tre gruppi di analisti** incaricati dell'analisi e gestione degli incidenti a complessità crescente: L1, L2 e L3. Il servizio si interfaccia inoltre con lo Smart HUB, per supporto nelle attivazioni del servizio, e con i Centri di Competenza/Partnership per competenze specialistiche utili all'erogazione del servizio.

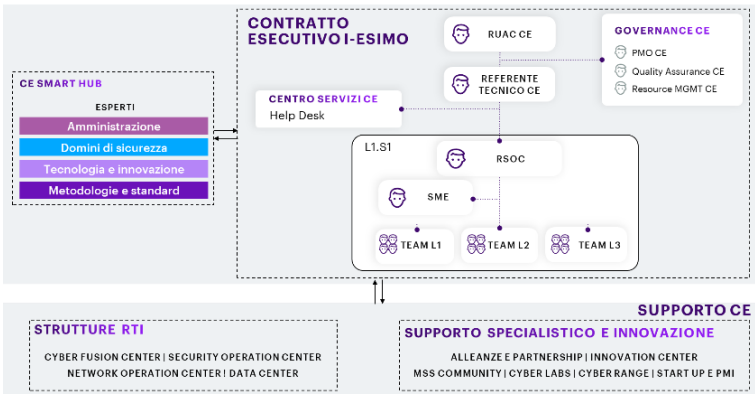


Figura 9 – Strutture coinvolte nel servizio

5.2.2 Team di servizio

Il 'SOC Team' che eroga il servizio è composto da esperti di Sicurezza certificati che operano all'interno di gruppi di lavoro ben definiti con chiara responsabilità e interagiscono tra loro e con l'Amministrazione 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':

FUNZIONE-TEAM	RUOLO / PROFILO	COMPITI E RESPONSABILITÀ
Responsabile del	RSOC / SP	Punto di contatto tra l'Amministrazione e il SOC team con le responsabilità elencate nel §5.2.2 (Security

servizio		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, prioritizza gli allarmi, effettua l'analisi degli eventi e la verifica, verificare la raccolta dei log dalle sorgenti attive, fornisce report predefiniti, propone la riduzione dei falsi positivi, notifica gli eventi alle Amministrazioni. Possiede certificazioni quali: SSCP, CEH.
Supporto di sicurezza Livello 2	Team L2 / Sr-ISC	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. Possiede certificazioni quali: GCIH, GPEN, GCFE.
Supporto di sicurezza Livello 3	Team L3 / Sr-ISC	Investiga eventuali problemi relativi alle funzionalità del SIEM, supporta la risoluzione in caso di interruzione della raccolta dei log, supporta il tuning delle regole esistenti e delle risorse associate, si interfaccia con la PA, raccoglie e trasmette evidenze, valutazione post incidente per miglioramento continuo, fornisce supporto tecnico per escalation in caso di incidenti complessi. Possiede certificazioni quali: OSCP, GREM, GCFA
Specialisti di Cyber Security	SME / SSA	Esperti verticali nelle tematiche Cyber Defense per supporto nell'erogazione del servizio SOC, miglioramenti e risoluzione problemi sulle tecnologie e investigazione complessa in caso di incidente. Possiede certificazioni quali: CCSA, GCTI, certificazioni avanzate di prodotto (Splunk, Cortex XSOAR).
Legenda: SP Security Principal, Sr-ISC Senior Information Sec. Consultant, Jr-ISC Junior Information Sec. Consultant, SSA Sec. Solution Architect		

5.2.3 Security Operation Governance

Data la sua criticità, il servizio utilizza un *framework* di comunicazione che prevede allineamenti a differenti livelli, da quello operativo fino a quello Direzionale/Leadership. Il framework è già attivo su diversi contesti ed è in grado di scalare e indirizzare le esigenze di **PA di diversa dimensione**. La profondità e la frequenza delle interazioni, è dettata dal livello di **complessità e maturità** della PA coinvolta. Il RSOC rappresenta il punto di contatto tra il Referente Tecnico della PA e il SOC Team; ha la responsabilità di: ✓stilare e condividere il **Questionario di Pre-Installazione** (*QPI*) contenente le informazioni necessarie al processo di *onboarding*, i contatti dei referenti operativi della PA e i processi di escalation, ✓valutare e convalidare eventuali fornitori/terze parti/feed che forniranno dati alla **piattaforma di correlazione** (*SIEM*), ✓condividere e confermare le **aspettative** della PA ed evidenziare/indirizzare qualsiasi potenziale disallineamento, ✓creare i **collegamenti** tra i vari referenti dei team coinvolti, ✓rendere **disponibili e accessibili** alla PA le informazioni operative legate al servizio SOC, ✓lavorare a contatto con i referenti della PA per recepire i riscontri operativi e tradurli in attività di **miglioramento continuo**, ✓aiutare a costruire una **Knowledge Base** con informazioni sull'ambiente della PA e sui processi e le procedure del servizio, ✓mantenere contatti regolari con eventuali altri team, esterni all'ambito sicurezza, per condividere informazioni rilevanti che possano aiutare/migliorare l'integrazione e la collaborazione, ✓garantire che il RTI sia informato, come parte del processo di *Change Management*, su tutto ciò che è rilevante per il team di sicurezza o su incidenti operativi ed emergenze, ✓identificare i processi di automazione che facilitino la condivisione delle informazioni e la risposta alle minacce per guidare una **reazione più rapida e accurata**, soprattutto quando sono coinvolti più team.

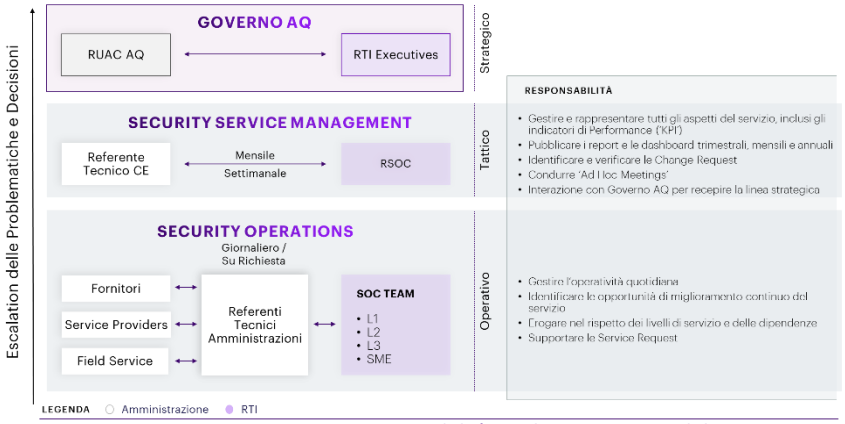


Figura 10 – Interazioni e responsabilità per la Governance del SOC

5.3 Modello Operativo

Il modello operativo del NG-SOC si basa su una stretta collaborazione tra i macro-processi di **Analisi e Monitoraggio della Sicurezza** e **Risposta agli attacchi e incidenti**, come rappresentato in figura.

Nello specifico, il macro-processo di **Analisi e Monitoraggio della Sicurezza** riportato in figura si articola nei sottoprocessi seguenti:

- **Raccolta delle sorgenti dati:** attraverso un processo standard che si avvale di checklist frutto dell'esperienza ventennale di Accenture e di Fastweb nel supporto delle PA, si offre un repository consolidato e scalabile di dati di sicurezza, inclusi eventi, *asset*, flussi e informazioni di contesto. I sistemi di memorizzazione sono gestiti secondo i più moderni standard di sicurezza quali ad esempio FIPS 140-2.
- **Attivazione di *use case* e regole di correlazione:** include la definizione, consolidamento e attivazione di un insieme di regole di correlazione di interesse per lo specifico contesto delle Amministrazioni contraenti.
- **Monitoraggio del SIEM e *alerting*:** il processo garantisce il monitoraggio continuo delle informazioni prodotte dal SOC. Questo include l'utilizzo di dashboard e canali necessari al monitoraggio continuo e completo dei sistemi, che permettano ad analisti, *team lead* e *stakeholder* in generale di avere visibilità sulla postura di sicurezza dell'Amministrazione.
- **Correlazione, identificazione e classificazione degli incidenti**: L'utilizzo di meccanismi di AI, *Analytics* e automazione, in aggiunta alle fonti esterne integrate, permette all'analista di incrementare significativamente la rilevanza e contestualizzazione delle segnalazioni in termini di completezza e accuratezza incrementando così il livello di efficacia del servizio.

Il macro-processo di **Risposta agli attacchi e incidenti** ha la responsabilità di gestire e, in caso, rispondere e notificare eventi di sicurezza nei confronti della PA contraente. Nello specifico, si articola nei seguenti sottoprocessi:

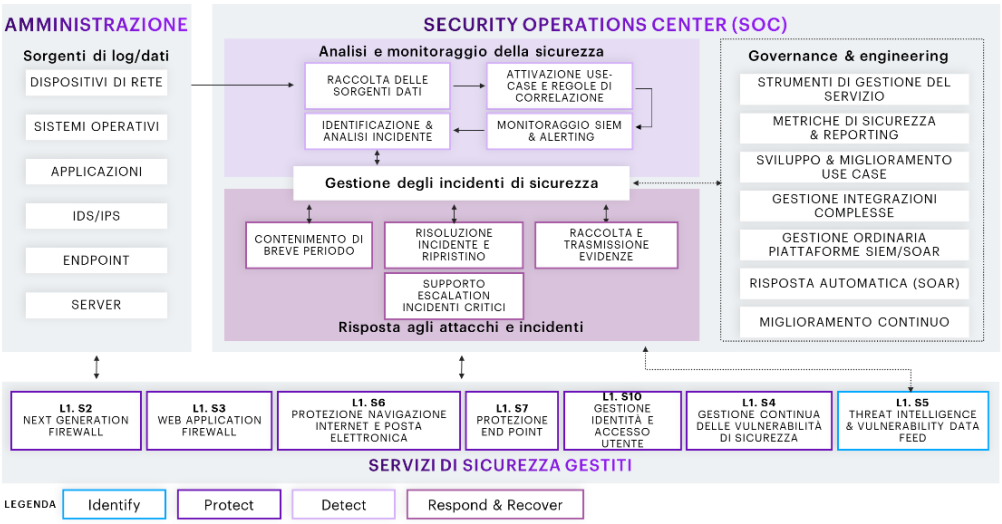


Figura 11 – Modello Operativo del SOC

- **Contenimento di breve periodo:** Identificazione e comunicazione verso la PA delle possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione.
- **Raccolta e trasmissione delle evidenze:** Acquisizione di eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente. Le evidenze digitali raccolte sono poi trasmesse al referente tecnico della PA e archiviate.
- **Risoluzione dell'incidente e ripristino:** Azioni necessarie per rispondere all'incidente in maniera pervasiva. La risoluzione dell'incidente include inoltre una valutazione a posteriori, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza e aumentare l'efficacia del SOC.
- **Supporto escalation incidenti critici:** In caso di incidenti di sicurezza critici sugli ambienti delle Amministrazioni, la cui gestione non rientri nella normale operatività prevista per il SOC, è previsto un processo di escalation verso gli SME del RTI al fine di investigare in maniera estesa sulla natura della compromissione e l'eventuale apertura di un tavolo tecnico con i vendor della tecnologia specifica per assicurare un confronto tempestivo, sfruttando gli accordi di partnership che garantiscono il massimo supporto nell'esecuzione delle attività. Data la natura altamente eterogenea degli scenari possibili, legati necessariamente alla specificità della compromissione, si assume che attività di questo tipo rientrino nel contesto di un ingaggio dedicato dei servizi professionali.

ATTIVITÀ	RTI	AMMINISTRAZIONE
Identificazione	R/A	
Classificazione	R/A	
Notifica	R/A	I
Contenimento	R/A	C
Risoluzione	C	R/A
Ripristino	I	R/A
Lesson Learned	R/A	C
*LEGENDA: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed*		

Figura 12 – RACI per le fasi di gestione degli incidenti

In figura si riporta la RACI relativa al modello operativo del servizio SOC in relazione alle fasi di gestione degli incidenti di sicurezza. L'assegnazione della priorità di gestione verrà effettuata in maniera coerente con i livelli specificati in ambito di gara.

5.3.1 Modalità di erogazione

Al netto della fase di setup iniziale delle soluzioni tecnologiche in uso dal SOC, l'attivazione del servizio per le singole PA passa per un approccio a fasi, con l'obiettivo di identificare e predisporre la raccolta dei log di interesse e attivare le regole di correlazione per lo specifico contesto. Si riporta nel seguito una descrizione delle singole fasi.

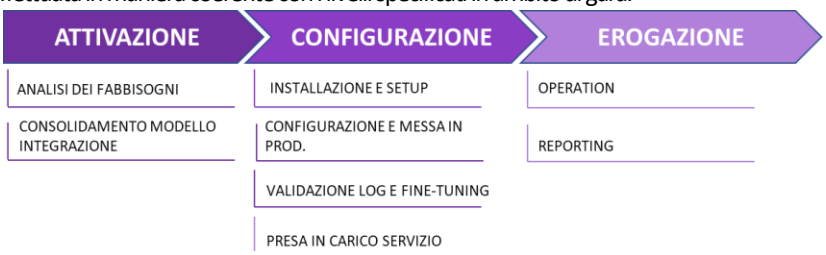


Figura 13 - Modalità di erogazione

ATTIVAZIONE	
Analisi dei Fabbisogni, Piano Operativo e Contratto Esecutivo	**Deliverable**: Piano Operativo e Contratto Esecutivo **Descrizione**: Il Team supporta l'Amministrazione nella stesura del Piano dei Fabbisogni in termini di esigenze di sicurezza, per definire, in particolare: ✓quantità e tipologie dei servizi da richiedere ✓modalità di erogazione e consuntivazione degli stessi ✓tutte le ulteriori caratteristiche utili ottenute dall'analisi del contesto tecnologico e applicativo. Kick off meeting volto ad avviare le attività propedeutiche all'erogazione del servizio riportate nella fase "Configurazione". Il Fornitore procede, quindi, con l'identificazione e contestualizzazione dei servizi, l'eventuale declinazione delle figure professionali e degli strumenti a supporto per finalizzare il Piano Operativo. Espletamenti economici e amministrativi in relazione al Contratto Esecutivo
Consolidamento modello di attivazione SOC	**Deliverable**: "Questionario di Pre-Installazione" (QPI) contenente tutti gli aspetti tecnici e organizzativi dell'ambito di monitoraggio **Descrizione**: Eventuale aggiornamento del Piano di Presa in carico (incorporato nel Piano Operativo). Attività conseguenti di: ✓consolidamento delle soluzioni tecnologiche in ambito ✓identificazione di eventuali prerequisiti di integrazione e raccolta delle sorgenti ✓consegna della documentazione necessaria all'attivazione del servizio ✓identificazione dei responsabili

CONFIGURAZIONE	
Installazione e setup	**Deliverable**: N/A **Descrizione**: Comprende: ✓predisposizione delle componenti di raccolta e inoltro dei log ✓installazione delle componenti nelle specifiche amministrazioni ✓attivazione dei flussi di rete e dati in ingresso e uscita necessari all'attivazione
Configurazione e messa in produzione	**Deliverable**: N/A **Descrizione**: Comprende: ✓configurazione dei dispositivi e sistemi in ambito ✓configurazione delle componenti di back-end delle soluzioni SIEM e SOAR ✓configurazione delle componenti di raccolta e inoltro
Validazione dei log e fine-tuning	**Deliverable**: N/A **Descrizione**: Comprende: ✓controllo della qualità dei log e rimozione dei falsi positivi ✓configurazione sicura delle componenti installate (hardening) ✓convalida degli eventi e attivazione dei casi d'uso
Presa in carico	**Deliverable**: "Checklist di Presa in Carico" (CPIC) **Descrizione**: Presa in carico delle piattaforme e avvio del monitoraggio attivo per la

CONFIGURAZIONE	
	specifica Amministrazione.

EROGAZIONE	
Operation	**Deliverable**: Report attività manutenzione **Descrizione:** Erogazione continuativa del servizio SOC come da modello operativo descritto al §5.3.
Reporting	**Deliverable**: Report di servizio **Descrizione**: Generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF

5.3.2 Controllo di Qualità e miglioramento continuo

Il processo di miglioramento continuo proposto è parte integrante del CDOM e, nello specifico, del servizio SOC; prevede un monitoraggio costante su base trimestrale degli indicatori di performance e qualità sopra definiti da parte del RSOC. I gap identificati rispetto ai livelli attesi vengono analizzati e catalogati secondo la combinazione di impatto sulla qualità e complessità di implementazione. Il RSOC disegna, discute e condivide con la PA una roadmap suddivisa tra azioni di tipo quick-win a breve e medio termine e prevede una serie di aree di intervento che riportiamo a titolo esemplificativo e non esaustivo, suddivise per ambiti tematici:

- **Tecnologica** (es. rivisitazione delle regole dei dispositivi, tuning dei log inviati, ampliamento e integrazione delle sorgenti, valutazione di ulteriori prodotti di sicurezza, affinamento della use-case library e/o dei playbook per la corretta prioritizzazione e l'analisi dei trend, tuning delle regole della piattaforma ASDM)
- **Processi** (es. revisione delle procedure di escalation, rivisitazione della matrice RACI, affinamento del processo di OnBoarding, eventuale ri-allineamento con il contesto di business e i nuovi scenari di minaccia)
- **Persone** (es. riassegnazione del team a supporto, training mirato ai referenti tecnici dell'Amministrazione, del SOC Team e delle terze parti).

In caso di **specifiche esigenze** emerse durante le regolari **service review** condivise con la PA, vengono organizzati workshop tematici dedicati, ove possibile, svolti in ambienti immersivi come i centri di innovazione citati al §17, sfruttando approcci come il **Design Thinking,** agevolato da simulazioni di miglioramento dei processi su **SPARK** (cfr. §4.8). Strumento di ausilio alle service review è **LimeSurvey** (cfr. §16.1.1) per raccogliere livello di gradimento e suggerimenti. Gli argomenti di cybersecurity trattati possono essere svariati, ad esempio: Strategia di CyberSecurity, Security Operations, Strategie di Platform e Content Development, Application Security, Insider Threat, Adversary Simulation. I risultati possono portare a una rivisitazione dell'Operating Model di Sicurezza dell'Amministrazione, una Roadmap evolutiva, un'analisi del Modello di Maturità, oppure uno specifico e dettagliato "piano di azione".

Inoltre, il capitale umano e professionale del pool di risorse impiegato che vanta un numero considerevole di certificazioni di settore, non solo opera all'interno del Servizio SOC mantenendo i più alti standard qualitativi, ma **partecipa attivamente alla CyberSecurity Room** come descritto al §17'. In questo modo vengono recepite le esigenze del Servizio SOC che, tradotte ove possibile in stream innovativi, concorrono al miglioramento costante dell'efficacia del servizio.

Per raggiungere tale scopo risulta fondamentale una corretta ed efficace definizione degli indicatori di prestazione (KPI), i quali sono stati definiti a partire dai seguenti principi: ✓i '*KPI*' possono differire o essere aggregati in base all'audience di destinazione ✓la valutazione deve essere fatta non solo sui numeri relativi, ma anche per i valori assoluti ✓i valori isolati non sono sufficienti, anche il trend e la progressione sono rilevanti ✓un singolo '*KPI*' può essere suddiviso in più valori, raggruppati per unità di business, geograficamente, ecc. ✓i picchi o i cambiamenti significativi devono essere analizzati e spiegati. Sulla base della valutazione dei '*KPI*' vengono definite e implementate le azioni di miglioramento, concordate con adeguati livelli di gestione.

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, in aggiunta agli indicati richiesti dal bando di gara si illustrano gli ulteriori indicatori di qualità previsti per il servizio in oggetto:

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "SOC"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_PICM	Presa in carico di un incidente da parte dei sistemi di monitoraggio - Tempo trascorso dall'accadimento dell'incidente alla registrazione sul sistema di TT da parte dei sistemi di monitoraggio	[#incidenti presi carico nei tempi previsti / #totale incidenti aperti] x 100 Tempo previsto di registrazione < 10'	Trimestre	95%
PCI_TIIS	Tempo di prima investigazione per incidenti di sicurezza	Come TIIS ma con frequenza maggiore e soglia più sfidante	Mensile	PCI_TIIS = 0 con tempi massimi di consegna della "prima investigazione" dimezzati rispetto a TIIS
KPI_ISU	Incidenti segnalati dagli utenti	Num. incidenti di cybersecurity segnalati dagli utenti e non dai sistemi di monitoraggio	Trimestre	Atteso un non incremento rispetto alla rilevazione precedente

5.3.3 Report aggiuntivi per l'Amministrazione

Il RTI ritiene il reporting e miglioramento continuo attività chiave per la completa ed efficace gestione dei servizi in ambito, in quanto componenti fondamentali nel monitoraggio e misurazione dell'efficacia e della maturità dei servizi erogati attraverso: ✓report forniti all'Amministrazione ✓analisi delle risorse e delle attività in base ai KPI definiti ✓supporto alla gestione tramite l'analisi dei risultati ottenuti ✓elaborazione di raccomandazioni e punti di miglioramento. In aggiunta ai report richiesti dal capitolato che verranno prodotti durante la normale operatività del servizio SOC, offriamo i seguenti report aggiuntivi:

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sulle tecnologie SOC solo qualora fossero previsti possibili impatti di servizio.

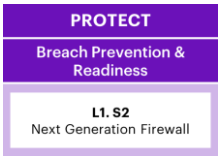
5.4 Interazioni

5.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
Next Generation Firewall	Log di audit ed eventi verso il SIEM	Input/ Output	I sistemi inviano log al SIEM affinché gli eventi generati dai NGFW possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza. Attivazione di eventuali azioni di risposta automatica.
Web Application Firewall	IoC	Input/ Output	Gli IoC provenienti dalla piattaforma di Threat Intelligence sono raccolti in input dai Next Generation Firewalls per limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash). Attivazione di eventuali azioni di risposta automatica.
Gestione continua delle vulnerabilità	Vulnerability Report	Input	Le vulnerabilità identificate dal processo di Vulnerability management possono essere correlate agli eventi di sicurezza per ridurre i falsi positivi e innalzare la criticità di eventi identificati sui target.
Threat Intelligence & Vulnerability Data feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence possono essere correlati agli eventi di sicurezza per identificare più rapidamente le nuove minacce in modo proattivo o per identificare minacce già presenti nel perimetro non precedentemente identificabili.
Protezione navigazione internet e posta elettronica	Log di eventi verso il SIEM	Input	I sistemi inviano log al SIEM affinché gli eventi generati dai sistemi di Navigazione Internet e di Posta Elettronica possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza
Protezione end point	Log di eventi verso il SIEM	Input / Output	I sistemi inviano log al SIEM affinché gli eventi generati dai sistemi di Protezione End Point possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza. Attivazione di eventuali azioni di risposta automatica.
Gestione identità e accesso utente	Log di audit ed eventi verso il SIEM	Input / Output	I sistemi inviano log al SIEM affinché gli eventi generati dai sistemi di Gestione identità ed accesso utente possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo e arricchire la ricostruzione della timeline di incidenti di sicurezza. Attivazione di eventuali azioni di risposta automatica.
Innovazione	CyberSecurity Room	Input / Output	Recepire le esigenze del Servizio SOC e tradurle ove possibile in stream innovativi, in modo da concorrere al miglioramento costante dell'efficacia del servizio.

6 PROPOSTA PROGETTUALE PER IL SERVIZIO "NEXT GENERATION FIREWALL"

6.1 Soluzione Proposta



Il **modello CDOM** (cfr. §§1 e 3.3) colloca questo servizio nel dominio di sicurezza "**Breach Prevention & Readiness**" allineata alla Funzione NIST "**Protect**".

Il servizio di **Next-Generation Firewall** (NGFW) rappresenta uno degli asset fondamentali del Centro servizi, in quanto consente di implementare i controlli di sicurezza essenziali alla protezione di rete, applicando restrizioni alle comunicazioni esterne o interne alla singola PA, limitando gli accessi delle singole risorse ai soli flussi di traffico definiti come leciti. Ciò è possibile utilizzando policy basate non solo sui **meccanismi classici di segregazione di rete L3 (network) e L4 (trasporto)**, ma anche su **capacità di analisi del layer applicativo**, ispezionando il contenuto dei messaggi scambiati con protocolli quali HTTP, FTP, SIP, ecc. che consentono di implementare **filtri molto più dettagliati** rispetto alle funzionalità base dei firewall standard. Ulteriori **elementi di valore** sono rappresentati dalla possibilità di definire regole basate sull'identità dell'utente, abilitando l'infrastruttura ad ammettere flussi di traffico in base al **principio least-privilege** e di procedere all'**ispezione di traffico TLS/SSL** necessaria per controllare efficacemente il traffico cifrato che costituisce gran parte del traffico interno ed esterno alle PA.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: più di 50, tra cui Ministero delle Infrastrutture e dei Trasporti, Regione Lombardia, AgID, RAI

Private: NEXI, A2A, ENI, primario operatore finanziario

Descrizione di un caso di successo - **Ministero delle Infrastrutture e dei Trasporti - Provveditorato Interregionale alle Opere Pubbliche per il Veneto, Trentino Alto Adige e Friuli Venezia Giulia** →**Esigenza** - Realizzazione dell'infrastruttura di sicurezza di rete del sistema "MO.Se" di Venezia, atta a contrastare eventuali attacchi e minacce apportate all'infrastruttura di rete ed ai servizi ospitati in Data Center →**Soluzione** – Fastweb ha realizzato un'architettura caratterizzata da un elevato grado di flessibilità, prestazioni e resilienza. Sono state condotte campagne di Network penTesting di tipo blackbox/greybox che hanno mostrato l'efficacia dei presidi di sicurezza Fortigate nel resistere agli attacchi simulati →**Benefici** - Il beneficio più evidente è stato una riduzione del rischio complessivo dell'intera architettura di rete: ✓forte resilienza dei bastioni Fortigate di resistere alle minacce garantendo una riduzione della superficie d'attacco e un miglioramento della postura di sicurezza del Network e dei sistemi, come confermato dai dati del servizio SIEM che hanno mostrato il trend di riduzione delle minacce intercettando un numero di IoC molto minore rispetto alla soluzione di sicurezza precedente ✓capacità di integrarsi con la soluzione Active Directory DS permettendo di implementare logiche di policy basate sull'identità dell'utente

6.1.1 Funzioni offerte

Il servizio prevede: un livello di **Interfaccia PA** utile all'interazione con il servizio, un livello di **Erogazione** in cui sono espletate le funzioni principali del servizio, un livello di **Automazione** (intelligent layer) che aggiunge funzioni avanzate, un livello **Interazioni** per le relazioni con gli altri servizi. I livelli comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative**, descritte di seguito.

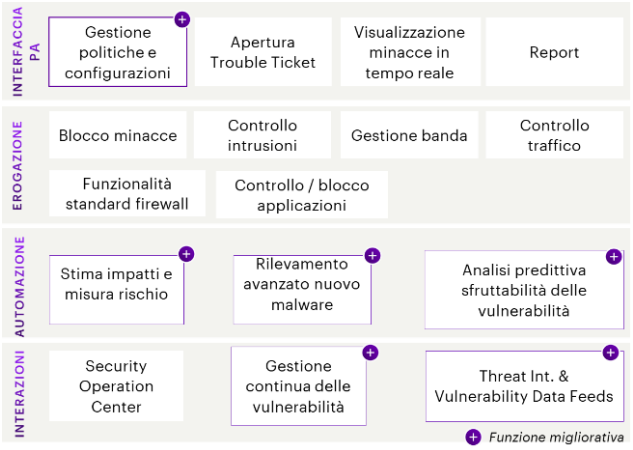


Figura 14 - Funzioni del servizio

- **Gestione politiche e configurazioni**: funzioni di "Geo-IP filtering e Geo-Blocking" per consentire la creazione di regole di policy da applicare a specifici paesi e/o regioni geografiche;
- **Stima degli impatti e misura del rischio**: la funzione esegue le stime di impatti e rischio sulle configurazioni implementate o che si prevede di implementare fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura. Tali valutazioni sono effettuate tenendo in considerazione: ✓la classificazione delle informazioni trattate, ✓la criticità del servizio abilitato per la PA, ✓le dipendenze e interazioni con altri servizi, funzioni e sistemi;
- **Rilevamento avanzato del malware**: la funzione prevede metodi avanzati di 'malware detection' fortemente potenziate dall'integrazione con il servizio di Threat Intelligence, nonché con il SOC e prevedono azioni automatizzate per isolare comportamenti di rete anomali che possono segnalare la presenza di malware noto o di possibili varianti;
- **Analisi predittiva della sfruttabilità delle vulnerabilità**: la funzione combina dati e informazioni sulle minacce da più fonti analizzando con un algoritmo di apprendimento automatico basato su ML, per anticipare la probabilità che una vulnerabilità venga sfruttata, anche grazie all'**Interazione con i servizi** di SOC, **ma anche di Gestione continua delle vulnerabilità e Threat Intelligence e Vulnerability Data Feeds** (cfr. §6.4.1).

6.1.2 Architettura tecnologica

La soluzione tecnologica NGFW offerta dal Centro Servizi è basata su tecnologia **Fortinet**, riconosciuta come **leader sul mercato** come attestato da Gartner in entrambi i report Magic Quadrant 2020 per Network Firewall e WAN Edge Infrastructure. Accenture, Fastweb e Fortinet vantano una pluriennale partnership che ha consentito di integrare tali tecnologie in sistemi informativi complessi ma, soprattutto, di definire una metodologia standard per poterla portare rapidamente e con strumenti di configurazione standard presso altri Clienti. In particolare Fastweb è il principale partner di Fortinet nell'ambito della PA. Il NGFW Fortinet, denotato dalla classe di prodotti **Fortigate**, fornisce una **ampia e consolidata copertura dei requisiti** di tecnico-funzionali espressi nel capitolato e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi.

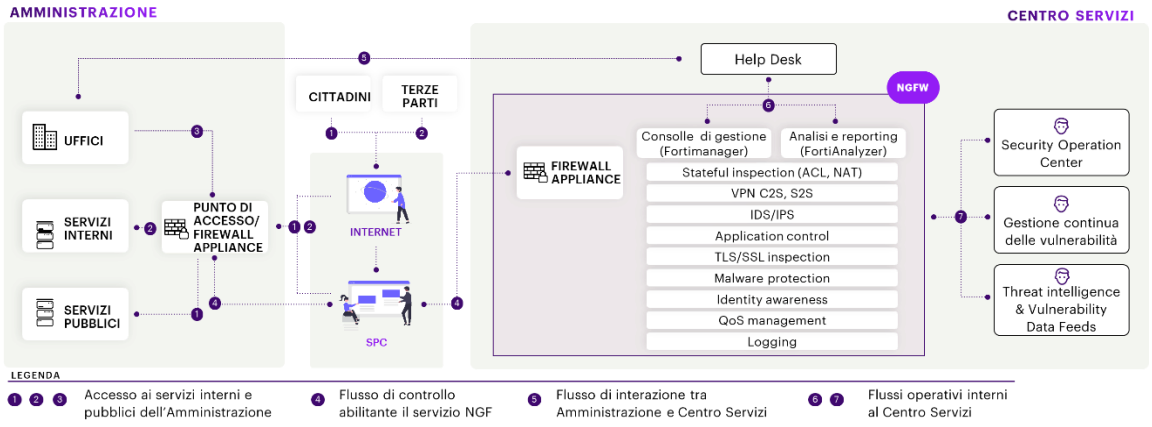


Figura 15 - Architettura tecnologica NGFW

L'architettura prevista per la fornitura di servizio prevede l'integrazione del NGFW (o gateway), nella sua forma fisica o virtuale, localmente presso la singola PA oppure remotamente presso il Centro Servizi (scelta subordinata agli accordi con la PA contraente), predisponendo una console di gestione centralizzata in esercizio presso lo stesso Centro Servizi. La scelta architetturale inerente all'installazione on-premise degli appliance presso la PA oppure remotamente presso il Centro Servizi sarà eseguita durante la fase di attivazione del servizio, subordinata alle caratteristiche dell'infrastruttura di rete della singola sede piuttosto che alla lista di servizi di sicurezza NGFW da attivare. La console di gestione centrale, denominata **FortiManage**r, consente di avere una visibilità generale sullo stato dei singoli gateway, permettendo la configurazione della soluzione e il relativo monitoraggio anche grazie all'integrazione con la soluzione SIEM, gli Active Directory o altri user repository. La possibilità di avere in unico punto la gestione di molteplici PA è garantita dal concetto di **Dominio Amministrativo** (ADOM – Administrative Domain), che consente la definizione di ambienti completamente indipendenti. Al fine di garantire funzionalità avanzate di analisi e reporting, sarà implementato un ulteriore elemento centrale di analisi, logging e reporting, denominato **FortiAnalyzer**, deputato alla raccolta e correlazione dei messaggi provenienti da tutti gli apparati attivi, con la possibilità di produrre report a diversi livelli di sintesi.

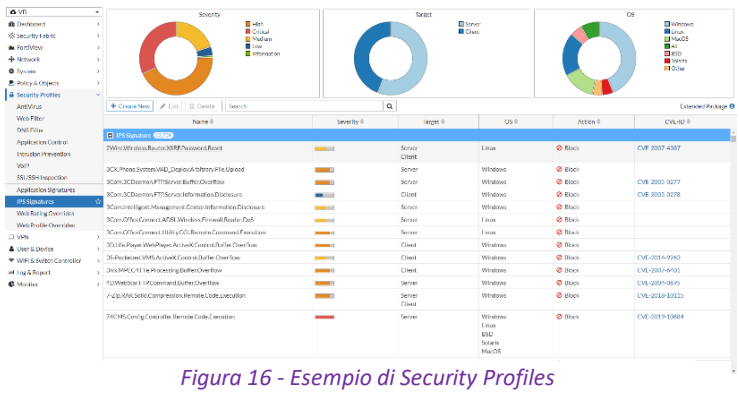


Figura 16 - Esempio di Security Profiles

6.1.3 Caratteristiche tecnologiche e prestazionali, comprese quelle migliorative

Gli appliance firewall saranno disponibili in versione chassis fisico o macchina virtuale al fine di garantire la **massima adattabilità** al contesto di rete e vincoli tecno logico/operativi. L'utilizzo di una forma piuttosto che di un'altra sarà concordata e selezionata dalla specifica PA.

Le caratteristiche degli **appliance FortiGate** vanno oltre quelle standard di stateful firewall, in quanto dotati di capacità di **ispezione dei contenuti avanzate fino**

al livello 7 del modello ISO/OSI. Questo garantisce capacità di ispezione sul layer applicativo con funzionalità di Intrusion Prevention**,** Antivirus, Cloud Sandbox, Application Control e Web Filtering, disponibili come security profile. In figura si fornisce un esempio della dashboard di analisi per erogare "IDS e IPS".

In particolare, questo tipo di appliance consente di attivare in maniera granulare tali funzionalità, associando uno o più security profile alle specifiche policy di accesso (ACL). In accordo con le **best practice di settore**, per ciascuna tipologia di traffico sarà predefinito un set di profili di sicurezza da abilitare su ciascuna categoria di traffico. Tuttavia, sarà possibile richiedere ed evadere richieste di apertura e controllo del traffico su cui abilitare o meno, determinati servizi in accordo con gli standard della specifica PA. In generale, saranno definite linee guida di sicurezza infrastrutturale che permetteranno di identificare flussi di comunicazione pre-approvati per i quali non è necessaria un'approvazione esplicita. In accordo con la PA sarà possibile definire un flusso di approvazione esplicito del provisioning delle regole in caso di deroga allo standard pre-approvato piuttosto che sempre necessario per ogni singola richiesta.

Service	Action	NAT	Security Profiles	Log
SSH UDP-22	ACCEPT	Disabled	SSL no-inspection	UTM
ALL	ACCEPT	Dyna_2...	SSL no-inspection	UTM
ALL	ACCEPT	NAT IN...	WEB web_monitor APP application_monitor SSL certificate-inspection	All
HTTP HTTPS	ACCEPT	pool_2...	WEB web_basic_security APP application_monitor SSL certificate-inspection	All

Figura 17 - Applicazione granulare security profiles per singola ACL

Inoltre, un aspetto **migliorativo** rispetto al modello di cybersecurity Zero Trust, è la possibilità di poter impostare **regole di accesso basate sull'identità dell'utente, indipendentemente dalla network location sorgente**. È importante quindi specificare che mediante un'integrazione con l'infrastruttura di autenticazione, quale ad esempio Active Directory, è possibile implementare policy di accesso specifiche per singoli utenti o gruppi di utenti, in base al principio del least-privilege. Considerando il contesto distribuito di accesso alle risorse, con un numero sempre maggiore di utenti in smart working, questa feature diventa indispensabile per garantire una **user-experience soddisfacente**. Inoltre, come elemento **distintivo e migliorativo** occorre considerare l'**integrazione dei gateway con la piattaforma di Threat Intelligence** (TIS) proprietaria di Accenture (cfr. §10.1.3), con la quale sarà **immediata** la distribuzione di IOC associati a URL, IP, domini e file malevoli per bloccare l'interazione degli asset della PA con risorse malevoli. Questa funzionalità è particolarmente utile nel caso sia necessario attuare una risposta immediata ad eventi di cybersecurity.

I NGFW Fortinet soddisfano appieno le **esigenze di prestazioni delle architetture IT ibride e hyperscale**, permettendo alle PA un'esperienza utente ottimale e gestire al meglio i rischi di cyber security. In linea con questo requisito e con le indicazioni formulate in capitolato, saranno forniti gateway con throughput diverso a seconda delle necessità delle singole PA.. I singoli componenti saranno aggiornati in base alle roadmap evolutive del vendor e le date pubblicate di End of Life e End of Support, al fine di garantire la **disponibilità in esercizio di appliance continuamente aggiornate e supportate**.

Ulteriore elemento **migliorativo** rispetto ai requisiti da capitolato riguarda i **livelli prestazionali** degli apparati che sono assicurati da una **elaborazione del traffico realizzata prevalentemente a livello hardware, anziché software, mediante l'utilizzo di circuiti integrati denominati Secure Processing Units (SPU)**. In particolare, le SPU hanno il compito di eseguire funzioni di sicurezza ad alto impatto computazionale come la decrittazione TLS/SSL (incluso TLS1.3), IPS e antivirus, in modo che la CPU centrale possa svolgere altre attività di elaborazione del traffico, **evitando impatti sulla fruizione dei servizi protetti dal gateway e impatti sulla esperienza utente**.

6.2 Organizzazione

6.2.1 Strutture coinvolte

Il servizio NGFW è erogato da un team specializzato su servizi di sicurezza infrastrutturale, che risponde a un **Responsabile del servizio;** il team è supportato da uno **SME** (Subject Matter Expert) esperto su tecnologie NGFW. Come per tutti i servizi, è previsto il supporto delle seguenti strutture:

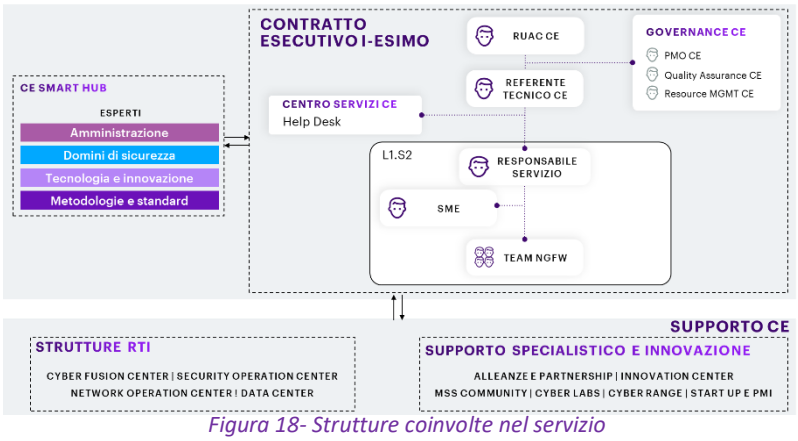


Figura 18- Strutture coinvolte nel servizio

- **CE SMART HUB**: team di esperti con lo scopo di fornire un contributo fondamentale in fase di Attivazione del servizio poiché, grazie alle loro specializzazioni su diversi Clienti, tecnologie e metodologie/standard, supportano il design del servizio in modo che possa erogare con il più alto livello di qualità le richieste della PA contraente. L'HUB sarà poi disponibile in corso di Erogazione in tutti i casi in cui il team del servizio abbia necessità di contributi specialistici nei domini sopra citati (es. è possibile richiederne l'intervento per supportare la PA nell'integrazione del gateway e l'abilitazione dei profili di sicurezza).
- **Centri di Competenza/Partnership** che forniscono competenze specialistiche utili all'erogazione del servizio. In particolare, il team di lavoro avrà la possibilità di avvalersi del supporto fornito dai CdC Infrastrutture (cfr. §3.x) e dai vendor.

6.2.2 Team del servizio

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
Governo del Servizio	Responsabile del servizio / Sr-ISC	Supporta la PA per la redazione del Piano dei Fabbisogni, redige il Piano Operativo. Coordina le attività del servizio per garantire che i risultati siano ottenuti nei tempi e con le modalità previsti. Rappresenta il punto di contatto con la PA; è incaricato della comunicazione con gli altri servizi e della condivisione delle informazioni.
SME NGFW	Supporto al team NGFW / SSA	Offre consulenza nella risoluzione di attività critiche (Incident, Change), problemi infrastrutturali o progetti specifici. È coinvolto nell'ottimizzazione del Servizio e supporta la PA nell'evoluzione dell'infrastruttura.
NGFW team	L2 Security Engineer / Sr-ISC	Supporta e integra le attività del L1 Security Engineer e si attiva per incident di priorità elevata e change complesse. Attiva il supporto dei Vendor e gestisce l'andamento della richiesta sino alla chiusura.

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
NGFW team	L1 Security Engineer / Jr-ISC	Registra il ticket e ne assegna la priorità, eseguendo l'analisi e la diagnosi iniziale. Esegue procedure per la risoluzione dei ticket o l'applicazione di workaround, attivando eventualmente procedure di escalation.

Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect

6.3 Modello operativo

6.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

Figura 19 - Modello operativo

6.3.2 Modalità di erogazione

Di seguito la descrizione delle attività.

ATTIVAZIONE	
Analisi dei Fabbisogni, Piano Operativo e Contratto Esecutivo	**Deliverable**: Piano Operativo e Contratto Esecutivo **Descrizione**: Il Team supporta la PA nella stesura del Piano dei Fabbisogni in termini di **esigenze di sicurezza**, per definire, in particolare: ✓quantità e tipologie dei servizi da richiedere ✓modalità di erogazione e consuntivazione degli stessi ✓tutte le ulteriori caratteristiche utili ottenute dall'analisi del contesto tecnologico e applicativo. Il Fornitore procede, quindi, con l'identificazione e contestualizzazione dei servizi, l'eventuale declinazione delle figure professionali e degli strumenti a supporto per finalizzare il Piano Operativo. Espletamenti economici e amministrativi in relazione al Contratto Esecutivo.
Presa in carico	**Deliverable**: Piano di Presa in carico aggiornato, Verbale di completamento del passaggio di consegne, verbali di SAL **Descrizione**: Eventuale aggiornamento del Piano di Presa in carico (incorporato nel Piano Operativo). Attività conseguenti di: ✓allocazione delle risorse ✓predisposizione strumenti ✓configurazione del Portale della Fornitura ✓condivisione ed eventuale adattamento del processo di gestione degli incidenti ✓predisposizione della documentazione sulle modalità di misurazione degli Indicatori di Qualità. Ove richiesti, ✓acquisizione di know how relativo al contesto organizzativo, tecnologico e funzionale ✓acquisizione di standard, modalità operative, linee guida e metodologie in uso presso la PA. Governo e Monitoraggio delle attività. Kick off meeting volto ad avviare le attività propedeutiche all'erogazione del servizio riportate nella fase "Configurazione"

CONFIGURAZIONE	
Installazione e setup	**Deliverable**: N.A. **Descrizione**: All'interno di questo processo rientrano: ✓Consegna dell'apparato presso la PA (consegna fisica o OVA) ✓Setup iniziale HW (rack & stack) o vHW (deployment virtual appliance) ✓Setup configurazione (major and minor version, patches, interfaccia management) ✓Integrazione nella rete della PA ✓Integrazione con le piattaforme centralizzate
Configurazione e messa in produzione	**Deliverable**: N.A. **Descrizione**: All'interno di questo processo rientrano: ✓Configurazione delle policy standard ✓Configurazioni specifiche rispetto al CE, eventuale porting di configurazioni da appliance esistenti ✓Test della configurazione ✓Passaggio in produzione ed eventuale swap da sistemi pre-esistenti ✓Tuning delle funzionalità attivate ✓Supporto post passaggio in produzione

EROGAZIONE	
Gestione ciclo di vita policy	**Deliverable**: N.A. Descrizione: ✓Creazione e modifica di policy di sicurezza ✓Estrazione informazioni quali esportazione di log, accessi, policy attive o procedure in essere
Operation	**Deliverable**: Report attività manutenzione **Descrizione**: Gestione di incidenti o problemi mediante: ✓l'applicazione di soluzioni permanenti utili a risolvere l'incidente ✓l'applicazione di workaround e analisi successiva della root cause per l'eliminazione definitiva di incidenti e problemi. Applicazione di aggiornamenti software, hotfix, operazioni di riavvio di specifici processi applicativi. Verifica funzionalità di base per alta affidabilità, backup e monitoraggio infrastrutturale
Reporting	**Deliverable**: Report di servizio **Descrizione**: Generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF

CHIUSURA	
Passaggio di consegne	**Deliverable**: Piano di Trasferimento di fine fornitura, Verbali di SAL, Reporting finale delle attività svolte **Descrizione**: ✓Sessioni di lavoro per il passaggio della conoscenza e sua verifica. ✓Governo e monitoraggio e supporto alle attività.
Consegna dei dati dell'Amm.ne	**Deliverable**: Dati **Descrizione**: Sono riconsegnati i dati riguardanti la PA che sono stati utilizzati durante il periodo di erogazione
Consegna della documentazione	**Deliverable**: Documentazione tecnica **Descrizione**: Verifica e Consegna della documentazione tecnica completa e aggiornata che è stata prodotta durante il periodo di erogazione

6.3.3 Livelli di assistenza

Il Modello Operativo per l'erogazione di **tutti i servizi** si basa su **tre livelli di lavorazione**, più un quarto livello per l'interazione con i Vendor tecnologici: ✓Il **Primo Livello (L1)** corrisponde all'Help Desk del Centro Servizi che effettua triage e ingaggia, laddove non riesca a risolvere autonomamente il ticket aperto dall'Amministrazione, il Secondo Livello ✓Il **Secondo Livello (L2)** corrisponde al team di specialisti dello specifico servizio che operano all'interno del Cento Servizi ✓Il **Terzo Livello (L3)** corrisponde ad esperti tecnologici (resi disponibili dal RTI), che intervengono laddove necessario per la risoluzione di incident critici e/o per interventi particolarmente complessi. Inoltre, si occupa dell'eventuale coinvolgimento dei Vendor Tecnologici **(L4)**. Tutte le interazioni tra i livelli sono registrate sulla

piattaforma di ticketing, che permette il tracciamento delle richieste e, in caso di mancata risoluzione da parte dei team di supporto coinvolti, l'attivazione delle procedure di escalation e il reporting relativo su SLA e KPI.

Il Modello permette al Fornitore di **massimizzare l'efficienza** e alla PA di **accedere a tutti gli skill necessari** a seconda delle esigenze che emergeranno durante il ciclo di vita del servizio. Tutte le procedure operative sono definite con la PA durante la Presa in Carico.

6.3.4 Controllo di Qualità

Già nella presente offerta il RTI propone degli indicatori per ciascun servizio. A seguire, essi potranno essere rivisti per meglio rappresentare la qualità dei servizi. Gli Indicatori da monitorare rientrano nelle seguenti categorie: ✓**Indicatori di Qualità** (IQ) previsti negli atti di gara, eventualmente ampliati con **Indicatori di Qualità Aggiuntivi** (IQA) proposti nella presente offerta ✓**Parametri di Controllo Interno** (PCI) - collegati agli IQ/IQA per l'identificazione anticipata di potenziali rischi, non hanno impatto contrattuale ✓**Indicatori Chiave di Performance** (KPI) - valutano il contributo dei servizi al raggiungimento di obiettivi di business definiti con la PA in avvio di Fornitura in base ai Fattori Critici di Successo (CSF), non hanno impatto contrattuale ma sono funzionali ad identificare segnalazioni da presentare al Cliente.

Di seguito gli indicatori previsti per il servizio in oggetto (data la natura estremamente tecnica di questo servizio non sono applicabili KPI).

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "NEXT GENERATION FIREWALL"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSA	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta	*Data_Notifj* = Data Ora di inoltro al SOC della segnalazione *Data_Incj* = Data Ora dell'incidente TNSA = $\sum_{J=1}^{n} Data\_notifj - Data\_Incj$	Trimestre	<1 ora per il 90% degli incidenti
PCI_TNSA	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta	Come IQA_TNSA	Mensile	<1 ora per il 95% degli incidenti

6.4 Interazioni

6.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
SOC	Log di audit ed eventi	Output	I sistemi inviano log al SIEM affinché gli eventi generati dai NGFW possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni di rilievo ai fine della cybersecurity e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza
Gestione continua delle vulnerabilità	Vulnerabilità in essere e potenziali	Input/ Output	Gli apparati scambiano con il servizio informazioni relative alle vulnerabilità identificate sui sistemi e relative configurazioni e ricevono informazioni in merito alla relativa criticità e prioritizzazione
Threat Int. & Vulnerability Data Feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence sono raccolti in input dai gateway FortiGate per limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash)

6.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui NGFW solo qualora fossero previsti possibili impatti di servizio.

6.5 Capacità di fornire visibilità e controllo degli utenti per creare policy, generare report ed eseguire indagini forensi

L'architettura e la tecnologia del servizio NGFW sono ideati per garantire la possibilità di avere un **controllo puntuale delle operazioni ammesse** agli utenti (in linea con il modello Zero Trust) e la possibilità di **analizzare i flussi di traffico sia a scopi di reportistica sia per esecuzione di indagini forensi** a seguito di incidenti di cybersecurity. L'implementazione di queste due macro-funzionalità è possibile mediante le tecnologie:

- **Fortinet Single Sign-On (FSSO)**, funzionalità disponibile sui gateway tramite la quale è possibile recuperare le informazioni di autenticazione degli utenti, con un approccio Agent-Based o Agentless, in modo da applicare in maniera trasparente policy user-based;

  FortiAnalyzer, elemento centrale dell'architettura che consente di analizzare e riassumere molteplici aspetti degli eventi registrati sui gateway, quali policy applicate, tentativi di accesso, performance dei dispositivi, sia a scopi reportistici che per condurre attività forensi e di risposta agli incidenti.

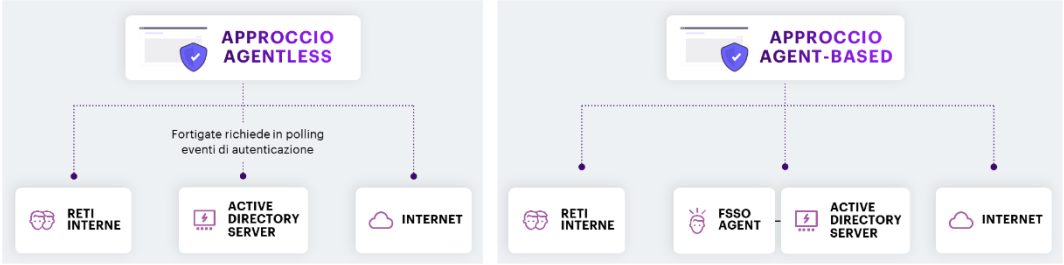


Figura 20 - Metodologie principali per implementazioni di policy basate sull'identità dell'utente

La funzionalità FSSO potrà essere implementata in diversi modi, a seconda del contesto della singola PA e dei requisiti raccolti durante la fase iniziale di ingaggio. Le modalità principali di implementazione sono le seguenti e hanno l'obiettivo di associare un IP ad una identità, al fine di applicare policy su base utente: ✓**Agentless** – il gateway è configurato in modalità polling al fine di recuperare gli eventi di autenticazione dall'identity provider o dall'identity store ✓**Agent-based** – un

FSSO agent è installato sui domain controller dell'Active Directory e inoltra gli eventi di autenticazione al Fortigate.

Esistono altre tecniche di implementazione che possono essere anche non trasparenti all'utente, come ad esempio l'autenticazione esplicita su un portale dell'appliance NGFW. Le modalità saranno ad ogni modo valutate e concordate durante la fase di attivazione del singolo CE. Si riporta in figura un esempio di applicazione di policy basata su utenti.

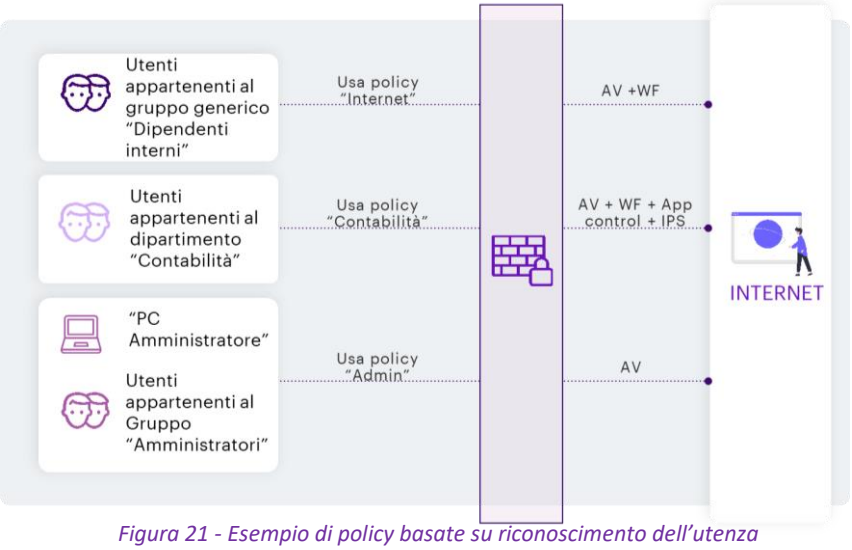


Figura 21 - Esempio di policy basate su riconoscimento dell'utenza

Le funzionalità di analisi sono assicurate centralmente mediante la piattaforma FortiAnalyzer che consente di creare ✓**Dashboard** per un monitoraggio degli eventi sia in tempo reale che storicizzati, ✓**Report** ad hoc a seconda delle esigenze. Di seguito si riportano alcuni esempi di Dashboard utili agli scopi descritti: stato degli eventi e delle minacce di sicurezza applicabili per PA, dettaglio delle regole implementate per la sicurezza di rete, elenco delle change applicate nel periodo di riferimento. Considerando il processo di Continuous Improvement, le dashboard e i report saranno personalizzabili e raffinabili, ove applicabile, secondo le esigenze delle singole PA.

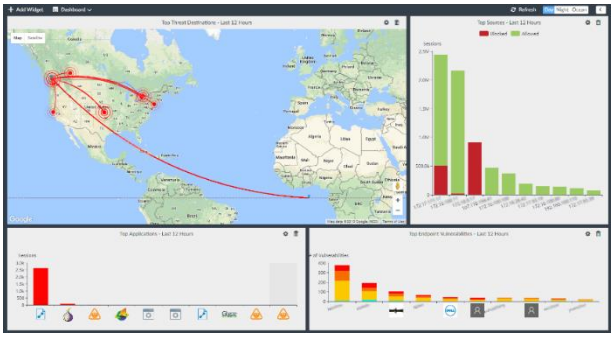
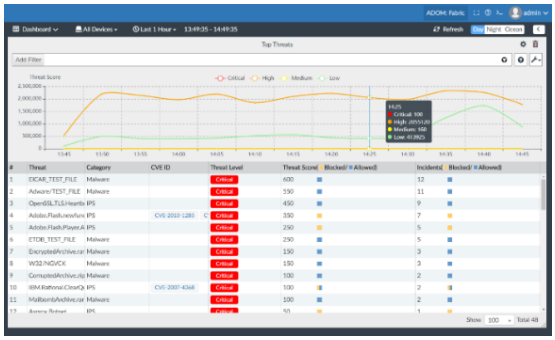
Security Monitor Dashboard	Top Threat Dashboard
	

Figura 22 - Esempi di Dashboard

7 PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL"

7.1 Soluzione Proposta

Il modello CDOM proposto (cfr. §§1 e 3.3) colloca il servizio di **Web Application Firewall** (WAF) nel dominio di sicurezza "Breach Prevention & Readiness" allineata alla Funzione NIST "Protect", riducendo così la superfice di attacco per le applicazioni web delle PA.

Il servizio **WAF** rappresenta uno dei principali asset di sicurezza del Centro Servizi, finalizzato alla protezione delle PA da attacchi veicolati ai dati delle applicazioni web, agendo da **filtro del traffico di rete** dello strato applicativo.

Le vulnerabilità delle Applicazioni Web possono portare a violazioni dei dati o al blocco di sistemi mission-critical per la PA, motivo per cui il servizio WAF proposto vuole superare i limiti dei normali Intrusion Detection System e dei tradizionali sistemi WAF che si affidano all'apprendimento delle applicazioni (manuale o automatico) per il rilevamento di anomalie e minacce. La nostra proposta adotta, invece, un approccio evoluto e completamente diverso al rilevamento delle minacce, grazie all'utilizzo un **motore di apprendimento automatico** (ML) che permette di costruire e aggiornare autonomamente un **modello di comportamento dell'utente** (Behavioral Analytics) ed utilizzare tale modello per discriminare il traffico lecito da quello malevolo, permettendo di bloccare in modo molto più efficace anche le minacce sconosciute (**exploit zero-day**). Questo nuovo approccio sfrutta, inoltre, **due livelli di apprendimento automatico**, uno basato sull'**AI** ed uno **sulle probabilità statistiche** per rilevare anomalie e minacce separatamente. Il primo livello costruisce il modello matematico per ogni parametro appreso e quindi attiva le anomalie per le richieste difformi. Il secondo verifica se l'anomalia è una minaccia reale o se si tratta di una varianza benigna (falso positivo).

Per assicurare che tutto il traffico venga correttamente protetto garantendo l'efficacia dei meccanismi di sicurezza attuati dal servizio WAF, sono previste **funzionalità di full SSL inspection (Deep Inspection)** al fine di garantire che anche il contenuto crittografato venga ispezionato dal presente servizio. Tramite le capacità di full SSL inspection è possibile proteggere le PA da tutte le tipologie di minacce, **anche se in traffico criptato** (es: https), prima di trasmettere il traffico al mittente.

Il corretto funzionamento del servizio WAF dipende, inoltre, da una coerente **interazione con tutti gli altri elementi dell'infrastruttura** e con un **modello operativo integrato**. Questo include la comprensione e la risposta agli errori e ai messaggi di allarme originati dal WAF, nonché da altri aspetti come la gestione delle modifiche alle politiche di sicurezza in concomitanza con le modifiche delle applicazioni WEB protette, garantendo così la corretta e piena disponibilità delle stesse. Si procede quindi ad integrare in modo agile il servizio WAF nel processo standard di gestione delle richieste di change per fare in modo che la distribuzione ed il test delle politiche di sicurezza avvenga prima negli ambienti non produttivi e solo successivamente in quelli di produzione. La distribuzione di specifiche firme o politiche direttamente in modalità di blocco può essere effettuata in caso di criticità o di attacco in corso, in accordo con le indicazioni di remediation ricevute dal servizio di monitoraggio di sicurezza SOC o dalle strutture di sicurezza delle PA finali. Questo assicura che l'**impatto è sempre valutato e ridotto al minimo**.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: Roma Capitale e Comune di Milano

Private: NEXI e Primario operatore finanziario

Descrizione di un caso di successo - **Roma Capitale** →**Esigenza** - Infrastruttura di sicurezza applicativa atta a proteggere il portale istituzionale di Roma Capitale →**Soluzione** – Fastweb ha realizzato un'architettura basta su FortiWeb →**Benefici** ✓facilità di migrazione di tutte le configurazioni e policy di sicurezza ✓servizi evoluti di sicurezza multi-minaccia in un'unica piattaforma di sicurezza che consente di contrastare efficacemente attacchi e minacce all'infrastruttura di rete.

7.1.1 Funzioni offerte

Il servizio prevede: un livello di **Interfaccia PA** utile all'interazione con il servizio, un livello di **Erogazione** in cui sono espletate le funzioni principali del servizio, un livello di **Automazione** (intelligent layer) che aggiunge funzioni avanzate, un livello **Interazioni** per le relazioni con gli altri servizi (cfr. §6.1.1). I livelli comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative**, descritte di seguito.

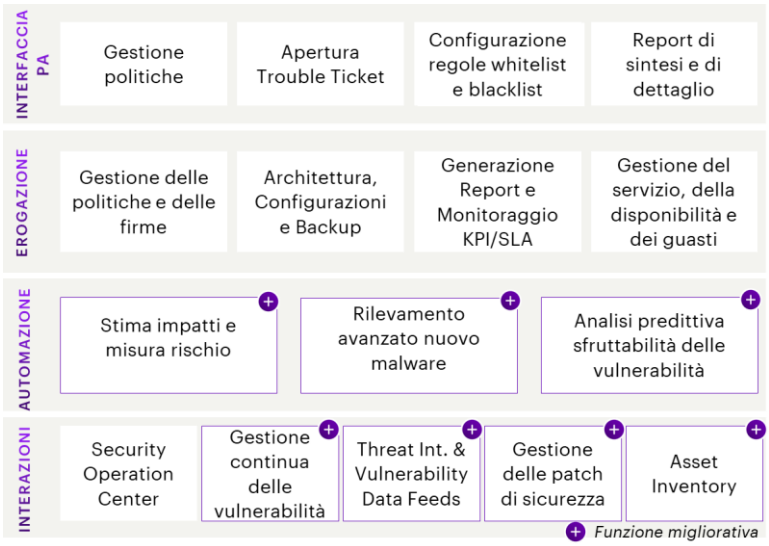


Figura 23 - Funzioni del servizio WAF

- **Stima degli impatti e misura del rischio**: la funzione esegue le stime di impatti e rischio sulle configurazioni implementate o che prevede di implementare, fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura. Tali valutazioni sono effettuate tenendo in considerazione: ✓la classificazione delle informazioni trattate, ✓la criticità del servizio abilitato per la PA, ✓le dipendenze ed interazioni con altri servizi, funzioni e sistemi.
- **Rilevamento avanzato del malware**: la funzione prevede metodi avanzati di "malware detection" fortemente potenziate dall'integrazione con il servizio di Threat Intelligence, nonché con il SOC e prevedono azioni automatizzate per isolare comportamenti di rete anomali che possono segnalare la presenza di malware noti o di possibili varianti; presenza di funzioni di "Protezione dagli attacchi DDOS - Distributed Denial of Service".
- **Analisi predittiva della sfruttabilità delle vulnerabilità**: la funzione combina dati e informazioni sulle minacce da più fonti analizzando con un algoritmo di apprendimento automatico basato su ML, per anticipare la probabilità che una vulnerabilità venga sfruttata, anche grazie all'interazione con i servizi di Gestione continua delle vulnerabilità e Threat Intelligence e Vulnerability Data Feeds.
- **Interazioni** con i servizi Threat Intelligence & Vulnerability Data Feed, Gestione continua vulnerabilità di sicurezza, Gestione delle patch di sicurezza, Asset Inventory, descritte al §7.4.1.

7.1.2 Architettura tecnologica

La soluzione tecnologica scelta dal Centro servizi prevede l'utilizzo della soluzione di WAF di Fortinet riconosciuta come leader sul mercato.

L'architettura prevista per la fornitura del servizio prevede l'integrazione del WAF, nella sua forma fisica o virtuale, localmente presso la singola PA oppure remotamente presso il Centro Servizi (scelta subordinata agli accordi con la singola PA), predisponendo una console di gestione integrata e centralizzata in esercizio presso lo stesso Centro Servizi. La scelta architetturale inerente all'installazione degli appliance presso la PA oppure remotamente presso il Centro Servizi sarà eseguita durante la fase di attivazione del servizio, subordinata alle caratteristiche dell'infrastruttura di rete della singola sede o alla lista di servizi di sicurezza WAF da attivare.

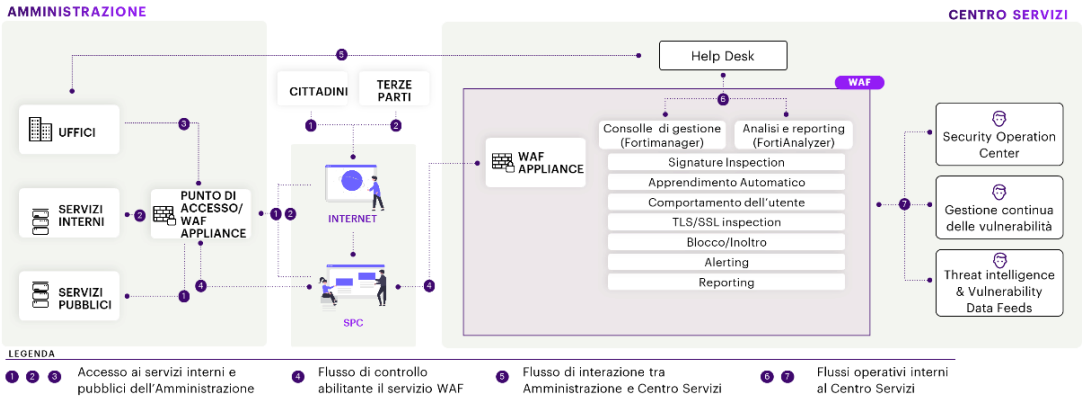


Figura 24 -Architettura tecnologica WAF

La gestione degli apparati WAF, analogamente a quanto già esposto per il servizio NGFW (cfr. §6), avviene mediante la console di gestione centrale **FortiManager** e l'ulteriore elemento centrale di analisi, logging e reporting, denominato **FortiAnalyzer**.

7.1.3 Caratteristiche tecnologiche e prestazionali migliorative

Gli apparati adottati dal servizio WAF saranno disponibili in versione chassis fisico o macchina virtuale (VM), al fine di garantire la massima flessibilità e adattabilità al contesto di rete, infrastrutturale e vincoli tecnologico/operativi. L'utilizzo di una forma piuttosto che di un'altra sarà concordata e selezionata dalla specifica PA.

La tecnologia Fortinet prescelta oltrepassa le capacità di protezione previste dal capitolato tecnico in quanto è in grado di fornire alle PA funzionalità evolute quali: ✓Approccio evoluto al **rilevamento delle minacce** che, oltre ai metodi "standard" basati su firma, sfrutta la probabilità per identificare le minacce piuttosto che eseguire corrispondenze precise con le attività osservate. ✓**ML**, che raccoglie dati su ciascun elemento dell'applicazione mentre gli utenti effettuano le normali interazioni con l'applicazione, utilizzando un modello statistico per determinare se una richiesta HTTP varia in modo significativo dalle richieste osservate in precedenza consentendo di definire delle azioni da applicare. ✓Un **ulteriore livello di apprendimento automatico** che, una volta identificata un'anomalia, determina se si tratta di una minaccia o semplicemente di una variazione benigna, come un errore di battitura, un nuovo carattere che non era stato visto in precedenza o anche un cambiamento legittimo all'applicazione stessa.

In questa proposta e in accordo con le best practice di settore, per ciascuna tipologia di applicazione e layer dello stack tecnologico sarà predefinito un set di regole di sicurezza da abilitare su ciascuna categoria di traffico. Tuttavia, sarà possibile richiedere ed evadere richieste di apertura e controllo del traffico su cui abilitare o meno determinati servizi, in accordo con gli standard della specifica PA. Inoltre, particolare importanza sarà fornita all' ottimizzazione dei processi operativi per il passaggio delle regole e delle policy tra i landscape di sviluppo e produzione per la modalità di apprendimento del traffico, tuning e blocco del traffico in modo da limitare la ricezione di alert per garantire che venga bloccato esclusivamente il traffico indesiderato (rimozione falsi positivi).

7.2 Organizzazione

7.2.1 Strutture coinvolte

Il servizio WAF è erogato da un team specializzato su servizi di sicurezza infrastrutturale ed applicativa che risponde a un **Responsabile del servizio**; il team è supportato da un **architetto** esperto su tecnologie WAF e da un **esperto** in ambito infrastrutturale.

Si propone, dunque, un servizio WAF gestito per competenze: la componente di «Platform Management» che si fa carico della gestione della parte System (versione & patch, utenze di sistema, capacity planning) e la componente di «Application Management» che si basa su un approccio application-oriented per ogni PA: supporto analisi applicative, politiche WAF, gestione delle firme, analisi dei falsi positivi e dei log.

Analogamente al servizio NGFW (cfr. §6.2.1) è previsto il supporto delle strutture CE SMART HUB e i Centri di Competenza/Partnership.

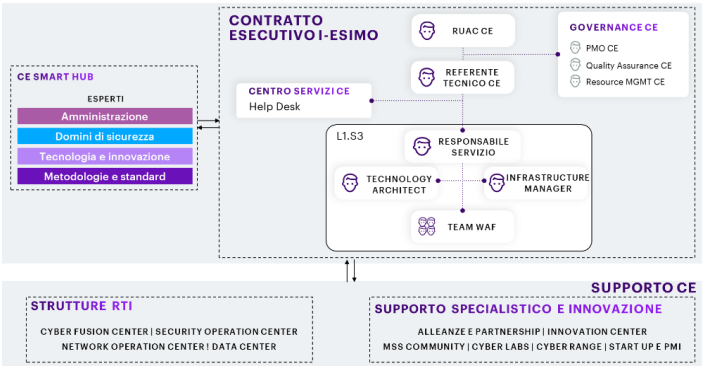


Figura 25- Strutture coinvolte nel servizio

7.2.2 Team del servizio

Di seguito sono dettagliati i ruoli organizzativi e i profili professionali che andranno a comporre il team di servizio WAF (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
Infrastructure Manager	Supporto al team WAF / Sr-ISC	Offre consulenza per le attività tecniche e di design riguardante la parte puramente infrastrutturale.
Technology Architect	Supporto al team WAF / SSA	Offre consulenza in ambito architetturale alla PA, ha una conoscenza approfondita del contesto e partecipa alla fase di analisi e di pianificazione delle attività.
WAF team	L2 Security Engineer / Sr-ISC	Supporta e integra le attività del L1 Security Engineer e definisce il design della soluzione supportato dal Supporto al team WAF e configura la soluzione.
WAF team	L1 Security Engineer / Jr-ISC	Registra il ticket e ne assegna la priorità, eseguendo l'analisi e la diagnosi iniziale. Esegue procedure per la risoluzione dei ticket o l'applicazione di workaround, attivando eventualmente procedure di escalation.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

7.3 Modello operativo

7.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

Figura 26 - Modello operativo servizio WAF

7.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di **Configurazione** ed **Erogazione** specifiche per il servizio in oggetto. Per le fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

CONFIGURAZIONE	
Installazione e setup	**Deliverable**: N/A **Descrizione**: All'interno di questo processo rientrano: ✓Consegna dell'apparato presso la PA (consegna fisica o OVA) ✓Setup iniziale HW (rack & stack) o vHW (deployment virtual appliance) ✓Setup configurazione (major and minor version, patches, interfaccia management) ✓Integrazione nella rete della PA ✓Integrazione con le piattaforme centralizzate
Configurazione e messa in produzione	**Deliverable**: N/A **Descrizione**: All'interno di questo processo rientrano: ✓Configurazione delle policy standard e dei profili d'ispezione ✓Configurazioni specifiche rispetto al CE, eventuale porting di configurazioni da appliance esistenti ✓Test della configurazione ✓Passaggio in produzione ed eventuale swap da sistemi pre-esistenti ✓Tuning delle funzionalità attivate ✓Supporto post passaggio in produzione

EROGAZIONE	
Gestione ciclo di vita policy	**Deliverable**: N/A **Descrizione**: ✓Creazione e modifica di policy di sicurezza ✓Estrazione informazioni quali esportazione di log, accessi, policy attive o procedure in essere
Operation	**Deliverable**: Report attività manutenzione **Descrizione**: Gestione di incidenti o problemi mediante: ✓l'applicazione di soluzioni permanenti utili a risolvere l'incidente ✓l'applicazione di workaround e analisi successiva della root cause per l'eliminazione definitiva di incidenti e problemi ✓Applicazione di aggiornamenti software, hotfix, operazioni di riavvio di specifici processi applicativi ✓Verifica funzionalità di base per alta affidabilità, backup e monitoraggio infrastrutturale

EROGAZIONE	
Reporting	Generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in formato Excel o PDF

7.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano di seguito gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO WEB APPLICATION FIREWALL				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSW	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta per il servizio WAF	*Data_Notifj* = Data Ora di inoltro al SOC della segnalazione *Data_Incj* = Data Ora dell'incidente TNSA = $\sum_{J=1}^{n} Data\_notifj - Data\_Incj$	Trimestre	<1 ora per il 90% degli incidenti
PCI_TNSW	Tempo di notifica al SOC di incidenti di gravità Altissima e Alta per il servizio WAF	Come IQA_TNSW	Mensile	<1 ora per il 95% degli incidenti
KPI_NABB	Numero di accessi da IP in blacklist bloccati	Numero di attacchi bloccati (include sia accessi da IP in blacklist che mancato rispetto di regole logiche)	Trimestre	Incremento < 50% rispetto alla rilevazione precedente

7.4 Interazioni

7.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione / Finalità
SOC	Eventi analizzati dal WAF	Output	Integrazione funzionale e tecnica delle piattaforme WAF e SIEM volta a consentire l'invio dei log al SIEM affinché gli alert di sicurezza generati dai WAF possano essere analizzati e correlati in real-time con gli eventi degli altri sistemi delle singole PA al fine di rilevare situazioni di rilievo ai fine della cybersecurity e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza.
Threat Int. & Vulnerability Data Feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence potranno essere raccolti in input dai WAF Fortinet al fine di limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash) in modalità preventiva e non solamente reattiva a seguito di un attacco.
Gestione cont. vulnerabilità di sicurezza	Vulnerabilità in essere e potenziali	Input/ Output	Gli apparati scambiano con il servizio informazioni relative alle vulnerabilità identificate sui sistemi e relative configurazioni e ricevono informazioni in merito alla relativa criticità e prioritizzazione
Gestione delle patch di sicurezza	Da Patch Management a WAF	Input	Per quelle applicazioni, laddove non è presente una patch ad una specifica vulnerabilità di sicurezza, si potrà effettuare l'enforcement tramite il servizio WAF per mitigare il rischio di impatto della vulnerabilità (virtual patching).
Asset Inventory	Da CMDB a WAF	Input	Ove presente una soluzione di Asset Inventory presso le PA, l'integrazione abilita la gestione centralizzata dell'asset, la compliance e i processi di patch management. L'integrazione sarà sia funzionale che tecnica delle piattaforme, volta a consentire l'acquisizione delle informazioni.

7.4.2 Reporting per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui WAF solo qualora fossero previsti possibili impatti di servizio e analisi della protezione applicata alle applicazioni. Esempi di report disponibili: PCI Reports, Attack Activity, Traffic Activity e Event activity.

7.5 Protezione da exploit zero-day, infezioni da malware e vulnerabilità

In aggiunta agli aspetti sopra indicati, il servizio WAF introduce anche le seguenti funzionalità, fondamentali per la protezione da exploit zero-day: ML, Rilevamento bot e Sandbox.

7.5.1 Machine learning

Il servizio WAF, tramite la tecnologia individuata, offre una funzione di apprendimento automatico che consente di rilevare il **traffico Web dannoso e i bot** (FortiWeb). Oltre a rilevare attacchi noti, la funzione è in grado di rilevare potenziali attacchi zero-day sconosciuti per fornire protezione in tempo reale per i server Web. Il modello di rilevamento delle anomalie della funzionalità di apprendimento automatico osserva gli URL, i parametri e il metodo HTTP delle sessioni HTTP e/o HTTPS che passano ai server web e costruisce modelli matematici per rilevare il traffico anomalo. FortiWeb utilizza due livelli di apprendimento automatico per rilevare attacchi dannosi. Il primo livello utilizza l'Hidden Markov Model (HMM) e monitora l'accesso all'applicazione e raccoglie dati per costruire un modello matematico dietro ogni parametro e metodo HTTP. Una volta completata, verifica ogni richiesta rispetto al modello per determinare se si tratta di un'anomalia o meno. Una volta che il primo livello di apprendimento automatico rileva una richiesta come anomala, viene attivato il secondo livello di apprendimento automatico per verificare se si tratta di un attacco reale o solo di un'anomalia benigna che dovrebbe essere ignorata. Per fare ciò, FortiWeb include modelli di minacce

addestrati (reti neurali) predefiniti. Ciascuno rappresenta una determinata categoria di attacco, come SQL Injection, Cross-site Scripting e così via. Ogni modello di minaccia è già addestrato sulla base dell'analisi di migliaia di campioni di attacco. I modelli di minaccia vengono continuamente aggiornati utilizzando il servizio di sicurezza FortiWeb. Quando vengono rilasciati nuovi tipi di attacco, il team FortiGuard analizza le nuove minacce e riqualifica il modello di minaccia pertinente. Il nuovo modello di minaccia viene quindi inviato a tutte le installazioni dei clienti in modo simile a come vengono aggiornate le firme.

7.5.2 Rilevamento bot

Il modello di rilevamento dei bot di apprendimento automatico basato sull'AI integra le regole esistenti basate su firme e soglie. Rileva bot sofisticati che a volte possono passare inosservati. Il modello di rilevamento dei bot osserva i comportamenti degli utenti da tredici dimensioni, ad es. quante volte le richieste HTTP vengono avviate dall'utente, se la richiesta utilizza versioni HTTP illegali, se recupera risorse JSON/XML.

Rispetto ai meccanismi tradizionali per rilevare i bot, il modello di rilevamento dei bot semplifica il tuning della soglia appropriata per rilevare comportamenti anomali degli utenti. In particolare, per sapere quante volte le richieste HTTP avviate da un utente devono essere considerate anomale, con il meccanismo tradizionale, potrebbe essere necessario sperimentare diversi valori di soglia e controllare continuamente il registro degli attacchi fino a quando non vengono riportati registri degli attacchi correlati per il traffico normale. Pertanto, FortiWeb utilizza un algoritmo basato SVM (Support Vector Machine) per creare il modello di rilevamento dei bot che autoapprende i profili di traffico dei client regolari. Quando arriva il traffico di un nuovo client, viene confrontato con quello dei client normali. Se non corrispondono, il modello consente di classificare il nuovo client come un'anomalia. Quando i profili di traffico dei client regolari variano notevolmente, FortiWeb aggiorna automaticamente il modello per adattarsi ai cambiamenti.

7.5.3 Sandbox

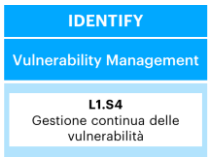
Il servizio FortiSandbox è una soluzione software sandbox che consente un accesso completo alla configurazione della stessa e invii illimitati per l'ispezione di oggetti sospetti o classificati come tali. Lla soluzione presenta i seguenti benefici: ✓**Riduzione dei rischi**. Con una sandbox dedicata basata sull'AI, si hanno a disposizione risultati in pochi minuti e non in ore, il che è fondamentale per ridurre il successo degli attacchi nell'odierno panorama delle minacce in continua evoluzione. ✓**Scalabilità**. Ridimensionamento della capacità di sandbox attraverso l'aggiunta di VM. ✓**Maggiore efficienza**. Integrazione del sandboxing nell'infrastruttura di sicurezza per automatizzare la protezione dalle violazioni senza la necessità di un team di sicurezza IT dedicato per monitorare costantemente le minacce.

8 PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL" – FUNZIONALITÀ AGGIUNTIVE

Con riferimento al servizio di "web application firewall" (di cui al par. 3.1.3 del Capitolato Tecnico speciale), il Raggruppamento conferma la presenza di funzioni di "Protezione dagli attacchi DDOS - Distributed Denial of Service".

9 PROPOSTA PROGETTUALE PER IL SERVIZIO "GESTIONE CONTINUA DELLE VULNERABILITÀ DI SICUREZZA"

9.1 Soluzione proposta



Il **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di Gestione continua delle vulnerabilità di sicurezza nel dominio di sicurezza "Vulnerability Management", riconducibile alla Funzione NIST "Identify". Il servizio in oggetto ha lo scopo di rilevare, monitorare e ridurre la superfice d'attacco esposta dalle PA contraenti. La nostra esperienza su vasta scala ci ha consentito di consolidare ed evolvere un **modello di servizio proprietario** che arricchisce ed estende la gestione dell'intero ciclo di vita delle vulnerabilità attraverso l'adozione di una **piattaforma TVMP (Threat and Vulnerability Management Platform)**, dispiegata c/o il Centro Servizi e integrata con altri sistemi di controllo (SIEM/SOAR, Threat Intelligence, NGFW/WAF, Asset Inventory/CMDB ove presenti), alla quale accede esclusivamente personale altamente qualificato e certificato (SANS, GEVA/GXPN, OSCP, OSCE, CEH, OPST, etc.). La proposta per il servizio si connota per le seguenti **caratteristiche distintive**: ✓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, MITRE kill-chain, etc.) capaci di sfruttarle; la fase di ricerca delle vulnerabilità agevola peraltro la ricostruzione (ove non presente) di un 'Asset Inventory' (con CCE e CPE) del patrimonio informativo delle PA 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** della PA 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; ✓**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,** come nel seguito descritti; ✓Reportistica relativa alle scansioni con un alto grado di personalizzazione di elementi quali: superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: circa 40 tra cui Azienda ULSS4 VENETO, IPZS, ENAC, MIUR, Agenzia delle Entrate, Università studi di Cagliari, Comune di Lecce

Private: Intesa Sanpaolo, ENEL, ENI, Poste Italiane, NEXI, Primario operatore finanziario

Descrizione di un caso di successo - **Azienda ULSS4 VENETO** →**Esigenza** - Indirizzare un ampio numero di misure minime di sicurezza AgID →**Soluzione** -Fastweb ha erogato un servizio avanzato di Asset Discovery & Profiling, Vulnerability Management costruito ad hoc, basato sulla piattaforma Qualys →**Benefici** ✓indirizzamento dei primi 4 AgID Basic Security Controls (ABSC) in contesti con decine di migliaia di host ✓verifica che tutte le conformità, una volta raggiunte, vengano nel tempo mantenute, evidenziando eventuali non conformità ✓processo di "Automated Asset Discovery" che, scansionando costantemente lo spazio di indirizzamento IP, consente di automatizzare il processo di inventario.

9.1.1 Funzioni offerte

Il servizio prevede i 4 livelli, già presentati al §6.1.1, che comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative** utili anche a supportare le Amministrazioni nelle fasi di progressiva riduzione della superficie d'attacco. Le migliorative sono di seguito descritte.

Figura 27 - Funzioni del servizio Gestione cont. vulnerabilità di sicurezza

- **Gestione dei piani e configurazione scansioni**: raccolta ed utilizzo delle informazioni secondo profili di utenza diversi, tramite un'interfaccia grafica e/o API.
- **Conduzione del servizio**: è previsto **supporto tecnico-organizzativo** volto al controllo dello stato d'avanzamento dei piani di rientro (include esecuzione controlli tecnici di '**re-check**' sulla persistenza delle vulnerabilità riscontrate) e **supporto tecnico-funzionale** per la risoluzione o mitigazione delle problematiche di sicurezza individuate (es. hardening, bug fixing, upgrading, fine tuning, replatforming).
- **Rendicontazione direzionale e rapporti tecnici***:* La funzione espone interfacce per consultazione, archiviazione, ricerca e download dei rapporti redatti al termine di ciascuna scansione (on-demand, pianificata, campagna, **re-check**, etc.). È prevista la stesura di un rapporto tecnico con le evidenze oggettive sulle vulnerabilità riscontrate e di una rendicontazione direzionale. La classificazione delle vulnerabilità si avvale di un modello di rischio basato sullo **standard CVSS**, che, tenendo conto di diversi fattori (es. vettore di attacco, complessità dell'attacco, livello dei privilegi richiesti, criticità dell'asset vulnerabile), assegna un punteggio ed un conseguente livello di rischio su 4 livelli (Low, Medium, High, Critical). Il TVM team (cfr. §9.2) su richiesta della PA può monetizzare il rischio residuo attraverso un'analisi quantitativa che si avvale degli output prodotti della funzione '**Stima degli impatti e misura del rischio'.** Nei rapporti sono altresì indicate le **azioni di rientro** volte alla risoluzione o mitigazione delle problematiche riscontrate con una **stima quantitativa degli interventi.**
- **Analisi e correlazione di vulnerabilità**: La funzione consente di ricostruire un contesto nel quale le vulnerabilità sono analizzate sia puntualmente che nel complesso al fine di identificare le potenziali **kill-chain** cui la PA potrebbe essere soggetta.
- **Classificazione dinamica degli asset**: La funzione consente di aggregare gli asset sulla base di una o più caratteristiche (es. sistema operativo, porte esposte e servizi). Le viste generate da questa classificazione consentono di ridurre notevolmente il tempo di gestione delle vulnerabilità in quanto abilitano campagne di patching, bug fixing, hardening, upgrading, fine tuning, replatforming mirate ed efficaci.
- **Stima degli impatti e misura del rischio***:* La funzione esegue le stime di impatto e rischio, informazioni oggetto poi di visualizzazione in tempo reale e/o tramite report periodici grazie ai canali di Interfaccia. Gli asset vulnerabili sono analizzati considerando: ✓la classificazione delle informazioni che trattano ✓la criticità del servizio che abilitano per la PA ✓le dipendenze/interazioni con altri servizi, funzioni e sistemi.
- **Rilevamento avanzato del malware**: La funzione prevede metodi avanzati di 'malware detection' che aumentano l'efficacia dei risultati delle scansioni individuando una serie di evidenze, correlate o correlabili, tali da rappresentare contesti nei quali potrebbero essere potenzialmente presenti tipologie note di malware, di potenziali varianti o di nuovo malware.
- **Analisi predittiva della sfruttabilità delle vulnerabilità**: La funzione combina dati e informazioni sulle minacce da più fonti analizzando con un algoritmo di apprendimento automatico basato su ML, per anticipare la probabilità che una vulnerabilità venga sfruttata.
- **Interazioni** con i servizi Security Operation Center, CMDB/Asset Inventory, Next Generation Firewall e Web Application Firewall, descritte al §9.4.1.

Cruscotti e viste personalizzabili

CRUSCOTTI DINAMICI - La funzione "Cruscotti dinamici personalizzabili" espone **cruscotti dinamici** sullo stato della sicurezza, personalizzabili in base alle esigenze della singola PA e accessibili da una console centralizzata della TVMP. Tali **cruscotti** sono sistematicamente aggiornati **(Real-Time dashboard)** al fine di **monitorare la superficie d'attacco in tempo reale**. Nell'ambito delle personalizzazioni già previste in base all'esperienza del RTI, sono disponibili **template e baseline di riferimento** che possono essere **arricchiti** con ✓indicatori ad hoc e aggregazioni/scomposizioni (es. geografiche e settoriali) ✓rappresentazioni grafiche per il **monitoraggio del patrimonio informativo nelle sue diverse categorizzazioni** (dispositivi, reti, infrastrutture, sistemi, dati, identità, ecc.), differenziate per livelli di utenza. Il cruscotto dinamico, in particolare, offre **di default** la possibilità di: ✓visualizzare graficamente i risultati delle singole scansioni ✓aggregarli per ottenere informazioni statistiche sulle vulnerabilità più frequenti e individuare quelle più rischiose ✓analizzare lo storico per valutare lo stato delle singole vulnerabilità nel tempo sullo specifico sistema informativo ✓disporre di una vista generale sul livello di esposizione delle PA, interagire direttamente con altri servizi (es. SOC per trouble ticketing, patch management, etc.) ✓classificare gli asset per tipologia (es. sistema operativo, database, app) ✓prioritizzare le vulnerabilità includendo 'feed' di threat intelligence, etc.

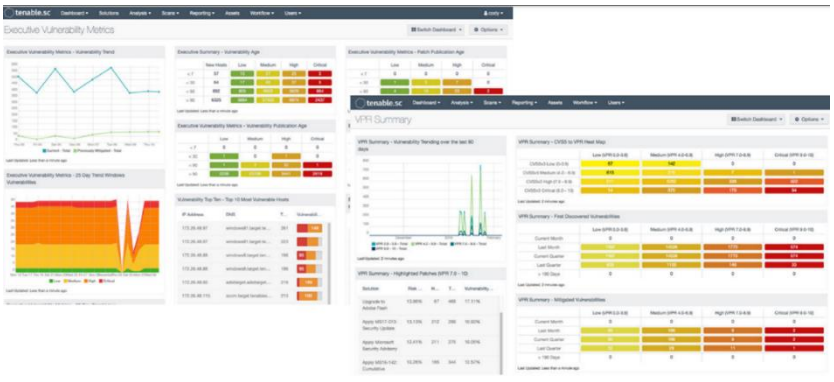


Figura 28 – Esempio Cruscotti dinamici

CRUSCOTTO DI 'ENTERPRISE RISK MONITORING' - AGGIUNTIVO - Si prevede, inoltre, l'apporto del TVM team (cfr. §9.2) per la realizzazione e l'aggiornamento di un **cruscotto aggiuntivo di 'Enterprise Risk Monitoring'** per la singola PA, nel quale la misura del rischio (che può stimarsi sia qualitativamente che quantitativamente) non sia limitata agli asset IT vulnerabili ma **afferisca ai processi e ai servizi** della PA abilitati da tali asset. Questa rappresentazione, mantenuta costantemente aggiornata, diviene fondamentale per supportare adeguatamente il percorso decisionale, nelle diverse PA, sia della dirigenza sia del personale tecnico

preposto alla sicurezza, dal momento che: ✓**favorisce** la corretta interpretazione dei rischi (monetizzati e non livellati) ✓**agevola** una miglior comprensione della superficie d'attacco esposta (processi/servizi e non asset IT) ✓**guida** l'assegnazione della priorità ai piani di rientro (suggerendo e stimando gli interventi necessari). Il TVM si renderà disponibile a personalizzare le viste per le singole PA contraenti.

Per **entrambi i cruscotti**, l'accesso sarà profilato e basato su ruoli/gruppi con diversi livelli e coni di visibilità. Le viste e le infografiche presenti nei cruscotti saranno esportabili su file, coerentemente ai profili d'accesso attivati presso le diverse PA. Le **esigenze di personalizzazione** saranno formalizzate in **requisiti, specifiche e mock-up** presentati alla PA e, una volta approvati, rilasciati in ambiente di produzione a integrazione delle viste sopra descritte.

Figura 29 – Esempio cruscotto di 'Enterprise Risk Monitoring'

CONTEXTUAL KNOWELDGE BASE - AGGIUNTIVA - Il TVM provvederà inoltre a rendere disponibile e aggiornare sistematicamente una **Contextual knowledge base** (CKB) con le casistiche e le migliori pratiche applicate per le diverse classi di vulnerabilità riscontrate e risolte sulle singole PA: in un'ottica di 'information sharing', ciascuna PA avrà la possibilità di pubblicare sul Portale di Fornitura, in toto o in parte, la propria CKB e renderla pertanto visibile alle altre PA, con le quali attivare anche confronti in modalità social (cfr. §16.2).

9.1.2 Architettura tecnologica

L'architettura della piattaforma TVMP riportata in figura 30 (integrata con tecnologia Tenable) che abilita il servizio è composta dalle seguenti componenti principali: ✓Una sonda fisica o virtuale**,** da installare nell'infrastruttura della PA contraente 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 necessaria la sonda sarà connessa alla rete della PA e sarà abilitata a comunicare 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 delle singole Amministrazioni; 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**.

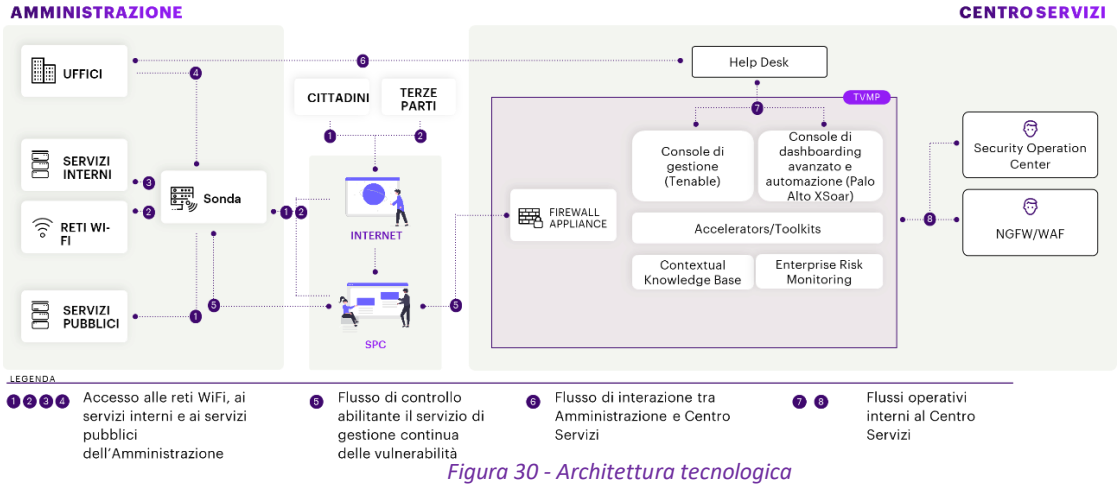


Figura 30 - Architettura tecnologica

9.2 Organizzazione

Nel contesto della struttura-tipo presentata al §6.2.1, il servizio è erogato da un unico gruppo di lavoro denominato **Threat and Vulnerability Management (TVM) Team**, che risponde a un **Responsabile del servizio**, il quale rappresenta il punto di contatto tra il TVM Team e l'Amministrazione ed è supportato da uno **SME** (Subject Matter Expert), esperto nell'ambito della Cyber Security. Il TVM Team viene di seguito descritto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
Automazione e integrazione	Resp. attività di integrazione / SSA	Gestisce le integrazioni del Centro Servizi in base alle esigenze delle singole PA, coordina le attività tra i team per l'aggiornamento e il miglioramento continuo con l'obiettivo di aumentare il livello di automazione del servizio
Gestione delle vulnerabilità	Resp. attività di gestione continua delle vulnerabilità di sicurezza / Sr-ISC	Configura gli strumenti software, gestisce le politiche di scansione e predispone le dashboard/cruscotti dinamici per le PA. Supervisiona le attività del team "Verifiche di sicurezza". Fornisce il supporto tecnico-funzionale per la risoluzione o mitigazione delle problematiche di sicurezza individuate (hardening, bug fixing, upgrading, fine tuning, replatforming, etc.)
Verifiche di sicurezza	Resp. attività di verifica di sicurezza / Jr-ISC	Esegue le attività di scansione, analizza i risultati e predispone i report executive e tecnici per ciascuna attività commissionata dalle Amministrazioni.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

Sempre in analogia con il §6.2.1, il Team del servizio è supportato ✓dal **CE Smart Hub** (es. per identificare in dettaglio le tecnologie critiche in uso presso la PA allo scopo di meglio contestualizzare i feed di Vulnerability) ✓dai **Centri di competenza** della rete di CyberFusion Center altamente specializzati nella ricerca e mitigazione di vulnerabilità ad alta complessità.

9.3 Modello operativo

9.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

Figura 31 - Modello operativo

9.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di **Configurazione** ed **Erogazione** specifiche per il servizio in oggetto. Per la descrizione delle fasi di **Attivazione** e **Chiusura** vale quanto decritto al §6.3.2.

CONFIGURAZIONE	
Deliverable: Pianificazione delle attività e personalizzazione del cruscotto dinamico (Real time Dashboard) / Specifiche di configurazione	
Predisposizione Configurazione	Descrizione: ✓definizione configurazione della sonda ✓Personalizzazione del cruscotto per raccogliere e monitorare i risultati ✓Definizione delle politiche di scansione ✓Selezione del perimetro di intervento ✓Pianificazione dell'attività
Procedura di Configurazione	L'installazione e configurazione della sonda sarà definita durante la presa in carico del servizio e prevede: ✓Un meeting di kick-off ✓L'installazione della sonda, che avverrà di concerto con i tecnici della PA nel caso in cui la sonda debba essere allocata presso un data center della PA ✓La configurazione della sonda sarà effettuata dal RTI
	Personalizzazione del cruscotto: ✓Definizione dell'entità sulla console centralizzata per la gestione della PA ✓Predisposizione delle viste in base alle esigenze della PA ✓Integrazione con il SOC che effettua il monitoraggio continuo delle vulnerabilità
Pianificazione	Pianificazione delle attività che include la redazione del Piano di Scansione

EROGAZIONE	
Deliverable: Report scansioni	
Verifica di sicurezza	Descrizione: L'erogazione rappresenta l'attività operativa durante la quale il servizio verificherà, attraverso le attività di scansione, la presenza di vulnerabilità per gli IP inclusi nel perimetro concordato con la PA. Le evidenze ottenute saranno rendicontate in appositi rapporti (tecnici e direzionali) e pubblicate sul Cruscotto dedicato alla PA contraente per consultazioni in tempo reale.
Esecuzione attività di verifica	Definizione campagna di scansione prevede: ✓Impostazione e configurazione delle policy di scansione sulla console centralizzata ✓Identificazione di reti / sistemi informativi in perimetro ✓Dry-Run tramite una scansione on-demand di prova su un sottoinsieme di sistemi informativi concordati ✓Pianificazione delle campagne di assessment sulla console centralizzata.
	Analisi risultati include: ✓Analisi delle evidenze ed approfondimenti del personale qualificato ✓Eliminazione dei falsi positivi.
	Il reporting include: ✓Executive report ✓Custom report, con associato supporto per eventuali richieste di chiarimento o approfondimento sui risultati della verifica effettuata e per le azioni di rientro volte al trattamento delle vulnerabilità riscontrate.
Integrazione e Cruscotti	Aggiornamento dashboard e integrazione: ✓Aggiornamento della dashboard (cruscotti dinamici) sulla console centralizzata ✓Integrazione con i sistemi del SOC per il monitoraggio continuo delle vulnerabilità.

9.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto:

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO GESTIONE CONTINUA DELLE VULNERABILITÀ DI SICUREZZA				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_PSV	Puntualità nella erogazione delle scansioni di vulnerabilità	Numero scansioni erogate nei tempi previsti / Numero scansioni pianificate da effettuare	Trimestre	85%
PCI_RICD	Num. giorni lavorativi di ritardo nella consegna di documentazione	Come RICD ma con frequenza maggiore e soglia più sfidante	Mensile	RICD = 0
KPI_NVGC	Numero di vulnerabilità rilevate	Numero di vulnerabilità rilevate dal servizio	Trimestre	Incremento<10% risp. rilev. precedente

9.4 Interazioni

9.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
SOC	Vulnerabilità	Output	L'integrazione tra la console di Tenable e il sistema SOAR Palo Alto Cortex XSoar consente a quest'ultimo di importare le vulnerabilità e arricchire Dashboard personalizzate per la gestione e il monitoraggio continuo delle vulnerabilità
Next Gen. e Web Application Firewall	Regole Firewall	Output	Configurazione delle regole firewall necessarie per la raggiungibilità del perimetro da sottoporre a scansione
CMDB/Asset Inventory	Asset	Input	Ove presente una soluzione di Asset Inventory presso le PA, input dei sistemi oggetto di scansione per la valutazione di riservatezza, integrità e disponibilità dei dati trattati dall'asset e la rilevanza del servizio della PA che abilitano

9.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive report da	A ogni	L'Executive report include come **elemento migliorativo** una vista di sintesi dell'esposizione alle minacce, delle analisi

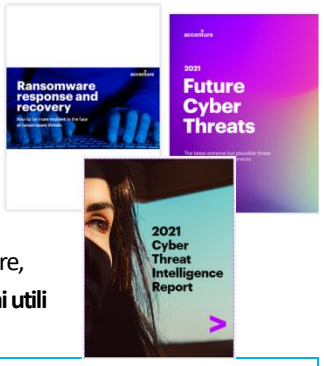
Capitolato	scansione	dei potenziali impatti e del livello di rischio sui processi dell'Amministrazione
Custom report da Capitolato	A ogni scansione	Il Custom report include come **elementi migliorativi**: ✓l'approfondimento tecnico sulle vulnerabilità individuate con ricostruzione delle potenziali kill-chain correlabili ✓le azioni tecnico-organizzative ed il piano di rientro da intraprendere per gestire le vulnerabilità con stima dell'impegno e competenze necessarie
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui NGFW solo qualora fossero previsti possibili impatti di servizio

10 PROPOSTA PROGETTUALE PER IL SERVIZIO "THREAT INTELLIGENCE & VULNERABILITY DATA FEED"

10.1 Soluzione Proposta

Il **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di Threat Intelligence & Vulnerability Data Feed (**TI&VDF**) nel dominio di sicurezza "Threat intelligence" (TI) riconducibile alla **Funzione NIST "Identify"**. Il servizio in oggetto è erogato dal Centro Servizi avvalendosi della piattaforma **piattaforma Threat Intelligence Service (TIS)**, sviluppata e gestita da Accenture che, a sua volta integra il servizio specialistico **iDefense** di Accenture che prevede l'accesso tramite interfaccia Intelgraph 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. Il servizio è reso disponibile tramite **una interfaccia web e accesso API** e si integra con il servizio di SOC di cui costituisce sia un provider informativo utile alla conduzione di indagini di sicurezza. La piattaforma fornisce informative complete e continuative (feed) relative alle minacce e vulnerabilità di sicurezza, specificamente adattate alle PA, grazie alla possibilità di utilizzare un'**ampia quantità di fonti informative OSINT** (Open Source Intelligence ad accesso libero) e **CLOSINT** (Closed Source Intelligence non liberamente disponibili). Il servizio è erogato da **oltre 10 anni** ad una molteplicità di Clienti operanti a **livello nazionale e internazionale** sui principali mercati di riferimento. **Fattore distintivo** del servizio è la possibilità di far leva su competenze e centri di ricerca di Accenture riconosciuti **a livello internazionale** che abilitano l'accesso a fonti informative necessarie per interpretare i fenomeni di sicurezza anche per il mercato italiano, spesso legati a minacce di sicurezza generate da gruppi che operano in paesi terzi. I centri di ricerca di Accenture, in tal senso, sono **riconosciuti a livello internazionale** e, con cadenza periodica, rilasciano **report di interpretazione dei fenomeni utili alla Security Community dei Clienti (Sitrep),** alcuni esempi in figura.

Figura 32 - Interfaccia web iDefense - Intelgraph



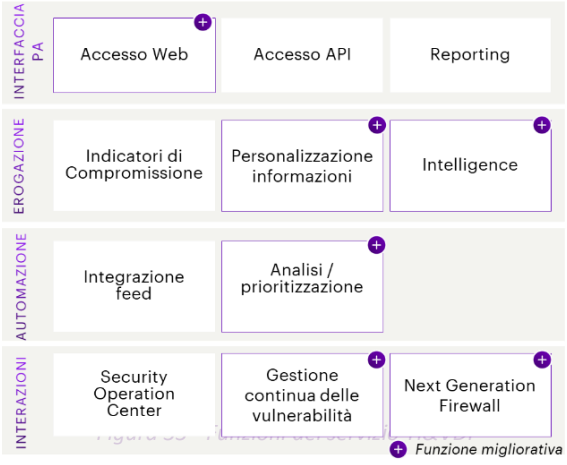
Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Private: Primario operatore delle Telecomunicazioni, Unicredit, ENI, CARIGE

Descrizione di un caso di successo - Primario operatore delle Telecomunicazioni →Esigenza - Supporto per la gestione proattiva delle minacce e delle vulnerabilità di sicurezza al fine di fornire informazioni più approfondite e aggiornate in tempo reale al servizio SOC e migliorare così le attività di threat hunting e il blocco preventivo degli IoC →**Soluzione** - attivazione per la raccolta di feed di Threat Intelligence e Vulnerability per fornire al Cliente le informazioni più aggiornate su campagne di attacco che interessano il settore e l'area geografica di riferimento, vulnerabilità che impattano le tecnologie in uso, IoC per i sistemi di Intrusion Prevention e Intrusion Detection →**Benefici** - Maggiore visibilità sui diversi tipi di minacce che potrebbero impattare il brand, prima ancora che gli eventi di abuso si verifichino, grazie ad una migliorata proattività nel contrasto a tali minacce.

10.1.1 Funzioni offerte

Il servizio **TI&VDF** consente di elaborare ed estrarre le informazioni necessarie attraverso le funzionalità offerte, articolate nei livelli riportati in figura (cfr. §6.1.1). Tali livelli comprendono tutte le funzionalità richieste dal Capitolato e ne aggiungono alcune **migliorative**, di seguito descritte.



- **Accesso web:** la piattaforma integra l'interfaccia Intelgraph 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 PA in funzione dei sistemi adottati. Tramite l'interfaccia è possibile consultare i bollettini predisposti dal team di Threat Intelligence (**TI**) e generare report personalizzati;
- **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 PA;
- **Analisi / Prioritizzazione:** la piattaforma dispone di funzionalità atte a filtrare le informazioni in funzione delle necessità della PA secondo meccanismi dinamici e continuativi che consentono di focalizzare l'attenzione sui fenomeni più rilevanti;
- **Interazioni** con i servizi Gestione Continua delle vulnerabilità e Next Generation Firewall, descritte al §10.4.1.

10.1.2 Feed di Threat Intelligence

I feed utilizzati per l'erogazione del servizio TI&VDF provengono ✓direttamente dai vendor dei prodotti, ✓da programmi di Bug Bounty e ✓da analisi effettuate da ricercatori di sicurezza ✓dal newtork Accenture costituito da tutti centri di competenza a livello Globale progressivamente acquisiti negli anni. 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 **71 feed** utilizzati raggruppati per **Tipologia** provenienti anche dai Centri di Competenza delle società acquisite quali **Symantec e Context-IS**.

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.

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 iDefense, i database di exploit per lo sfruttamento delle vulnerabilità disponibili in rete e i risultati del programma di Bug Bounty di iDefense
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.

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.

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.

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.

10.1.3 Architettura tecnologica

Tra gli elementi di **valore** della piattaforma Threat Intelligence Service (TIS) si evidenzia l'integrazione con il servizio SOC cui fornisce informazioni in merito alle minacce di sicurezza reali e potenziali, nonché Indicatori di Compromissione (IoC) che alimentano la piattaforma SIEM.

L'architettura del servizio prevede la possibilità per le PA di accedere alla piattaforma TIS tramite **un'interfaccia web** o tramite **API protette**. Il servizio può inoltre essere ingaggiato tramite il servizio di Help Desk che, a sua volta, accede alle interfacce della piattaforma TIS.

La piattaforma raccoglie i feed informativi e procede alla loro **elaborazione in modo automatizzato**. I data feed uniformati tramite la transcodifica nel formato STIX 2.1, un linguaggio strutturato specificamente utilizzato per lo scambio di informazioni di Cyber Threat Intelligence correlati al fine di ottenere informazioni di Intelligence il più possibile approfondite e complete.

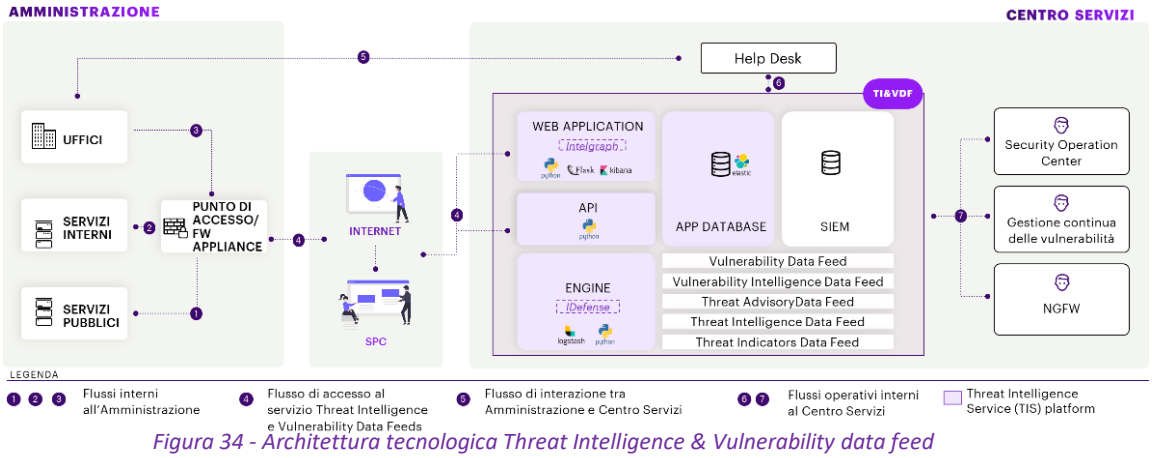


Figura 34 - Architettura tecnologica Threat Intelligence & Vulnerability data feed

La piattaforma si basa su **tecnologie open source** quali: ✓**Stack Elastilk (ELK)** che include (i) Elasticsearch, un search engine utilizzato per la ricerca e l'analisi dei dati, (ii) Logstash, una data processing pipeline che colleziona simultaneamente dati provenienti da molteplici fonti, li trasforma e li invia ad uno "stash" come Elasticsearch, (iii) Kibana, un software di data visualization che consente di visualizzare i dati in Elasticsearch mediante grafici e tabelle; ✓**Python**, un linguaggio di programmazione adattabile e largamente utilizzato per numerosi progetti anche in ambito cyber security; ✓**Flask**, un micro web framework scritto in Python utilizzato per la costruzione di applicazioni web.

10.2 Organizzazione

Nel contesto della struttura-tipo presentata al §6.2.1, il servizio è erogato da un unico gruppo di lavoro – TI Team, che risponde a un Responsabile del servizio, il quale rappresenta il punto di contatto tra il Team e la PA ed è supportato da uno SME (Subject Matter Expert). Il Team sarà così composto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
SME TI	Supporto al team TI / SSA	Offre consulenza per l'interpretazione di specifiche minacce identificate dal servizio di threat intelligence. Analizza le nuove minacce e fornisce indicazioni per l'arricchimento continuo dei vulnerability feed
TI team	L2 Security Engineer / Sr-ISC	Gestisce casi / incidenti che richiedono competenze avanzate. Supporta le attività evolutive della piattaforma TIS tramite l'individuazione delle fonti utilizzabili per la collezione dei feed di Intelligence e Vulnerability e la definizione delle strategie di raccolta dei dati
TI team	L1 Security Engineer / Jr-ISC	Si occupa di implementare sistemi di raccolta e condivisione dei feed provenienti dalle fonti OSINT e CLOSINT individuate, di eseguire la transcodifica dei dati per uniformarne i formati e di procedere alla configurazione e alla manutenzione complessiva della piattaforma TI
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

Sempre in analogia con il §6.2.1, il Team del servizio è supportato ✓dal CE Smart Hub (es. per identificare in dettaglio le tecnologie critiche in uso presso la PA allo scopo di meglio contestualizzare i feed di Vulnerability) ✓dai Centri di competenza della rete dei CyberFusion Center altamente specializzati nella gestione delle attività di threat intelligence.

10.3 Modello operativo

10.3.1 Processi

In figura una rappresentazione di sintesi del modello operativo.

10.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di **Configurazione** ed **Erogazione** specifiche per il servizio in oggetto. Per le fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

Figura 35 - Modello operativo

CONFIGURAZIONE	
Configurazione Amministrazione	**Deliverable**: "Configurazione del servizio TI&VDF", che riporta le informazioni necessarie per la configurazione del servizio **Descrizione**: il servizio viene configurato con le seguenti informazioni relative alla PA fornite tramite il portale utenti e il servizio di Help Desk: ✓Nome della PA ✓Fascia del servizio richiesta ✓Nominativi, ruoli e informazioni di contatto dei referenti che riceveranno i feed, per la configurazione dei canali di ricezione ✓Canali di ricezione dei feed prescelti dall' PA (es. email, SMS)
Configurazione feed	**Deliverable**: "Configurazione del servizio TI&VDF" - sezione con l'elenco dei feed desiderati, i metodi di raccolta dei feed ed i risultati dei test effettuati allo scopo di verificare che la ricezione di tali feed sulla piattaforma TIS sia ottimale e che i dati siano leggibili e disponibili alla consultazione **Descrizione**: la raccolta, l'invio e la ricezione dei feed vengono configurati mediante le informazioni contenute nell'elenco dei feed previsti per la PA, il cui numero è da stabilirsi sulla base della fascia di servizio scelta
Configurazione della piattaforma	**Deliverable**: "Configurazione del servizio TI&VDF" - sezione sull'esito della configurazione della piattaforma TIS per l'accesso alla PA secondo le modalità previste. Vengono inoltre fornite le credenziali utilizzabili per l'accesso diretto alla piattaforma **Descrizione**: la piattaforma TIS viene configurata per consentire la ricezione dei feed previsti e per garantire l'accesso al Cliente. Viene effettuato il training del personale dell'PA che potrà accedere alla piattaforma per la consultazione diretta dei feed
Configurazione API e integrazione	**Deliverable**: "Configurazione del servizio TI&VDF" - sezione sui i risultati dei test effettuati per verificare che la ricezione dei dati mediante i sistemi in uso della PA sia ottimale e che i dati siano leggibili e disponibili alla consultazione **Descrizione**: vengono configurate le integrazioni necessarie per la consultazione dei feed raccolti dalla piattaforma mediante Interfacce di Integrazione (API). Vengono inoltre fornite le credenziali per utilizzare le API della piattaforma
EROGAZIONE	
Interrogazione feed	**Deliverable**: N/A **Descrizione**: funzionalità di interrogazione dei feed da parte della PA in due modalità: ✓**Lista completa**: la PA ha accesso alla lista completa dei feed e dei dati raccolti, consultabili direttamente sulla piattaforma TIS o tramite API ✓**Lista filtrata**: sulla piattaforma TIS o tramite API, la PA può eseguire ricerche mirate e avanzate mediante appositi filtri che consentono di accorpare i dati di interesse sulla base di diversi parametri (tipologia, data, contesto, associazioni di IoC, ecc.); ✓**Reporting**: la PA può generare report a partire dalle ricerche effettuate, scaricabili dalla piattaforma o ottenibili tramite API
Feeding altri strumenti	**Deliverable**: N/A **Descrizione**: la piattaforma TIS offre una sezione per monitorare lo stato e il numero delle segnalazioni inviate al SIEM del SOC. Tale sezione comprende anche le segnalazioni di IoC, inviate al SIEM automaticamente, e consente la generazione di report
Generazione reportistica	**Deliverable**: N/A **Descrizione**: i report del servizio TI&VDF possono essere generati on demand con due modalità: ✓**Reporting manuale**: mediante l'accesso diretto dalla piattaforma e la consultazione dei feed, è possibile generare manualmente tramite la Dashboard della piattaforma i report contenenti le informazioni di interesse, selezionabili tramite criteri flessibili (es. per campagna d'attacco, famiglia di malware, indicatori) ✓**Reporting automatico**: è possibile generare in modo automatizzato i report contenenti le informazioni di interesse mediante le API fornite

10.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "THREAT INTELLIGENCE & VULNERABILITY DATA FEED"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
PCI_USSS_TIV	Tempo di disponibilità dei servizi oggetto di fornitura e degli strumenti a supporto	Come USSS ma con frequenza maggiore e soglia più sfidante	Mensile	99%
KPI_RIP	Giorni di ritardo nell'installazione delle patch di sicurezza in carico alla PA ma dietro nostra segnalazione di vulnerabilità	Numero installazioni effettuate nei tempi previsti / Numero installazioni pianificate da effettuare (misurati sugli incident chiusi ove applicabile)	Trimestrale	85%

10.4 Interazioni

10.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
SOC	Indicatori di Compromissione	Output	Gli Indicatori di Compromissione e i dati di intelligence raccolti sono trasmissibili al sistema SIEM gestito dal servizio di SOC al fine di migliorare le attività di threat hunting
Gestione continua delle vulnerabilità	Informazioni sulle vulnerabilità in essere e potenziali	Input / output	Scambio di informazioni sulle vulnerabilità che possono essere di pertinenza delle PA al fine di integrarle nel ciclo di gestione e rimedio delle vulnerabilità stesse
Next Gen. Firewall	Indicatori di Compromissione	Output	Distribuzione di Indicatori di Compromissione direttamente sui firewall per prevenire e identificare le minacce di sicurezza

E' previsto l'utilizzo dei formati STIX/TAXII per l'integrazione con il sistema SIEM.

10.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
TI Report - Amministrazione	On Demand	Report generabile tramite API o Dashboard della piattaforma TIS, contenente i dati riguardanti la PA, ottenuti mediante i feed. È possibile generare il report in qualsiasi momento, filtrando dati, indicatori e fonti.
TI Report -Settore pubblico italiano	On Demand	Report generabile tramite API o Dashboard della piattaforma TIS, contenente i dati anonimizzati riguardanti le PA, ottenuti mediante i feed. È possibile generare il report in qualsiasi momento, filtrando dati, indicatori e fonti.
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sui NGFW solo qualora fossero previsti possibili impatti di servizio

11 PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA"

11.1 Soluzione proposta

Il modello **CDOM** proposto (cfr. §§1 e 3.3) colloca il servizio di Protezione Navigazione Internet e Posta Elettronica nel dominio di sicurezza: "**Breach Prevention & Readiness**", riconducibile alla Funzione NIST "**Protect**". Il servizio ha lo scopo di proteggere gli utenti e i sistemi delle PA da minacce esterne di natura cyber provenienti da web e/o email e di preservare affidabilità, disponibilità, riservatezza e integrità delle comunicazione tra le componenti client e server del patrimonio informativo posto in perimetro. La vasta esperienza su scala internazionale del RTI ha consentito di consolidare ed evolvere un **modello di servizio proprietario** che arricchisce ed estende la protezione dei canali d'interazione web, mail e client-server, attraverso l'adozione della piattaforma **SWMGP (Secure Web and Mail Gateway Platform)**, dispiegata c/o il Centro Servizi e integrata con altri sistemi di controllo attivo e passivo (SIEM/SOAR, TIS, FWM), alla quale accede esclusivamente personale esperto, altamente qualificato e certificato (SANS, OSCP, OSCE, CEH, OPST, etc.). La SWMGP integra **tecnologie leader di settore** (FortiGate SWG, FortiMail) e **strumenti e acceleratori proprietari** del RTI per consentire agli specialisti la massima **efficacia** nella gestione degli allarmi e la massima **efficienza** nei tempi di risposta e risoluzione. Il Centro Servizi del RTI si avvale, peraltro, della rete di CyberFusion Center resa disponibile da Accenture e altamente specializzata sia nella "deep inspection" del codice scaricato da internet (sandboxing basato sia su analisi comportamentale che su firme) che nel rilevamento di accessi ad applicazioni Cloud (SaaS) non conformi alle politiche delle PA contraenti (attraverso liste d'accesso e controlli granulari per la fruizione delle funzionalità), così come della rete di monitoraggio del traffico internet resa disponibile da Fastweb attraverso le proprie infrastrutture di sicurezza tipiche di un provider di servizi internet.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: più di 30 tra cui INPS, ISTAT, Consiglio Nazionale delle Ricerche, Comune di Napoli

Private: NEXI, Intesa Sanpaolo, Primario operatore finanziario

Descrizione di un caso di successo – INPS → Esigenza - Realizzazione e gestione di una infrastruttura di "secure web gateway", per circa 30.000 utenti, che consente di bloccare l'accesso a siti web potenzialmente malevoli in tempo reale, aggiornando la propria base dati in maniera automatica e quindi riconoscere il download di applicazioni potenzialmente dannose →**Soluzione** - È basata sulla tecnologia leader di mercato e caratterizzata da una componente centrale di gestione e dalle componenti gateway (fisiche) dislocate "on premise" presso INPS →**Benefici** - ✓assicura analisi del traffico, rilevazione e blocco dei comportamenti dannosi ✓aggiornamento delle liste dei siti (ogni 24 ore per il database dei contenuti, 5 minuti per il Real Time update e 15 minuti per l'Antivirus).

11.1.1 Funzioni Offerte

Il servizio prevede i **4 livelli**, già presentati al §6.1.1, che comprendono tutte le funzionalità richieste da Capitolato, incluse quelle avanzate di **Application Control**

e **Deep inspection** (dettagliate al §11.5) e ne aggiungono alcune **migliorative** di seguito descritte.

Funzioni migliorative per Protezione della Navigazione Internet

Predictive Machine Learning Sandboxing: il servizio è abilitato da una soluzione di rilevamento di **minacce complesse** che esegue analisi dinamiche volte a identificare sia **malware non ancora noto** sia **malware e ransomware creati appositamente** con proprietà di sandbox evasion. I controlli preventivi volti a disarmare le minacce all'interno della rete vengono attivati dagli output dell'intelligence applicata alle sandbox di investigazione. Contenuti e comportamenti utente vengono, infatti, simulati in ambiente protetto e analizzati da strumenti e personale specializzato nella ricerca di potenziali allegati alle email di natura malevola, utilizzando **algoritmi avanzati di ML** e **AI per filtrare e analizzare** file con peculiarità non note.

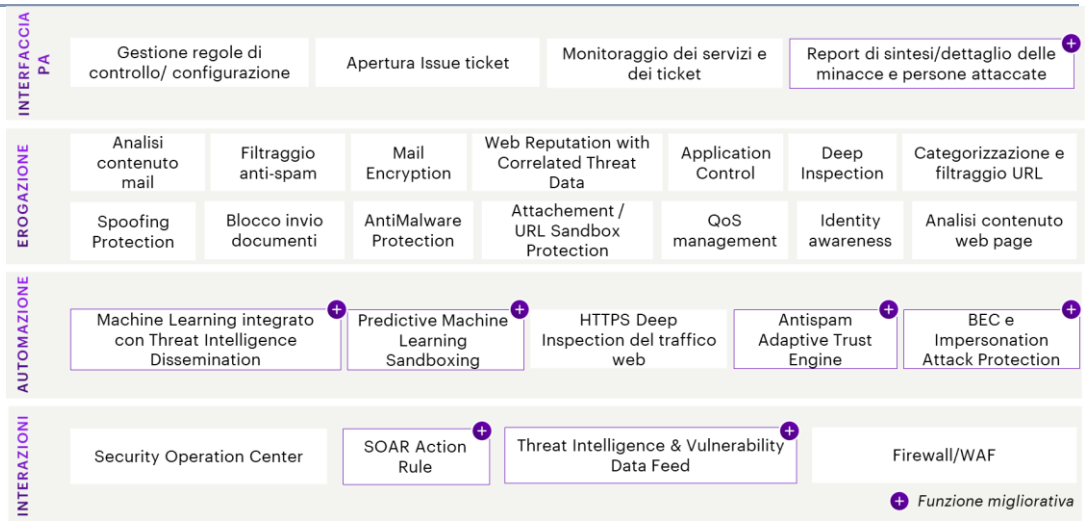


Figura 36 – Funzioni del Servizio

Funzioni migliorative per Protezione della Posta Elettronica

✓**Adaptive Trust Engineering**: Il servizio contempla il tracciamento delle relazioni mittenti-destinatari e il monitoraggio transazioni/interazioni per misurare le reti di fiducia e migliorare il rilevamento delle minacce, unitamente alla protezione delle email in uscita (funzionalità **aggiuntive**: attachment e URL analysis, recipient verification, impostor detection, account compromission detection) ✓**Business Email Compromise e Impersonation Attack Protection**: Il servizio si avvale di algoritmi avanzati volti alla protezione da attacchi di Impostor Detection, Business Email Compromise (Account compromission detection), CEO Fraud e Whaling, Display Name Attacks; prevede, inoltre, l'applicazione di **filtri basati sulla reputazione** dell'indirizzo IP di provenienza e/o URL, oltre che la protezione da email massive e campagne aggressive di marketing.

Funzioni migliorative comuni alla protezione della Navigazione Internet ed alla Posta Elettronica

✓**Reporting**: Il servizio prevede la produzione, periodica o a richiesta, di rendicontazione direzionale (executive summary) e tecnica di dettaglio (technical report) che riporta gli utenti più attaccati e le più rilevanti tipologie di minacce a cui sono sottoposti (es. l'elenco dinamico "Most attacked People" da porre sotto protezione di navigazione link nelle email attraverso sandbox, oppure la lista dei VIP account soggetti ad impersonification attacks), con informazioni utili per pianificare un **percorso di security awareness** mirato e individuale ✓**ML Integrato con Threath Intelligence Dissemination**: Il servizio si avvale di un sofisticato motore di ML che analizza eventi relativi a navigazione internet e comunicazioni di posta, sulla base delle evidenze prodotte dalla threat intelligence e volte a garantire la massima copertura dalle minacce più recenti (Core capabilities: FortiGuard Labs, Fortinet Security Fabric e proprietarie Accenture) ✓**Integrazione con Threat Intelligence & Vulnerability Data Feed**: Il servizio ricostruisce attivamente e sistematicamente una 'situational awareness' di contesto che rende fruibile ai servizi di Cyber Defence Governance (interagendo con threat monitoring and hunting) per aumentare la capacità di rilevamento nel caso di eventuali **scenari di attacco complessi** (es. attraverso threat data enrichment riportante informazioni su esperienze di navigazione o caselle attaccate dallo stesso malware seppur con mail apparentemente diverse) ✓**On demand investigation**: Servizio per analisi 'on demand' richieste dalle PA e relative a esperienze di navigazione o comunicazioni mail con allegati che richiedano approfondimenti o supplemento d'indagine. Interazioni ulteriori sono con i servizi SOC, Next Generation Firewall e Web Application Firewall dettagliatamente descritte al §11.4.1).

11.1.2 Architettura tecnologica

La piattaforma SWMGP è basata su tecnologia **Fortinet** integrata con strumenti e acceleratori proprietari del RTI. L'architettura prevista per la fornitura del servizio di protezione ✓della **navigazione internet** si avvale del modulo FortiGate SWG (Secure Web Gateway) ✓e quella per la protezione della **posta elettronica** del modulo FortiMail. Gli **acceleratori** Accenture della piattaforma SWMGP includono: ✓Standalone sandbox environment ✓Stack inspectors ✓Threat intel extra feed receiver ✓Threat Intelligence Dissemination. Tali strumenti sono resi disponibili agli specialisti del RTI per consentire gli approfondimenti sulle minacce complesse che richiedono attività di '**reverse engineering**'. La soluzione proposta prevede integrazione di appliance fisiche o virtuali presso i CED delle PA oppure implementazione remota presso il Centro Servizi, scelta subordinata a specifiche di contesto (es. caratteristiche

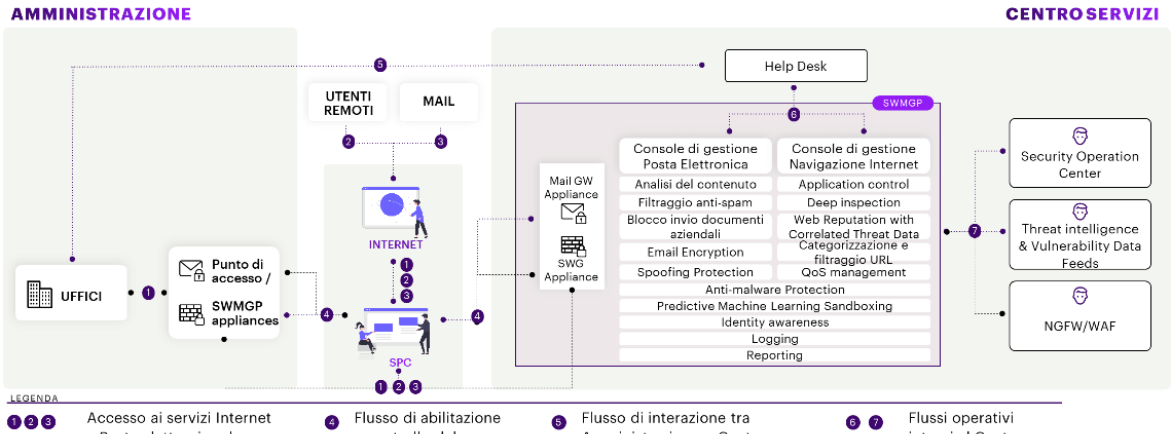


Figura 37 – Architettura tecnologica SWMGP

dell'infrastruttura di rete) e accordi con la singola PA. La scelta sarà effettuata in fase di attivazione del servizio. Il servizio si avvale inoltre dell'integrazione con i moduli **FortiGuard (antivirus)** e **Fortinet Security Fabric**. Il FortiGate SWG (**navigazione internet**) verrà utilizzato in modalità **transparent proxy** ovvero senza necessità di configurazioni lato client. Il servizio di **protezione della posta** verrà erogato in modalità **Gateway** per la protezione del traffico email sia in entrata che in uscita; opererà anche in modalità **out-of-line** per la scansione e il **clawback** (richiamo email) delle minacce direttamente in Microsoft 365 utilizzando l'API Graph.

11.2 Organizzazione

Nel contesto della struttura-tipo presentata al §6.2.1, il servizio è erogato da un unico gruppo di lavoro denominato **Web Navigation and Email Protection (WNEP) Team**, che risponde a un **Responsabile del servizio**, il quale rappresenta il punto di contatto tra il WNEP Team e la PA; il WNEP Team sarà così composto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall):

SOTTO-TEAM	RUOLO / Profilo	COMPITI E RESPONSABILITÀ
Team Email	Responsabili erogazione servizio Protezione posta elettronica / Sr-ISC + Jr-ISC	Il team presidia lo stato della sicurezza della posta elettronica, esegue analisi su base quotidiana e gestisce richieste SR, ingaggiato dall'Help Desk per erogare i servizi di cui al § successivo.
Team Firewall	Responsabili erogazione servizio Protezione Navigazione Internet / Sr-ISC + Jr-ISC	Il team presidia lo stato della sicurezza della navigazione web, esegue analisi su base quotidiana e gestisce richieste SR, ingaggiato dall'Help Desk per erogare i servizi di cui al § successivo.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant		

Sempre in analogia con il §6.2.1, il Team del servizio è supportato ✓dal CE Smart Hub (es. per identificare in dettaglio le tecnologie critiche in uso presso la PA allo scopo di meglio contestualizzare i controlli su navigazione e posta) ✓dai Centri di competenza della rete di CyberFusion Center altamente specializzati nella ricerca e mitigazione di attacchi ad alta complessità su navigazione web e posta elettronica.

11.3 Modello operativo

11.3.1 Processi

In figura una rappresentazione di sintesi delle fasi del servizio.

Figura 38 – Modello operativo

11.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di Configurazione ed Erogazione specifiche per il servizio in oggetto. Per la descrizione delle fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

CONFIGURAZIONE	
Configurazione sistemi	**Deliverable**: Specifiche di configurazione **Descrizione**: Configurazione degli apparati (tramite policy/regole standard o personalizzate. Integrazione con gli altri servizi interdipendenti
Migrazione dati	**Deliverable**: Piano di migrazione e specifiche ETL **Descrizione**: Migrazione policy/regole standard o personalizzate per configurare gli apparati
EROGAZIONE	
Gestione profili di navigazione	**Deliverable**: Matrice di profilazione **Descrizione**: L'Help Desk indirizza la creazione e/o la modifica dei profili di navigazione Internet, abilitando/disabilitando/limitando l'accesso a diverse categorie di siti web
Personalizzazione categorie e filtri nav.	**Deliverable**: Specifiche di navigazione **Descrizione**: Creazione di categorie 'custom' di siti web per il filtering della navigazione Internet
Gestione soglie anti-spam	**Deliverable**: Specifiche anti-spam **Descrizione**: Gestione delle soglie di spam e high-spam personalizzate per singoli o gruppi di utenti (con filtering ulteriore e dedicato per alcune classi di utenti – VIP)
Gestione allegati di posta	**Deliverable**: Specifiche di controllo allegati **Descrizione**: Gestione dei filtri di blocco degli allegati in base a: tipologia, estensione e profilo di rischio associato ai file
Controllo accessi via white/black-listing	**Deliverable**: Access Control List(s) **Descrizione**: Gestione delle liste di controllo accessi per la protezione della posta elettronica e per la navigazione Internet
Esfiltrazione email malevole	**Deliverable**: Verbale di rendicontazione attività **Descrizione**: Gestione delle richieste di rimozione di email dalla posta elettronica di uno o più utenti (comprese tutte le successive conversazioni correlate)

Non elencate, sono altresì previste le attività di **Aggiornamento e Manutenzione** curate in autonomia dal centro servizi. Tali attività possono riguardare aggiornamenti software, hotfix, operazioni di riavvio di specifici dispositivi, atti a garantire il corretto svolgimento dei servizi di protezione. In particolare, la gestione degli **avanzamenti software e firmware** verrà notificata, programmata ed eseguita fuori orario base e preservando la continuità del servizio.

11.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, illustriamo gli indicatori aggiuntivi per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSA	Cfr. §6.3.4			
PCI_TNSA	Cfr. §6.3.4			
KPI_NAUB	Numero accessi a URL pericolosi bloccati	Conteggio complessivo degli eventi	Trimestre	Riduzione rispetto alla misura del periodo precedente
KPI_NMSB	% messaggi spam bloccati rispetto ai totali	Rapporto tra messaggi bloccati e messaggi ricevuti	Trimestre	Incremento rispetto alla misura del periodo precedente

11.4 Interazioni

11.4.1 Flussi verso altri servizi

ALTRO SERVIZIO	FLUSSO	I/O	DESCRIZIONE/FINALITÀ
SOC	Audit log e log di eventi di sicurezza	Output	La piattaforma SWMGP trasmetterà i log di sicurezza (audit e alarms) al SIEM affinché gli eventi di navigazione internet e inerenti alla posta elettronica possano essere correlati con gli eventi di altri sistemi per ricostruire correttamente gli scenari dei casi d'uso posti sotto monitoraggio.
SOC via SOAR	Filtering rules	Input	Regole puntuali per l'applicazione di filtri di navigazione e/o di controllo di comunicazioni/allegati di posta elettronica attivate da automatismi SOAR (actionable triggers).
Threat Int. & Vulnerability Data Feed	Audit log e log di eventi di sicurezza	Output	La piattaforma SWMGP trasmetterà i log di sicurezza (audit e alarms) al servizio di Threat Monitoring per aumentare la conoscenza del contesto nel caso di incidenti, investigazione o approfondimenti.
Threat Int. & Vulnerability Data Feed	Ind. di Compromissione (IoC) e Indicatori di Attacco (IoA)	Input	Gli IoC/IoA provenienti dalla piattaforma di Threat Intelligence di Accenture sono inviati alla piattaforma SWMGP (moduli FortiGate SWG e FortiMail) e costantemente aggiornati per aumentare il livello di copertura verso minacce recenti.
Next Generation Firewall e Web Application Firewall	Firewall rules ed IDS/IPS signatures	Output	Regole Firewall e firme per IDS/IPS, per filtering e continuous analysis del traffico a livello applicativo (layer 7).

11.4.2 Report aggiuntivi per l'Amministrazione

NOME REPORT	PERIODICITÀ	DESCRIZIONE
Threats/Malware report	settimanale	Tipologie di minacce di cui sono stati oggetto gli utenti, indicando per ciascun caso la presenza di eventuali casi andati a segno.
Most Attacked People	mensile	Riepilogo delle persone più attaccate nel periodo, sia su navigazione internet che su posta elettronica.
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese

11.5 Caratteristiche funzionali avanzate

Le modalità d'impiego delle funzionalità avanzate del servizio rese disponibili alle PA saranno concordate in fase di attivazione e predisposte in fase di configurazione. Un processo di miglioramento continuo attivato in fase di erogazione e governato dal centro servizi fornirà alle PA le proposte di ottimizzazione delle configurazioni al variare del panorama delle minacce e delle specificità di contesto, al fine di mantenere i più alti standard di protezione anche in divenire.

11.5.1 Deep Inspection

Il servizio contempla un meccanismo di protezione avanzata dalle minacce, che esegue una verifica preliminare sulla conformità di browser e plug-in che hanno eseguito la richiesta della URL e una successiva ispezione completa e profonda del contenuto del pacchetto. L'esecuzione della deep inspection è in grado di rilevare qualsiasi malware nascosto all'interno di una risorsa web, sia esso noto (via signature matching) o ignoto (behavioral based), attraverso avanzate funzionalità di prevenzione fondate su AI/ML che si avvalgono di algoritmi predittivi applicati alla sandbox per rilevare varianti complesse di malware recenti e/o attacchi di tipo Zero-Day. Il servizio rileva iFrame nascosti, cross-site scripting, segni di tentativi di phishing e ransomware, furto di cookie e comunicazioni botnet ai server C&C. Tutti i pacchetti sono sottoposti a ispezione in profondità poiché tipicamente le pagine web sono dinamicamente generate con contenuti personalizzati costituiti da centinaia di oggetti ottenuti dalle fonti più varie; ogni oggetto rappresenta pertanto una potenziale minaccia e viene considerato non attendibile indipendentemente dalla fonte (zero-trust). L'analisi del traffico criptato (incluso il protocollo TLS 1.3) viene eseguita ad alte prestazioni (leader di settore), il servizio permette la completa ispezione in real-time del traffico criptato su tutte le porte e i protocolli. La conoscenza del panorama delle minacce combinata con la capacità di rispondere rapidamente agli allarmi è abilitata da ricercatori Accenture iDefense e Fortinet che setacciano quotidianamente su scala globale il web (clear, dark, deep) per scoprire minacce emergenti e sviluppare contromisure efficaci. **Più di 250.000 organizzazioni nel mondo** si avvalgono della tecnologia proposta.

11.5.2 Controllo Accessi ad applicazioni cloud SaaS non conformi

Il servizio contempla un meccanismo di controllo accessi d'avanguardia tale da garantire connessioni veloci e sicure e consentire ai dipendenti di lavorare da qualsiasi luogo utilizzando Internet per accedere alla rete aziendale, ottimizzando peraltro l'uso della larghezza di banda della rete, prioritizzando o bloccando il

traffico in base all'applicazione. Basato sul paradigma zero-trust, il servizio fornisce una sicurezza completa avvalendosi dell'identità digitale emergente dal contesto e dell'applicazione di politiche d'accesso per applicazioni SaaS che si riflettono nei profili di sicurezza assegnati/assegnabili dinamicamente all'utente in base al rischio attinente a identità, dispositivo e localizzazione. Il rischio associato all'utente viene costantemente aggiornato in base alla propria risk-posture e al raggiungimento di soglie predefinite/configurabili, può essere automaticamente assegnato un profilo d'accesso più limitato, sino alla restrizione totale della navigazione in caso di comportamenti sospetti. Il controllo accessi applicativo migliora la sicurezza e soddisfa i requisiti di conformità in virtù dell'applicazione di policy volte a consentire, negare o limitare l'accesso a specifiche applicazioni od a categorie di applicazioni (con attuazione in tempo reale). Il servizio vanta uno dei più rilevanti database di applicazioni (su tecnologia Fortinet, leader di mercato) costantemente aggiornato per proteggere le PA da funzionalità rischiose e consentire piena visibilità e controllo delle sessioni/chiamate in esecuzione. Il servizio è in grado di riconoscere la **totalità di protocolli applicativi** dei maggiori servizi SaaS ad oggi esistenti, classificati per tipologie (es. Cloud Storage, Social Networks, e-commerce, Media and TV Streaming, Team Working, Remote Desktop Tools, Videocall and messaging tools). Risulta peraltro possibile definire profili di accesso differenti che blocchino/permettano l'utilizzo di tutte/alcune categorie o di singoli applicativi non conformi alle politiche aziendali, applicando sistemi di white-listing/black-listing granulari. **L'actionable intelligence** fornita attraverso il servizio di controllo delle applicazioni proviene dal team di sviluppo globale di FortiGuard Labs, leader del settore e attivo nella ricerca sulle vulnerabilità.

12 PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA" - FUNZIONALITÀ AGGIUNTIVE

Con riferimento al servizio di "protezione navigazione internet e posta elettronica" (di cui al par. 3.1.6 del Capitolato Tecnico speciale), il Raggruppamento conferma la presenza di funzioni di protezione della posta anti-phishing e anti-ransomware.

13 PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE DEGLI END POINT"

13.1 Soluzione Proposta

Partendo dal modello **CDOM** (cfr. §§ 1 e 3.3) definiamo le componenti per le operazioni di sicurezza a copertura del servizio di Protezione degli Endpoint. Il CDOM colloca questo servizio nel dominio di sicurezza "**Breach Prevention & Readiness**" / Funzione NIST "**Protect**".
Il servizio di protezione degli Endpoint (PEP) rappresenta uno degli elementi chiave forniti dal Centro Servizi per garantire la sicurezza delle infrastrutture delle PA, operando direttamente sui dispositivi in uso agli utenti abilitando sia l'identificazione di anomalie di processo che le azioni di contenimento e reazione da implementare in caso di violazione. La soluzione tecnologica di Endpoint Protection proposta è basata su tecnologia **TrendMicro ApexOne**, riconosciuta come leader sul mercato da **Gartner nel Magic Quadrant 2021** di Endpoint Protection Platform. Tale tecnologia fornisce un'ampia e consolidata copertura dei requisiti di tecnico-funzionali espressi nel capitolato e rappresenta un elemento fondamentale e raccomandato nel catalogo offerto del Centro Servizi. Accenture, Fastweb e Trend Micro collaborano nell'esecuzione di numerose progettualità a livello globale su clienti di diversi settori. Importante sottolineare che Accenture, Fastweb e Trend Micro collaborano congiuntamente nello sviluppo delle soluzioni presso i propri Clienti unendo le competenze di prodotto e di system integration e gestione che, congiuntamente, consentono di adeguare il prodotto alle effettive necessità dei Clienti. All'interno di tale collaborazione si procederà anche a indirizzare uno sviluppo/integrazione di prodotto dedicata alle PA. La soluzione proposta consente di ✓effettuare l'ispezione del traffico generato dalla postazione di lavoro, ✓controllare lo scambio di dati (Data Loss Prevention – DLP) in maniera tale che le informazioni sensibili non possano essere trasferite ad attori non autorizzati ✓controllare lo stato di compliance dei dispositivi rispetto a policy di sicurezza ben definite ✓inviare log al SIEM integrandosi nel Servizio di Security Operation Center e abilitando il monitoraggio 24x7. La soluzione sfrutta tecniche di rilevamento delle anomalie avanzate tramite: ✓metodologie di **ML** prima e durante l'esecuzione dei file ✓tecniche di **cancellazione del rumore di fondo**, come censimento ed elenchi di utenti autorizzati, a ogni livello di rilevamento, per ridurre drasticamente i falsi positivi ✓tecniche specifiche per la protezione contro script, iniezioni, ransomware e attacchi a memoria e browser, grazie a un'innovativa **analisi del comportamento**.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: 2 - Guardia di Finanza, Croce Rossa Italiana

Private: Veritas

Descrizione di un caso di successo - **Guardia di Finanza** →**Esigenza** - Implementazione di una soluzione di end point protection per diverse migliaia di postazioni di lavoro, che sia in grado di effettuare il monitoraggio e la protezione delle postazioni di lavoro da rischi derivanti dalla navigazione web o da altri fattori di rischio →**Soluzione** – Fastweb ha realizzato una soluzione con tecnologia leader di mercato che prevede l'installazione di SW agent sugli endpoint distribuibili in maniera semi-automatica attraverso piattaforme di sw deployment dell'Amministrazione →**Benefici** - ✓protezione dalle minacce informatiche più recenti, incluse le minacce fileless ✓riduzione del rischio di esposizione ai cyberattacchi, grazie all'hardening degli endpoint ✓incremento del livello di sicurezza dei dispositivi utilizzati dai dipendenti attraverso avanzati controlli cloud-enabled ✓protezione dei server e degli endpoint senza comprometterne le performance ✓gestione semplificata della sicurezza delle postazioni di lavoro tramite una console unificata.

13.1.1 Funzioni offerte

Il servizio prevede i **4 livelli**, già presentati al §6.1.1, che comprendono tutte le funzionalità richieste da Capitolato e ne aggiungono alcune **migliorative** di seguito descritte.

✓**Anti malware avanzato**: la soluzione proposta prevede l'applicazione di algoritmi di ML prima e durante l'esecuzione dei processi, al fine di rilevare più accuratamente attività associabili a malware, ivi incluse forme **fileless e ransomware**; ✓**Host-based Intrusion Prevention System (IPS)**: una funzionalità che consente di mantenere i sistemi protetti contro vulnerabilità note e sconosciute (Zero Day vulnerabilities); tale funzionalità è ulteriormente potenziata dall'integrazione con le informazioni rese disponibili dalla Trend Micro Zero Day Initiative (ZDI) che, tramite la ricerca strutturata di nuove vulnerabilità, consente di identificarle in anticipo (giorni, settimane o mesi prima rispetto alla concorrenza) e abilitare il patching virtuale con cui è possibile anticipare una patch ufficiale da parte del fornitore;

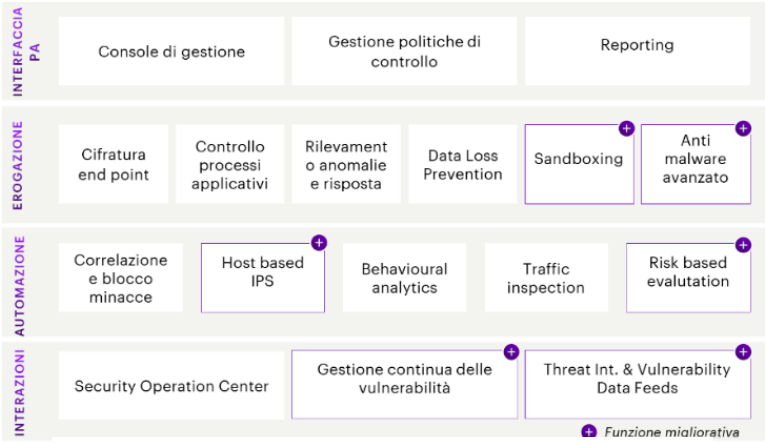


Figura 39 - Funzioni del servizio Protezione Endpoint

✓**Risk based evaluation***:* per ogni change funzionale ed infrastrutturale la soluzione consente di eseguire la stima di impatti e rischio sulle configurazioni implementate o che si prevede di implementare fornendo all'utente e all'operatore una vista chiara delle modifiche necessarie per una configurazione sicura; tali valutazioni sono effettuate tenendo in considerazione: la classificazione del servizio impattato, la criticità del servizio abilitato per la PA e le dipendenze ed interazioni con altri servizi, funzioni e sistemi ✓**Sandboxing** per l'analisi degli elementi sospetti che richiedono di approfondimenti specifici ✓Interazioni con i servizi **Gestione continua delle vulnerabilità di sicurezza** e di **Threat Intelligence & Vulnerability Data Feed**, dettagliatamente descritte al §13.4.1).

13.1.2 Architettura tecnologica

L'architettura tecnologica prevede: ✓**componenti centrali (Apex Central)**, localizzate nel Centro Servizi, che consentono la gestione delle funzionalità di endpoint protection, oltre alle funzionalità di reportistica e analisi degli eventi di sicurezza in caso di segnalazioni; ✓**componenti distribuite (agent)** basate su agent da installare sui dispositivi utenti da proteggere, compatibilmente con le versioni di sistema operativo supportati (scelta subordinata agli accordi con la PA contraente).

Tramite la componente Apex One Server, la piattaforma di controllo centralizzata comunica con gli agenti distribuiti al fine di impostare su ognuno di essi le configurazioni amministrative relativamente alle funzionalità di sicurezza, istruendoli ad eseguire determinati controlli, impostare esclusioni e attivare allarmi. L'agente sul dispositivo utente comunica con l'infrastruttura centrale per la condivisione di dati telemetrici utili agli analisti per le fasi di rilevazione e risposta agli attacchi. La soluzione abilita una comunicazione tra agente e server di gestione centrale indipendente dalla locazione dell'utente tramite la componente **edge relay** consentendo il controllo degli utenti anche quando connessi tramite internet, condizione che si verifica tipicamente con l'adozione di forme di **lavoro agile** (smart working).

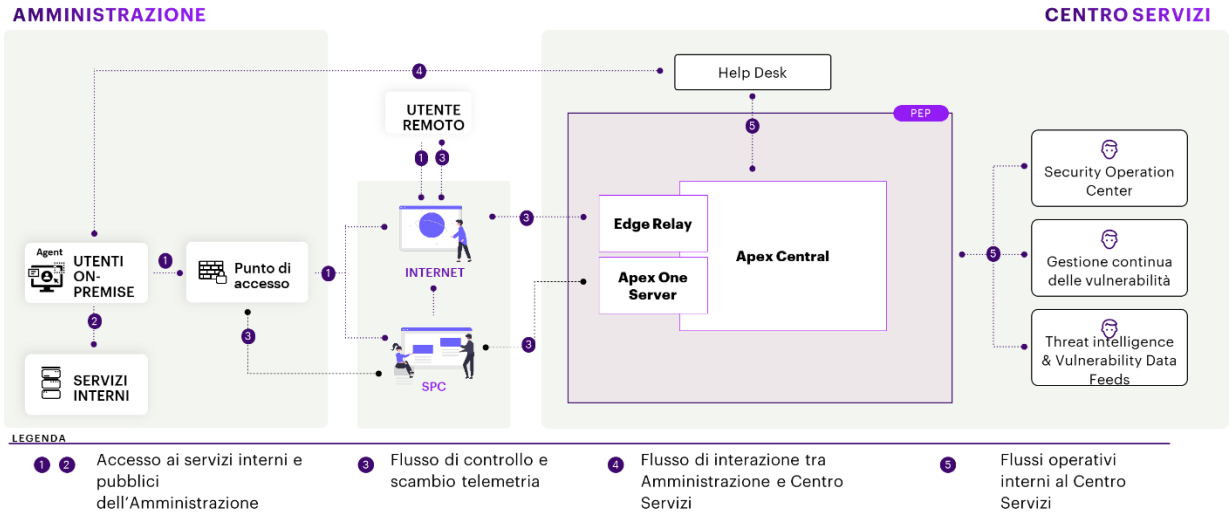
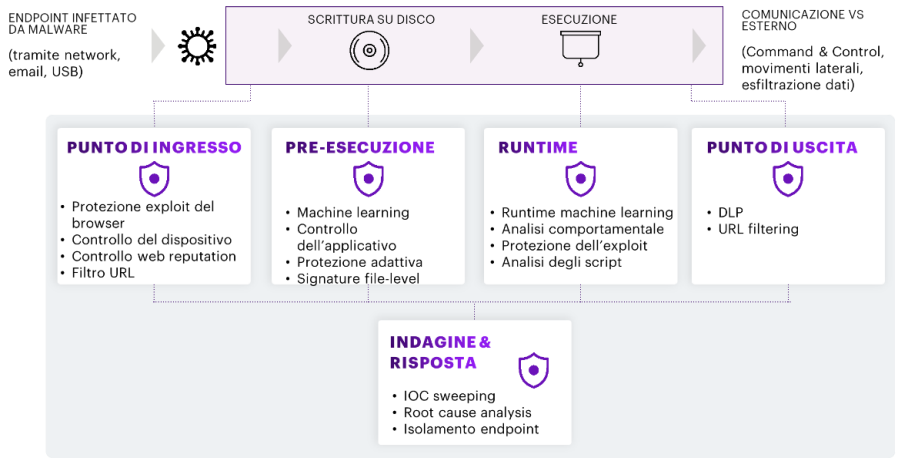


Figura 40 – Architettura Tecnologica Protezione Endpoint



La console centrale consente di avere un unico punto di visibilità e analisi degli eventi, abilitando al contempo la possibilità di gestire in maniera indipendente più domini amministrativi, ossia insieme di agenti che condividono le stesse configurazioni ed eseguono gli stessi compiti. Nel momento in cui viene rilevata una minaccia, l'agente può essere istruito per applicare diverse azioni quali blocco, quarantena o eliminazione dell'oggetto. Inoltre, la soluzione è **integrata con ambienti di sandboxing:** gli oggetti sospetti possono essere inviati alla sandbox (ubicata nei DC del RTI) per un'analisi avanzata. Gli amministratori possono accedere ad una reportistica dettagliata che dimostra ogni singola azione effettuata dall'oggetto analizzato nell'ambiente protetto come comandi powershell lanciati, file o chiavi di registro modificate e chiamate URL verso l'esterno.

13.1.3 Caratteristiche tecnologiche e prestazionali migliorative

La soluzione proposta ha al suo interno diversi fattori distintivi e migliorativi. In particolare introduce i seguenti elementi distintivi: ✓sistema automatizzato avanzato di rilevamento e risposta, a una varietà sempre più ampia di minacce, tra cui fileless e ransomware; ✓approfondimento delle informazioni, capacità investigative ampliate e visibilità centralizzata tramite una forte integrazione SIEM e l'adozione di un set di API aperto; ✓protezione integrata gestita da un singolo agente per rilevamento, risposta e indagine delle minacce, riducendo l'effort di gestione da parte delle singole PA. La soluzione consente inoltre di intervenire sulla catena di attacco in diversi momenti e applicando azioni di contenimento fra loro complementari, come indicato in figura, nelle seguenti fasi del ciclo operativo del malware: infezione dell'endpoint, pre-esecuzione, esecuzione runtime, uscita per esfiltrazione dati o esecuzione di movimenti laterali.

13.2 Organizzazione

13.2.1 Strutture coinvolte

Il servizio Protezione degli Endpoint è erogato da un team specializzato, che risponde a un **Responsabile del servizio**; il team è supportato da uno SME (Subject Matter Expert) esperto su tecnologie Endpoint Protection. Come per gli altri servizi è previsto il supporto delle seguenti strutture: ✓**CE SMART HUB** (cfr. §6.2.1) ✓**Centri di Competenza/Partnership** che forniscono competenze specialistiche. In particolare, il team di lavoro avrà la possibilità di avvalersi del supporto aggiuntivo del Cyber Fusion Center del RTI e il supporto specialistico del vendor. Il team è composto (tranne il Responsabile del servizio con caratteristiche uguali a quelle presentate al §6.2.2 per il servizio Next Generation Firewall) come da tabella seguente.

13.2.2 Team del servizio

Sotto-Team	Ruolo / Profilo	Compiti e Responsabilità
SME Protezione Endpoint	Supporto al team Protezione Endpoint / SSA	Offre consulenza per l'installazione / configurazione della soluzione in caso di problematiche specifiche e/o nella gestione di eventi / incidenti che non possono essere gestiti con le azioni di analisi e rimedio ordinarie. Viene inoltre coinvolto per l'ottimizzazione della soluzione nel suo complesso.
Team Protezione Endpont	L2 Security Engineer / Sr-ISC	Supporta e integra le attività del L1 e si attiva per incident di priorità elevata e change complesse. Attiva il supporto dei Vendor e gestisce l'andamento della richiesta sino alla chiusura.
Team Protezione Endpont	L1 Security Engineer / Jr-ISC	Esegue procedure per la risoluzione delle richieste relative a installazioni, configurazioni e incidenti, attivando eventualmente procedure di escalation verso L2 in caso di necessità.
Legenda: Sr-ISC Senior Information Security Consultant, Jr-ISC Junior Information Security Consultant, SSA Security Solution Architect		

13.3 Modello operativo

13.3.1 Processi

Si riporta a seguire una rappresentazione di sintesi del modello operativo.

Figura 42 - Modello operativo

13.3.2 Modalità di erogazione

Di seguito viene presentata la descrizione delle attività delle fasi di configurazione ed erogazione specifiche per il servizio in oggetto. Per le fasi di **Attivazione** e **Chiusura** vale quanto descritto al §6.3.2.

CONFIGURAZIONE	
Setup e supporto alla distribuzione degli agenti	**Deliverable**: "Report distribuzione degli agenti" contenente la definizione delle funzionalità incluse nel pacchetto di installazione e del report finale di distribuzione degli agenti. **Descrizione**: Si procederà a ✓definizione del pacchetto di installazione dell'agente al fine di soddisfare le esigenze di sicurezza definite nell'analisi dei fabbisogni, ✓supporto per la strategia di distribuzione degli agenti (compatibilità con i sistemi, wave pilota, modalità di deployment), ✓verifica della copertura dei sistemi in perimetro.
Configurazione e messa in produzione	**Deliverable**: "Configurazione del servizio Protezione degli EndPoint", contenente il dettaglio delle policy implementate e i test eseguiti per validazione del deployment. **Descrizione**: Si procederà a: ✓ implementazione delle policy di sicurezza per garantire la protezione degli endpoint, ✓esecuzione di test per verificare che le policy implementate siano efficaci dal punto di vista funzionale di sicurezza e che non blocchino l'operatività della PA.

EROGAZIONE	
Gestione ciclo di vita policy	Deliverable: Aggiornamento delle policy di sicurezza
	Si procederà alla manutenzione continua delle policy di sicurezza in funzione delle esigenze espresse dalla PA e/o da evidenze provenienti dal Servizio SOC e/o di Threat Intelligence e Vulnerability Feed
Operation	Deliverable: Report attività manutenzione
	Si procederà alla gestione di anomalie mediante: ✓l'applicazione di soluzioni permanenti, ove già disponibili, utili a risolvere la casistica ✓l'applicazione di workaround e analisi successiva della root cause in assenza di soluzioni disponibili. Nel continuo si procederà alla verifica dello stato della soluzione e dei relativi processi di controllo
Reporting	Deliverable: Report di servizio
	Si procederà alla generazione di report standard e personalizzati, corredati di statistiche e grafici ed esportabili in xls o pdf

13.3.3 Controllo Qualità

Nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "PROTEZIONE DEGLI END POINT"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_TNSA	Cfr. §6.3.4			
PCI_TNSA	Cfr. §6.3.4			
KPI_NVMB	Virus e malware bloccati: Numero medio di eventi per end point	Numero virus e malware bloccati / Numero di end point	Trimestre	Riduzione rispetto alla misura precedente

13.4 Interazioni

13.4.1 Flussi verso altri servizi

Altro Servizio	Flusso	I/O	Descrizione/Finalità
Security Operation Center (SOC)	Log di audit ed eventi verso il SIEM	Output	I sistemi inviano log al SIEM affinché gli eventi generati dagli endpoint e dalle elaborazioni della console centrale possano essere correlati con gli eventi di altri sistemi al fine di rilevare situazioni d'interesse per la cybersecurity e di arricchire di informazioni la ricostruzione della timeline di incidenti di sicurezza
Gestione continua delle vulnerabilità	Vulnerabilità in essere/potenziali	Input/ Output	La console centrale scambia con il servizio informazioni relative alle vulnerabilità identificate sui sistemi e relative configurazioni e riceve informazioni in merito alla relativa criticità e prioritizzazione
Threat Intelligence & Vulnerability Data Feed	IoC	Input	Gli IoC provenienti dalla piattaforma di Threat Intelligence sono raccolti in input dalla console centrale ApexOne per limitare l'accesso a URL, IP e domini oltre al trasferimento di file malevoli (mediante hash)

13.4.2 Report aggiuntivi per l'Amministrazione

Nome Report	Periodicità	Descrizione
Executive Summary servizio	Mensile	Riassunto dell'andamento mensile del servizio, evidenziando: ✓i volumi di richieste ricevuti, gestite ed eventuali backlog per il mese di riferimento con relativi dettagli (es. gruppo di competenza, severità) ✓i valori di KPI e SLA ✓gli incidenti gestiti ✓situazioni rilevanti nel mese quali particolari minacce rilevate, eventuali compromissioni e risposte eseguite
Technical report servizio	Mensile	Dettaglio di incidenti gestiti e remediation applicate, oltre a indicazioni sulle maggiori minacce, includendo azioni congiunte da applicare sugli endpoint solo qualora fossero previsti possibili impatti di servizio.

14 PROPOSTA PROGETTUALE PER IL SERVIZIO "FORMAZIONE E SECURITY AWARENESS"

La formazione dei dipendenti su tematiche di cyber security è uno degli aspetti fondamentali per sensibilizzare il personale delle PA sulle tematiche inerenti alla sicurezza delle informazioni ed evitare che comportamenti non adeguati dei singoli soggetti possano compromettere la sicurezza dell'intero sistema. Il servizio proposto ha lo scopo di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi. Il CDOM proposto (cfr. §§1 e 3.3) colloca il servizio di Formazione e Security Awareness nel dominio di sicurezza "**Breach Prevention & Readiness**" riconducibile alla Funzione NIST "**Protect**". Al fine di erogare un servizio efficace è necessario fare leva su una serie di fattori innovativi, necessari a garantire il coinvolgimento dell'utente in funzione della percezione che questo ha della sicurezza informatica e dei rischi indotti dalla sua operatività quotidiana, distinti in funzione di ruoli e mansioni ricoperte. Tra i fattori innovativi della proposta evidenziamo, in particolare: ✓**Assessment delle competenze dell'utente** prima dell'esecuzione degli interventi di awareness con l'obiettivo di definire azioni adeguate e motivanti nel percorso di formazione; ✓**Coinvolgimento dell'utente** tramite diversi canali e strumenti, specificamente definiti in funzione delle caratteristiche ricoperte nell'organizzazione delle PA e dei rischi di sicurezza ad esso pertinenti; ✓Utilizzo di **canali e-learning** che facilitano l'accesso continuativo ai servizi e coinvolgono l'utente in percorsi di formazione progressivi nel tempo, con contenuti che possono essere usufruiti secondo le disponibilità operative; ✓Sviluppo di contenuti formativi tramite le **agenzie di Accenture dedicate** al mondo della comunicazione e dell'interattività così da fornire format e qualità di contenuti video e grafici adeguati ad ottenere un forte livello di engagement sulla tematica; ✓Supporto della Fastweb Digital Academy che ha l'obiettivo di portare un contributo alla crescita di innovazione e cultura digitale nella società italiana tramite la definizione di corsi di formazione in Cybersecurity; ✓Adozione di **strumenti di verifica** del livello di formazione acquisito sulla base di meccanismi basati su analytics e AI per la somministrazione di test di verifica specifici, simulazioni (real life assessment) e certificazione / riconoscimento dei risultati raggiunti; ✓Disponibilità di **personale altamente specializzato** e certificato su tematiche di sicurezza informatica e continuità operativa (certificazioni ISO 27001, ISO 22310, CSX, CISA, CISSP, CISM) che predispone, sviluppa specificamente ed eroga i contenuti formativi; ✓Disponibilità, su richiesta, di **interventi formativi dedicati** da erogare in aula o comunque con risorse dedicate alle singole PA.

Credenziali pubbliche e private (con attestati disponibili) - Elenco non esaustivo

Pubbliche: IVASS, ASL Frosinone

Private: primario Gruppo assicurativo europeo, primario Gruppo bancario europeo, 2 primari Gruppi bancari italiani, primario operatore in ambito Pagamenti, associazione di categoria di imprese italiane

Descrizione di casi di successo - Si rimanda al §14.2.

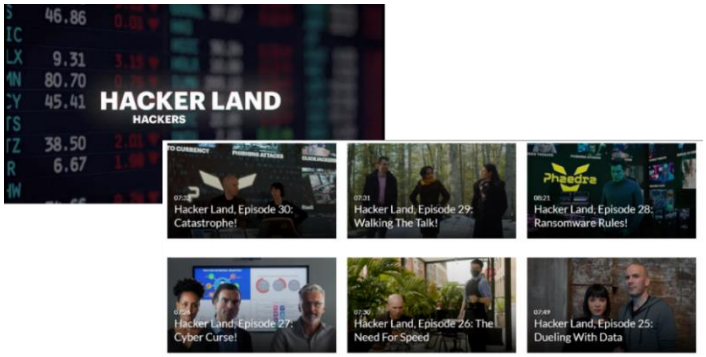
14.1 Metodologia e asset disponibili

I contenuti di sicurezza informatica richiedono approcci specialistici per poter essere efficaci in quanto si rivolgono ad una platea molto eterogenea in termini di competenze e necessità. A tal fine Accenture ha definito una metodologia specifica, denominata **Accenture Security Awareness Journey**, che intende adottare per poter indirizzare al meglio gli interventi verso ciascuna categoria di utenti. Secondo tale metodologia, ciascuna iniziativa deve rispondere a 3 specifiche domande: **Who, What, How**, quali sono i target dell'iniziativa, quali contenuti devono essere sviluppati e qual è il mezzo di comunicazione più efficace tenuto conto dei messaggi da veicolare e dei target a cui questi sono rivolti. È inoltre previsto che lo sviluppo della consapevolezza nelle persone e l'efficacia del programma siano supportati da metriche e strumenti di monitoraggio appropriati. Per ogni iniziativa è impostato e analizzato un KPI specifico.

Tale approccio consente di definire un modello di servizio specifico per le PA che prevede: ✓**Segmentazione audience**: identificazione e clusterizzazione dei target da coinvolgere nel programma di formazione distinguendo il personale operativo dal personale con ruoli di responsabilità ✓**Definizione canale di erogazione**: identificazione del canale di erogazione delle iniziative (privilegiando il canale e-learning ritenuto il più efficace per raggiungere il personale delle PA) ✓**Sviluppo dei contenuti**: definizione dei contenuti da erogare in funzione del target identificato e aggiornamento degli stessi con cadenza periodica in base all'evoluzione

delle minacce di sicurezza e del contesto operativo delle PA ✓**Erogazione dei contenuti**: fornitura del servizio di e-learning tramite piattaforma dedicata su cui vengono abilitati gli utenti e che include i moduli di verifica dell'apprendimento e programmazione, su specifica richiesta, di sessioni in aula e/o da remoto con specialisti di sicurezza per l'approfondimento di specifiche tematiche ✓**Verifica apprendimento**: introduzione di strumenti di verifica delle competenze tramite campagne interattive (es. simulazioni di phishing) e campagne di gaming.

In termini di asset Accenture dispone di una propria piattaforma e-Learning descritta nel §14.4 che include strumenti di formazione già utilizzati e testati in tema di security awareness. Tale piattaforma, include in particolare i moduli **Hackerland**, una serie di video, di pillole formative e di test specificamente sviluppati per utenti esperti e non esperti su tematiche di Cyber Security tra cui, a titolo esemplificativo: ✓Come lavorare in sicurezza da casa; ✓Come evitare attacchi ransomware; ✓Come gestire le mail di phishing. Questi contenuti sono per altro conformi a quanto messo a disposizione in termini metodologici **da AgID per le PA**. La piattaforma è adottata da Accenture a livello globale per tutti i propri dipendenti e potrà essere sviluppata ad hoc in base alle esigenze formative delle PA contraenti.



14.2 Competenze

L'erogazione di servizi di Security Awareness richiede l'integrazione di diverse competenze su cui Accenture dispone di risorse riconosciute a livello di mercato: ✓**Competenze in ambito Cyber security** al fine di proporre e definire contenuti adeguati alle esigenze delle PA; ✓**Competenze in ambito comunicazione/media** per poter identificare le migliori metodologie per il coinvolgimento degli utenti; ✓**Competenze in ambito sviluppo e gestione applicativa** per poter implementare strumenti di e-learning in modalità efficace. Accenture dispone di competenze fortemente specialistiche in tema di Security Awareness e le valorizza integrando risorse con formazione in ambito cyber security con risorse con formazione finalizzata a sviluppare ed erogare contenuti agli utenti finali. L'utilizzo di queste competenze ha permesso di raggiungere risultati estremamente significativi presso i Clienti italiani ed europei di Accenture: ✓Presso un **primario Gruppo assicurativo europeo** la prima campagna di security awareness ha raggiunto il 98% - quasi 13.000 - dipendenti; il successo dell'iniziativa, oltre all'elevatissima numerosità degli utenti che hanno aderito, è dimostrata dalle attività di verifica eseguite tramite campagne di phishing che hanno portato ad una diminuzione del tasso di esecuzione di operazioni malevole (click sui link malevoli riportati nelle mail) al 20% rispetto ad un tasso di partenza pari al 39%. ✓Presso un **primario Gruppo bancario italiano** sono stati erogati interventi di security awareness finalizzati ad aumentare il livello di consapevolezza dei dipendenti di tutto il Gruppo (oltre 90.000 dipendenti in 108 Legal Entities) su svariati aspetti di cyber security; Accenture ha implementato e gestito una specifica Security Academy predisponendo contenuti formativi specifici e definendo metriche specifiche di misurazione dei risultati che hanno evidenziato come circa il 98% degli utenti hanno completato il percorso formativo nei tempi predefiniti. ✓Presso un **primario operatore in ambito Payments** sono stati erogati interventi formativi predisponendo materiale dedicato quali brochure, screensaver, newsletter, ecc.; l'intervento ha coinvolto circa 1.300 dipendenti e ha portato a una riduzione del tasso di esecuzione di operazioni malevole dal 42% al 26%. ✓Presso **un'associazione di categoria di imprese italiane** è stata condotta una campagna di alfabetizzazione alla sicurezza informatica, volta a fornire ai propri dipendenti un set di conoscenze utili a prevenire, tramite adeguata consapevolezza, incidenti di sicurezza che avrebbero potuto mettere a rischio la sicurezza dei dati trattati, alcuni anche particolari, in ottica GDPR; il successo dell'iniziativa è testimoniato dalla progressiva estensione dell'intervento ad un parco utenti sempre più esteso, sia di natura IT che non IT.

In aggiunta Accenture eroga servizi di Security Awareness tramite **interventi diretti nelle Università italiane** al fine di promuovere la diffusione della cultura di sicurezza, oltre che tramite la partecipazione a Osservatori e Centri di Ricerca nazionali e istituzionali. Lo stesso avviene nell'ambito di eventi specifici dedicati alla community di cybersecurity aperti al pubblico o per specifici Clienti. Si evidenzia inoltre: ✓**Accenture Cybergame** organizzato in diverse sedi, tra cui il Cybertech Europe, uno degli eventi più importanti in ambito cyber security e che, tramite l'adozione di modalità interattive e di gaming, ha consentito a studenti/ricercatori di sfidarsi tentando di violare i sistemi di un'ipotetica azienda e ricevendo supporto/formazione da parte degli esperti di Accenture ✓la **CISO Academy**, un evento formativo specificamente dedicato ai CISO delle più grandi aziende mondiali al fine di discutere le modalità di sviluppo delle soluzioni di cyber security e condividere ambiti di miglioramento anche tramite sessioni di design thinking specifiche.

14.3 Proposte innovative - Canali e strumenti

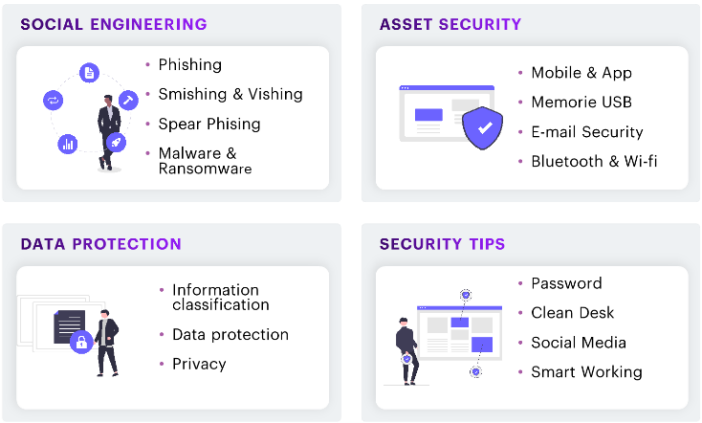
- Erogheremo i servizi di awareness utilizzando canali e strumenti che saranno studiati specificamente per rispondere alle esigenze dei singoli utenti e che saranno definite in funzione di: ✓**rischi di sicurezza** indotti da ruolo/mansione ricoperti e dagli strumenti informatici utilizzati ✓**livello di conoscenza** di partenza verificato tramite test di valutazione ✓**disponibilità di tempo e strumenti** per accedere ai servizi di awareness. Tra i canali e gli strumenti che si intende utilizzare si evidenziano: ✓**Training online**: corsi di formazione basati sul web, di alta qualità e con un design reattivo. Offrono ai discenti l'opportunità di comprendere i principali argomenti relativi alla sicurezza informatica in un brevissimo lasso di tempo utilizzando esempi pratici. Gli elementi interattivi trasformano il corso in una vera esperienza per il discente e forniscono quindi un modo efficiente per custodire i messaggi chiave rilevanti; ✓**Corsi in aula**: sessioni dedicate a specifici gruppi di utenti su tematiche

predefinite o studiate ad hoc rispetto alle esigenze delle PA erogate da personale specializzato su tematiche di cyber security; ✓**Newsletter e E-Card**: invio di messaggi puntali tramite newsletter o eCard per condividere informazioni e aggiornamenti in modo rapido e conciso a molte persone, garantendo una diffusione efficace delle informazioni senza un sovraccarico delle stesse; ✓**Webinar**: lezioni da remoto di esperti riconosciuti. A seconda del livello di dettaglio e dell'argomento desiderato, la gamma di possibili relatori spazia da specialisti IT a criminologi, giornalisti e autori accademici. Da brevi discorsi di apertura a presentazioni dettagliate: il tipo e l'ambito della lezione possono essere organizzati individualmente; ✓**Flyer e brochure**: vasta gamma di prodotti stampati relativi alla sicurezza informatica. Ogni prodotto è pensato per un target specifico e si distingue per il suo design unico. Sono un formato accessibile per presentare in modo conciso argomenti complessi in modo che possano essere visualizzati a colpo d'occhio; ✓**Quiz**: gli argomenti sulla sicurezza informatica sono ottimi contenuti per i quiz. Un quiz combina un'attività interattiva e informazioni in un formato perfetto sia per testare che per aggiornare le conoscenze esistenti sulla gestione sicura dei dati digitali; ✓**Campagne di simulazioni**: le simulazioni vanno oltre il puro contenuto di apprendimento, sono dimostrazioni realistiche, come l'invio di e-mail sospette, che possono essere utilizzate per evidenziare l'importanza di essere cauti con le e-mail e, in generale, aumentare la consapevolezza dei discenti; ✓**Podcast**: i podcast sono un modo ideale per trasmettere regolarmente brevi informazioni in un formato stimolante e compatto, soprattutto per contenuti a lungo termine. I discenti possono essere informati a lungo termine attraverso discussioni con esperti ed esperienze reali sui temi della sicurezza informatica; ✓**Consigli del giorno**: il formato "consigli del giorno" offre l'opportunità di fornire ai discenti consigli utili sulla sicurezza informatica. Brevi consigli, domande o inviti all'autoriflessione posti all'interno di questo formato aiutano ad aggiornare e consolidare le proprie conoscenze e a renderne più facile l'attuazione; ✓**Ebook periodici** su aspetti di cyber security per tutti i dipendenti da inviare tramite mail; forniscono strumenti utili, suggerimenti pratici e tutto quello che è necessario sapere per proteggere i dispositivi e i dati personali degli utenti quando connessi in rete. Il gradimento dei discenti su canali e strumenti sarà raccolto tramite questionari somministrati su **LimeSurvey** (cfr. indicatore IQA_SUTR, §14.5).

14.4 La piattaforma di formazione

Al fine di indirizzare le esigenze delle Amministrazioni, rendiamo disponibile la piattaforma di e-learning **"Accenture Security Training"** sviluppata negli anni anche sulla base dell'esperienza interna di utilizzo dei moduli Hackerland, installata presso il Centro Servizi e aggiornata di continuo in termini di contenuti informativi. Gli utenti potranno accedere tramite il Portale della fornitura che gestirà i processi di accesso e autenticazione in modalità sicura e reindirizzerà direttamente gli utenti sulla piattaforma target. La piattaforma prevede una struttura modulare che include: ✓**Sezione di Awareness**. Un innovativo sistema integrato di e-Learning che consente di coinvolgere tutta l'organizzazione in un percorso di apprendimento che sia al contempo educativo e stimolante; ✓**Sezione Phishing**. Un innovativo sistema di e-training, in funzione AntiPhishing, che produce risultati efficaci grazie alla sua metodologia di training on the job e alle caratteristiche di automazione e ML; ✓**Sezione Informativa**. Un percorso di formazione video basato su una metodologia induttiva e realizzato con tecniche di produzione avanzata e con uno storytelling particolarmente coinvolgente. All'interno di questa sezione sono collocati i moduli Hackerland.

La **Sezione di Awareness** è progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, con un approccio a rilascio costante e graduale: ✓la formazione impegna il partecipante per pochi minuti a settimana, con un percorso che ne mantiene elevata l'attenzione ✓tutte le lezioni sono disponibili in formato multimediale, con la possibilità di fruire dei contenuti sia in formato video sia in formato testo ✓il linguaggio divulgativo è pensato per poter essere fruito dal personale non specializzato nella Cyber Security ✓ogni lezione è corredata da test di valutazione del livello di apprendimento ✓la metodologia di Gamification, corredata da premi e riconoscimenti, stimola l'apprendimento e premia l'eccellenza ✓l'organizzazione in team consente di attivare competizioni virtuose e coinvolgenti tra team diversi ✓le funzioni di Student Caring automatiche, attraverso sollecitazioni e reminder ad hoc, motivano la partecipazione ✓ogni modulo formativo è auto-consistente perché affronta uno specifico argomento critico ✓ogni modulo è disponibile multilingua.



In figura alcuni dei contenuti, che tengono conto dell'analisi svolta relativamente al corso reso disponibile dall'AgID e ai relativi contenuti affrontati, resi disponibili sulla piattaforma che saranno progressivamente aggiornati nel tempo, per poterli adattare alle esigenze delle PA e al contesto dinamico delle minacce di sicurezza.

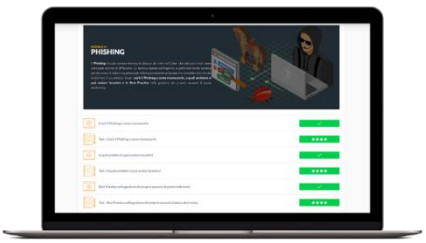
La **Sezione Phishing** è focalizzata su quello che si conferma essere il principale punto di vulnerabilità delle organizzazioni pubbliche e private. Il programma di esercitazione si basa sull'apprendimento esperienziale. L'utente viene sottoposto con frequenza variabile, ma con continuità, ad attacchi simulati che tendenzialmente sono destinati a diventare sempre più complessi e sfidanti.

Il modulo segue un processo adattivo per modellare le campagne di simulazione, con lo scopo di aumentare l'efficacia dell'esercitazione, riproducendo l'esperienza reale dell'utente e le strategie di attacco adottate dai criminali Cyber. Le simulazioni vengono specializzate automaticamente sulla base del profilo comportamentale dell'utente, seguendo la logica del "personal training", con una metodologia che sottopone l'utente a un programma di esercitazione che tiene conto della capacità dell'individuo di resistere agli attacchi. Ogni volta che l'utente fallirà la simulazione, attivando l'azione ingannevole verrà esposto direttamente a un intervento formativo di Awareness, intervento che fornirà dettagli sulla tipologia di attacco subito.

È prevista una specifica funzionalità di reportistica, fruibile attraverso una **dashboard**, che consente, grazie a metriche avanzate, di valutare il rischio e di seguire la sua concreta riduzione durante l'avanzare del programma.

La **Sezione Informativa** è composta da una serie di video focalizzati sulle principali minacce Cyber e su come queste possono concretamente colpire individui e

organizzazioni. I contenuti sono arricchiti di tutte le componenti di access control, engagement e monitoring proprie della piattaforma e sono raccontati con stili diversi, da quello cyber-investigativo a quello cyber-news, per renderlo ancora più attrattivo e ingaggiante.

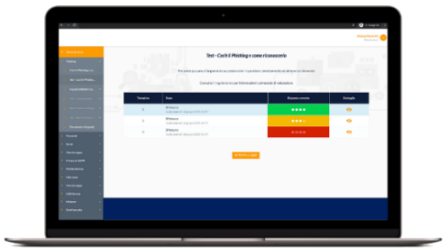


La piattaforma sarà resa disponibile secondo 2 percorsi, definiti **base** e **avanzato**, così da indirizzare l'esigenza di cluster differenti. Il percorso base include un subset di contenuti per ciascun modulo ed è destinato agli utenti che hanno minori necessità formative in ambito cyber security, mentre il percorso avanzato include tutti i contenuti resi disponibili.

Nello specifico il percorso base include 4 contenuti del modulo di Awareness, 4 video del modulo informativo e 4 attacchi simulati per il modulo di phishing. Il percorso avanzato include invece 36 contenuti del modulo di Awareness (erogati agli intervalli che si ritiene di definire), 6 video del modulo informativo e non prevede un limite di attacchi simulati, così da garantire un percorso modulare basato sul profilo comportamentale del singolo utente. In fase di attivazione del servizio, si procederà con l'Amministrazione richiedente ad articolare le modalità di accesso ai 2 percorsi e a valutare la necessità di attivare anche una o più lezioni in aula con specialisti di sicurezza su specifiche tematiche.

14.5 Tecniche innovative di verifica dei livelli di awareness raggiunti

All'interno delle attività previste sono incluse quelle finalizzate alla raccolta degli esiti di ciascuna iniziativa aventi lo scopo di monitorare l'andamento del programma di awareness e di verificare i risultati raggiunti ed il livello di sensibilizzazione degli utenti. Sono previste differenti modalità per le attività di verifica e sensibilizzazione volte a garantire: ✓Un monitoraggio costante durante il rilascio delle iniziative previste per garantire che tali iniziative siano sempre efficaci e che eventuali lesson learnt possano essere sfruttate per le iniziative non ancora lanciate ✓La misurazione del livello di consapevolezza che i discenti hanno raggiunto partecipando ad ogni singola iniziativa ✓La misurazione del livello di consapevolezza che i target hanno raggiunto partecipando al programma di Security Awareness nel suo complesso, attraverso un innovativo sistema di e-training, con una funzione Anti-Phishing e Anti-Smishing, che produce risultati efficaci grazie alla sua metodologia di training on the job e alle sue caratteristiche di automazione e adattività con l'ausilio di AI ✓La misurazione del livello di consapevolezza che l'Amministrazione ha raggiunto partecipando al programma di Security Awareness ✓Un costante coinvolgimento dei target che devono essere raggiunti dalle iniziative previste dal programma di Security Awareness.



Le componenti della piattaforma per la verifica delle conoscenze acquisite dall'utente e dell'effettiva capacità di mettere in atto quanto appreso, sono: ✓**Quiz** (verifica di tipo formale, attraverso test di verifica relativi agli argomenti delle singole lezioni): ✓Ogni lezione è corredata da test di valutazione del livello di apprendimento; ✓Trimestralmente è proposta agli utenti una verifica intermedia dell'apprendimento che ha il duplice scopo di verificare le conoscenze apprese e consolidare le nozioni apprese fino a quel momento. ✓**Campagna di phishing** (verifica di tipo esperienziale, attraverso "verifiche sul campo" della capacità di reazione dell'utente alla minaccia cyber attraverso un simulatore di campagne di Phishing e Smishing): ✓Le simulazioni sono gestite attraverso un sistema di AI, per essere automaticamente modulate sulla base del profilo comportamentale del singolo utente e della sua capacità di resistere agli attacchi ✓Le simulazioni sono organizzate, come impostazione predefinita, a cadenza mensile, tale cadenza può essere modificata e personalizzata in base alle esigenze dell'azienda ✓Ogni volta che l'utente fallirà la simulazione, verrà indirizzato direttamente ad un intervento formativo di Awareness con dettagli sulla tipologia di attacco subito.

In aggiunta, attraverso la funzionalità di recupero del debito formativo, il sistema individua gruppi di utenti la cui curva di apprendimento è inferiore alla media aziendale e suggerisce attività di training / verifica esperienziale al fine di recuperare il gap comportamentale, in termini di Cyber Strenght.

La piattaforma offre, inoltre, un'efficace reportistica, in grado di soddisfare le esigenze di tutte le figure professionali coinvolte nelle attività di verifica e i ruoli specifici che sono coinvolti nei programmi formativi e addestrativi, quale: ✓**Reportistica per gli utenti**, che fornisce una fotografia chiara dell'andamento del percorso individuale, fornendo anche un metro di paragone altrettanto chiaro con il resto dell'azienda. Di particolare impatto la reportistica relativa alle funzioni di gamification, con l'esposizione delle classifiche. ✓**Reportistica** per **i supervisori**, con l'analisi aggregata e di dettaglio di numerosi KPI di partecipazione e con l'esposizione degli indicatori relativi alla gamification "a squadre"; reportistica facilmente esportabile ai fini della comunicazione interna. ✓**Reportistica per le risorse** umane, con indicatori di partecipazione tracciati al livello massimo di dettaglio (lezione/utente). ✓**Reportistica dedicata alla** competizione **"a squadre"**, con la possibilità di identificare la figura del "team leader", in grado di agire da motivatore della propria squadra, anche grazie ad una serie di tool a supporto della funzione. ✓**Reportistica specifica delle "**verifiche **sul campo"** (Phishing e Smishing), di particolare interesse anche per le funzioni di Cyber Security, con analisi aggregata e di dettaglio, non solo dei dati relativi al click-rate, ma anche ad una serie di indicatori di rischio particolarmente sofisticati, in grado di diventare supporto indispensabile ad eventuali azioni di remediation. ✓**Un report**, creato automaticamente **in formato presentazione**, che consente di comunicare i risultati degli interventi **ai livelli direzionali**.

Infine, nel contesto delle categorie degli indicatori da monitorare specificate al §6.3.4, si illustrano gli indicatori di qualità previsti per il servizio in oggetto.

INDICATORI DI MONITORAGGIO DELLA QUALITÀ DEL SERVIZIO "FORMAZIONE E SECURITY AWARENESS"				
Codice	**Descrizione**	**Formula**	**Periodo**	**Soglia**
IQA_SUTR	Soddisfazione utenti training valutata tramite questionario somministrato ai discenti e-learning	% di risposte "Soddisfatto" / risposte complessive	Trimestre	SUTR>80%
PCI_SLCS	Come SLCS	Come SLCS ma frequenza maggiore e soglia più bassa	Mensile	PCI_SLCS =1
KPI_FTAP	Fallimento test anti-phishing	% di soggetti che hanno fallito il test anti-phishing per ciascuna campagna	Evento	Riduzione rispetto misura precedente

15 PRESENZA DI ULTERIORI FUNZIONALITÀ AGGIUNTIVE

Il Raggruppamento conferma la presenza contemporanea delle seguenti funzionalità aggiuntive: ✓Servizio "Next Generation Firewall": funzioni di "Geo-IP filtering e Geo-Blocking" per consentire la creazione di regole di policy da applicare a specifici paesi e/o regioni geografiche; ✓Servizio "Gestione continua delle vulnerabilità di sicurezza": raccolta ed utilizzo delle informazioni secondo profili di utenza diversi, tramite un'interfaccia grafica oppure tramite API; ✓Servizio "Threat Intelligence e Vulnerability Data feed": utilizzo dei formati STIX/TAXII per l'integrazione con il sistema SIEM.

16 PORTALE DELLA FORNITURA

Principale strumento a supporto dei processi di interazione e comunicazione è il **Portale della Fornitura**, punto di accesso alle informazioni e ai repository sull'AQ e agli strumenti di gestione e di erogazione dei servizi da parte di tutti gli stakeholder, secondo vari livelli di abilitazione. Il suo disegno è frutto dell'esperienza di successo che le aziende dell'RTI hanno accumulato sui portali di fornitura (es. Accenture nel CQ Sistemi Gestionali Integrati e negli AQ Digital Transformation e Servizi Applicativi Cloud nonché Fastweb nel CQ SPC Cloud L2), dalla quale traiamo spunto per alimentare una costante evoluzione di funzionalità erogate e tecnologie sottostanti. Il Portale rappresenta sia la vetrina sui servizi in essere e uno strumento di collaborazione e condivisione delle esperienze tra le PA sia lo strumento di gestione dell'AQ; è realizzato con una **soluzione robusta e rapidamente adattabile** a ogni esigenza, grazie a molti strumenti **nativamente integrati** che abilitano gli stakeholder all'uso di numerose funzioni di collaborazione. Lo strumento integra: ✓un front-end pubblico realizzato su tecnologia open source Drupal ✓un back-end basato su prodotti MS Office365 e funzionalità realizzate ad-hoc ✓piattaforme di monitoraggio (Power BI) per l'analisi dell'utilizzo del portale e degli indicatori di sintesi dei contratti ✓funzionalità di knowledge management supportate da algoritmi di AI. Particolare importanza è data agli aspetti di Business Intelligence ad uso sia delle singole PA ma soprattutto di Consip e degli Organismi di Controllo; le funzioni di monitoraggio implementate permettono dunque di avere una vista su tutti gli aspetti di performance relativi all'AQ.

In particolare, attraverso l'accesso profilato alle singole PA e alla fruibilità multicanale il portale si pone come lo strumento di knowledge sharing abilitante la condivisione tempestiva delle best practice e delle informazioni tra le Amministrazioni.

Il Portale funge da principale punto di accesso grazie alla sua integrazione con le soluzioni adottate per l'esecuzione dei contratti quali, ad esempio, la piattaforma **ServiceNow** (leader nel workflow e knowledge management, cfr. §4), le componenti ITSM, PPM, Performance Analytics e SLA Management. La massima integrazione tra gli strumenti di governo della fornitura e le soluzioni tecnologiche utilizzate per l'erogazione dei contratti di fornitura è abilitata da uno strato di API, realizzate in formato standard SOAP e REST seguendo le indicazioni di AgID. ServiceNow mette a disposizione anche una innovativa soluzione di **knowledge management** basata sull'impiego di un datalake di fornitura che consentirà di implementare la knowledge base, fruibile da tutte le risorse del RTI e delle Amministrazioni secondo modalità innovative (es. ricerche in linguaggio naturale) e sulla quale si potranno effettuare attività di correlazione dati/ML producendo razionali/report a supporto della successiva erogazione (es. elementi tecnici impiegabili nell'analisi di nuovi contesti o per velocizzare il problem solving nell'ambito della maintenance) o avere accesso ad informazioni particolarmente importanti (es. le lessons learned).

16.1 Soluzioni tecnologiche e funzionalità del Portale di fornitura

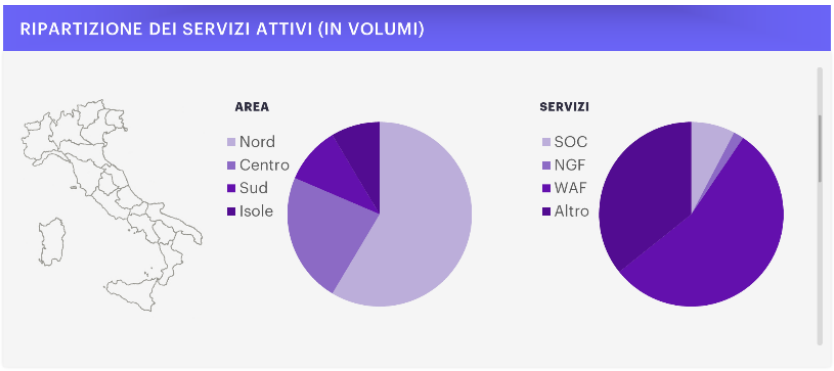
Il Portale della Fornitura è realizzato in modo da essere utilizzabile secondo le indicazioni dell'AgID e nel rispetto delle linee guida di **accessibilità** che garantiscono la fruizione a tutte le categorie di utente. Il progetto di implementazione segue a tale scopo un approccio di **User Center Design** (UCD) e reattivo, grazie alla dinamicità delle soluzioni proposte, e un approccio di **Continuous Improvement** basato sui feedback ricevuti dagli utenti e sulle analisi condotte sui dati di web analytics, questi ultimi raccolti grazie a **Google Analytics** o strumenti analoghi. L'intero Portale è realizzato con interfacce **responsive** per essere fruibile indipendentemente dalla piattaforma utilizzata (desktop, tablet, smartphone). Ulteriore potenziamento dell'esperienza **Mobile** è fornito dalla funzionalità offerte out of the box dall'app mobile Teams che, in quanto integrata con il portale, permette all'utente di accedere alle **funzioni di collaborazione** e di ricevere le notifiche rilevanti anche attraverso lo smartphone. Per assicurare il raggiungimento dei più alti livelli di usabilità, in accordo e in collaborazione con Consip, potranno essere condotti in corso d'opera dei test di usabilità individuando un campione di utenti e utilizzando il **protocollo eGLU LG 2018.1**, citato anche all'interno del **Piano triennale per l'Informatica nella PA 2020–2022**, che permette una semplice e immediata valutazione del portale da parte degli utenti finali e la conseguente individuazione di interventi migliorativi; questo anche grazie all'ampia esperienza maturata in portali compatibili con le linee guida AGID (es. INAIL, MEF). Per la realizzazione del portale prevediamo l'integrazione con il sistema di autenticazione **SPID** (Sistema Pubblico di Identità Digitale), in modo da agevolare l'accesso alle aree post-login da parte degli utenti PA, e l'integrazione con strumenti **Office 365** e funzionalità custom che permettono non solo di coprire tutte le richieste del Capitolato Tecnico ma anche di fornire ulteriori funzioni, nell'ottica di formulare una proposta migliorativa rispetto ai requisiti di base. Il portale, i cui oneri di hosting, gestione e aggiornamento mensile dei contenuti sono a carico del RTI, è supportato da un'attenta configurazione della profilazione degli utenti, al fine di gestire in sicurezza l'accesso alle informazioni presenti. In particolare, l'utente non accreditato naviga l'Area Pubblica a disposizione senza necessità di registrazione, mentre le altre aree del portale sono riservate a utenti profilati che accedono tramite l'inserimento di credenziali appositamente create o grazie all'integrazione con SPID. Gli utenti possono essere appartenenti ai fornitori di servizi, alle PA, agli **Organismi di coordinamento e controllo** o a terze strutture appositamente indicate. La soluzione può contare su un alto livello di sicurezza applicativa, in parte garantito direttamente dalla tipologia delle licenze che saranno utilizzate. Si elencano di seguito alcune peculiarità: ✓**abilitazione del**

doppio fattore di autenticazione, particolarmente utile per le utenze amministrative e con ampi permessi (es. utenze dedicate agli organismi controllori); accesso condizionale basato su dispositivo per bloccare o limitare l'accesso su dispositivi non gestiti; criteri per disconnettere gli utenti dalle sessioni dopo un periodo di inattività ✓**prevenzione perdita dei dati** su più livelli, quali: criteri per identificare i documenti e impedirne la condivisione; Limite alla sincronizzazione dei dispositivi in domini specificati ✓**crittografia** per l'utilizzo di **Microsoft Teams** e SharePoint Online, mantenendo al sicuro la messaggistica istantanea, riunioni e siti dei team. È consentito solo l'accesso sicuro. Non verranno effettuate connessioni autenticate tramite HTTP, ma verranno invece reindirizzate a HTTPS. I dati sono crittografati a livello di disco usando la crittografia BitLocker e a livello di file tramite chiavi. ✓ **La rete Yammer è privata**. Solo gli utenti con un indirizzo di posta elettronica valido e verificato possono accedere a Yammer, social network di Enterprise con sicurezza integrata a tutti i livelli. Yammer è conforme al livello C nel framework di conformità di Office 365, che soddisfa le clausole del modello SOC 1, SOC 2 e ISO 27001.

Per maggiori dettagli sulla strutturazione delle aree del Portale, le relative funzionalità e modalità di interazione con le Amministrazioni si invita alla consultazione del §16.2 Soluzioni e/o processi e/o strumenti di comunicazione e di collaborazione in chiave "social" con le Amministrazioni.

16.1.1 Strumenti di analisi dei dati e reporting

Tutte le funzionalità di reportistica sono progettate grazie al framework **Accenture Data Driven**: una tecnica di gestione e visualizzazione dei dati volta ad acquisire Data Fluency, vale a dire la capacità di leggere i dati e trarne **insights a supporto delle decisioni**. Proponiamo l'utilizzo di **Power BI** per tutti gli aspetti legati alla reportistica, in particolare nelle aree **Collaborazione e Monitoraggio** e **Osservatori**. Lo strumento, tramite **report statici e dinamici**, offre agli Organismi di Coordinamento e alle PA la possibilità di effettuare analisi multidimensionali su tutti i parametri espressi all'interno del Capitolato: ✓dati di qualità e sicurezza; >customer satisfaction misurata con la soluzione **LimeSurvey** ✓livelli di servizio e indicatori di qualità e di digitalizzazione ✓valori economici dei Servizi sottoscritti. Particolare attenzione è rivolta alla realizzazione dei cruscotti di monitoraggio relativi ai Piani dei Fabbisogni, Piani Operativi e Servizi in Esecuzione. In accordo con Consip, report statici relativi **ad avanzamenti** delle iniziative contrattuali, **numerosità delle iniziative** attive e concluse, **indicatori di digitalizzazione**, potranno essere resi disponibili nelle aree Comunicazione (area pubblica) e Informativa. In generale, sono **offerte** agli utenti del portale funzioni per ✓ricevere **periodicamente** versioni aggiornate di uno o più report nella propria casella e-mail ed ✓essere informati della disponibilità di **nuove versioni dei report** (WhatsApp, Telegram), anche senza accedere alla piattaforma.



Sono messi a disposizione report che monitorano l'andamento generale dell'AQ tramite parametri quali: ✓numero dei **Piani di Fabbisogni** realizzati con il dettaglio del loro stato (numero Servizi associati, percentuale Servizi completati/attivi, budget consumato) e con drill down sul dettaglio dei Servizi associati ✓andamento e stato dei **Piani Operativi** ✓**numero e volumi di Servizi**, con drill down sulla distribuzione territoriale e per tipologia di PA ✓numero dei **servizi/interventi** con il dettaglio del loro stato di avanzamento e del budget assegnato, consumato e residuo.

MS Power BI è totalmente integrato con **MS Excel**: è pertanto facile effettuare degli export sia in formato Excel che nei formati più comuni (es. csv, json, xls etc.). Il meccanismo permette di salvare periodicamente e in maniera automatica un determinato set di report all'interno della piattaforma SharePoint online, dove resterà disponibile per i diversi stakeholder.

16.2 Soluzioni e/o processi e/o strumenti di comunicazione e di collaborazione in chiave "social" con le Amministrazioni

Tra gli obietti del Portale della Fornitura c'è quello di favorire la collaborazione e la comunicazione tra le varie PA che partecipano all'AQ: in questo modo le soluzioni implementate presso un'amministrazione possono essere condivise e riutilizzate dalle altre PA. Il portale prevede l'implementazione di funzioni abilitanti per la collaborazione tra le PA tramite l'utilizzo di **MS Teams** e **MS Yammer**, opportunamente integrati nel Portale della Fornitura. Gli utenti hanno quindi la possibilità di creare ambienti virtuali di collaborazione, gruppi di lavoro, organizzare riunioni e web conference. L'efficacia e la potenza di questi strumenti di **Digital Workplace** trova conferma nella capacità del RTI di garantire il funzionamento senza soluzione di continuità di sistemi strategici nazionali. Un ruolo fondamentale viene svolto dall'Area **Collaborazione e Monitoraggio**, all'interno della quale la componente **Yammer** permette di creare un vero e proprio **Entreprise Social Network** in grado di favorire la condivisione delle esperienze e del know how in modalità social. Lo streaming social permette alle PA di condividere i propri risultati ma anche di consultare i risultati ottenuti dalle altre PA, con la possibilità di accedere alle informazioni di dettaglio. Grazie all'implementazione di un **motore di raccomandazione**, verranno mostrati dei post generati in automatico che consigliano all'utente di consultare determinati contenuti, quali schede di altre PA che hanno intrapreso percorsi affini, schede di descrizioni di nuove tecnologie/framework/soluzioni, risultati raggiunti da altre PA, condivisi per favorire il knowledge sharing e la collaborazione. Sulla piattaforma sono svolte analisi di **social listening**, volte a trovare e tracciare le conversazioni online attorno a specifiche keyword, frasi ed eventi e attorno allo specifico servizio o alla specifica PA. Ciò permette di ottenere feedback in real-time che aiuteranno a migliorare lo sviluppo dei servizi.

Area Comunicazione

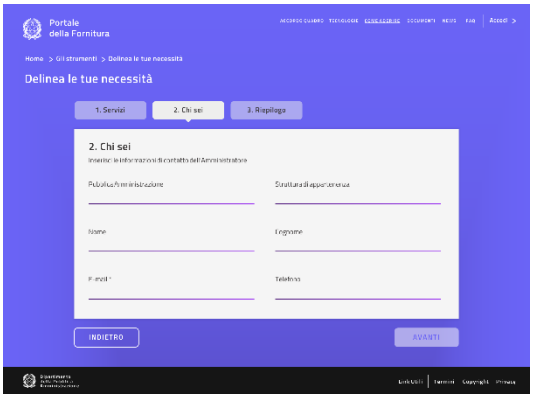
L'area in oggetto, aperta al pubblico, funge da vetrina per tutti i contratti in corso relativi all'AQ con l'obiettivo di esporre in maniera eloquente e completa tutte le informazioni necessarie alle singole PA per comprendere: ✓i vantaggi nell'aderire all'AQ e i benefici derivanti dall'accesso alle best practice e alla reportistica accessibile agli aderenti ✓le modalità di partecipazione. Gli strumenti che la landing page ha a disposizione sono: ✓**contenuti informativi e interattivi** esaustivi in formato testuale, grafico e video ✓**social proof** costituita dalle testimonianze delle PA aderenti raccolte nel corso dell'erogazione ✓**reportistica e documentazione** relativa alle iniziative svolte o in corso ✓strumenti **di simulazione e di contatto avanzati**. In accordo con Consip, è disponibile già in questa sezione il **Pre-Configuratore del piano dei fabbisogni,** ovvero lo strumento che permette alla PA di creare una prima versione del piano dei fabbisogni in modo semplice e intuitivo - attraverso una **user experience** mutuata dalle best practice dell'interazione dei portali e-commerce. La base dati del portale è costantemente aggiornata (tecnologie, trend, framework, procedure, ecc.) nel tempo. Al termine del processo, l'utente è invitato a eseguire il primo step per la registrazione al portale, propedeutico per l'adesione all'AQ, verificando l'utenza prima di procedere agli ulteriori step e dare i permessi di navigazione relativi. Per seguire l'andamento dell'AQ, nella parte bassa della pagina sono predisposti i canali Telegram, tramite iscrizione, mailing list e notifiche tramite WhatsApp, previo consenso a ricevere i contenuti.

L'utente PA dispone inoltre di **strumenti automatici per la richiesta di informazioni**: ✓**Assistente Virtuale**, addestrato per rispondere a tutti i quesiti relativi al funzionamento e alle modalità di adesione all'AQ formulati in linguaggio naturale, per apprendere e migliorare la capacità di risposta durante le interazioni ✓**FAQ** costantemente aggiornate per ricevere assistenza personalizzata: ✓**WhatsApp**, con un numero dedicato monitorato da un bot ✓**form** per richiedere di essere contattato ✓pagina social.

L'area Comunicazione, inoltre, costituisce lo strumento di promozione proattiva delle iniziative e dei servizi relativi all'AQ. I contenuti vengono constantemente aggiornati anche in base all'esperienza maturata dalle PPAA che già usufruiscono degli stessi, in modo tale da facilitarne la condivisione e la divulgazione. A tal proposito, i contenuti promozionali possono essere condivisi tramite l'utilizzo delle **funzionalità di social sharing integrate nel portale.** Ciò consente sia di aumentare la visibilità dei contenuti del portale verso una platea estesa, sia di **recepire e stimolare,** al suo interno, **le discussioni che nascono sui social sui contenuti condivisi**.

Area Informativa

Con le informazioni e gli strumenti che guidano concretamente la PA nell'aderire all'AQ, costituisce l'area di supporto e comunicazione di dettaglio riservata alle PA. In particolare, in una sotto-area dedicata la PA ha accesso a tutta la documentazione di riferimento per i servizi offerti all'interno dell'AQ, aggiornata e scaricabile, tra cui la guida alla stima e alla misurazione degli effort progettuali con dettagli su servizio/intervento. In un'apposita sottosezione sono inoltre contenute le descrizioni di tutte le soluzioni migliorative che il RTI mette a disposizione, e le pagine all'interno delle quali i modelli operativi sono resi in forma grafica, con spiegazioni di dettaglio a supporto; in questo modo viene fornita una chiara descrizione sulle caratteristiche specifiche, per indirizzare la scelta su un modello operativo piuttosto che un altro. Da quest'area è infine possibile accedere al **Configuratore del piano dei fabbisogni,** che costituisce lo strumento che il RTI mette a disposizione delle PA per supportarle nel delineare le proprie esigenze, con l'obiettivo finale di rendere l'adesione all'AQ il più efficace possibile. Il Configuratore guida l'utente attraverso tre passi: ✓il **primo** step prevede una serie predefinita di domande volte a delineare il contesto all'interno del quale la PA opera, identificare e quantificare le esigenze sulle quali si baserà il piano dei fabbisogni con il duplice obiettivo di tracciare le caratteristiche specifiche della PA e di definire una prima profilazione utile sia per il secondo step, sia per le funzioni implementate nelle altre sezioni del portale ✓il **secondo** step, grazie al supporto di un **motore di raccomandazione** e sulla base di un database all'interno del quale sono raccolte le esperienze delle altre PA e i dati di benchmark di mercato, guida l'utente in una serie di scelte che configurano ulteriormente la sua richiesta consigliando tecnologie, soluzioni, framework e altre specifiche ✓il **terzo** step permette di scaricare una prima versione del piano dei fabbisogni, salvata nella propria area personale e che costituisce il punto di inizio del processo di adesione all'AQ poiché, contestualmente o in qualsiasi altro momento, è possibile inviare il piano generato in modo da organizzare la consulenza di supporto con lo scopo di delineare definitivamente le esigenze. Quest'ultima fase viene abilitata dall'utilizzo di **riunioni online e strumenti di collaborazione** che permettono il confronto real time per perfezionare il piano condiviso.



A supporto del processo di individuazione e configurazione dei fabbisogni interviene la componente **Yammer** che favorisce la socializzazione delle esigenze e delle esperienze pregresse, sulla quale si innesta sia il dialogo diretto con **i** consulenti esperti dei bisogni della specifica PA e in grado di anticiparne le necessità, sia la shared knowledge, che si fonda sulla condivisione delle esperienze/deliverable. Gli esperti dell'AQ HUB ✓verificano con i Responsabili Tecnici dei servizi i deliverable e li rendono disponibili nel Portale debitamente sanitizzati ✓promuovono storytelling da parte dei protagonisti dei CE per sviluppare "forme di riconoscimento" in PA analoghe ✓inseriscono i contenuti all'interno di Yammer per favorire la discussione e la condivisione tra le PA.

Area Project Management

In quest'Area, ad accesso riservato e profilato, un PA può attivare, monitorare e gestire i contratti e i servizi/interventi affidati. Accedendo all'area Project Management, l'utente abilitato della PA inizia la navigazione con la selezione del Contratto di interesse, sia attivo che chiuso. La prima sezione nella parte superiore della pagina riguarda i **servizi in evidenza** che possono richiedere l'attenzione dell'utente per: recente cambio di stato, intervento di attivazione/approvazione richiesto, alert su indicatori di qualità, aggiunta di una nuova issue, superamento delle scadenze, ecc. L'utente ha quindi la possibilità di selezionare uno dei servizi per verificarne lo stato, entrando nella pagina specifica del servizio. Tale sezione incorpora le funzionalità di workflow per il ciclo di vita documentale (elaborazione documenti, approvazioni, review e modifiche tramite strumenti di collaboration). In particolare:

- **Funzionalità di validazione dei documenti e di approvazione da parte dell'Amministrazione**: L'approvazione di un documento si delinea come un processo fatto di diversi step, ognuno dei quali coinvolge determinati attori, che devono effettuare specifici controlli e decidere se il documento può procedere al prossimo step del flusso. L'utente abilitato della PA inizia la navigazione con la selezione del Contratto di interesse, all'interno del quale è presente la sezione dedicata alla gestione documentale e relativa archiviazione. È possibile generare/caricare a sistema differenti tipologie di documento, il cui **flusso approvativo** è preventivamente definito con l'individuazione dei "poteri di firma" sia lato PA sia lato RTI (Il ciclo di vita dei documenti ufficiali è definito nel Piano della Qualità Generale e verificabile nella Prima Release del Portale) e che saranno implementati a sistema tramite gestione della profilazione delle utenze, facendo ricorso ove necessario, a SPID e/o alla firma elettronica qualificata. La configurazione avviene attraverso lo strumento di **Workflow grafico**, completamente configurabile. I processi approvativi possono essere gestiti in modo centralizzato, tramite applicazione desktop o client web. Lo **stato di avanzamento** può essere mantenuto sotto controllo grazie ad un cruscotto: per ogni documento è possibile visualizzare a quale punto del flusso di approvazione si è arrivati, quali azioni sono state svolte da ogni utente e quando. In caso di necessità, inoltre, vi è la possibilità di delegare l'approvazione di un documento ad un altro collega abilitato.

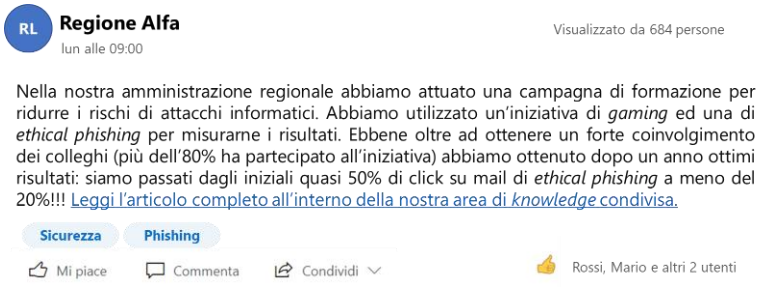
Ogni documento è classificato per tipologia, contraddistinto da un **codice identificativo univoco**, ne viene tracciato il versioning e lo storico dei cambi di stato, ivi incluso lo step approvativo. Lo scambio del documento tra i vari utenti è sempre tracciato in real time e le diverse versioni sono sempre disponibili, senza il rischio che qualcun altro lavori sul documento prima che l'utente incaricato della fase precedente abbia terminato il proprio task o ricevuto l'approvazione di quanto inserito. Inoltre, ogni utente riceve una **notifica** nel momento in cui è richiesto qualche tipo di approvazione.

- **Esecuzione del contratto esecutivo**: fase operativa in cui sono erogati i servizi: ✓il Team di PMO coordina le attività di Project/Program Management e di Risk Management ✓i Responsabili Tecnici dei Servizi coordinano le attività richieste. Al suo interno è presente la funzionalità di pianificazione e gestione, in particolare quella per richiedere l'Estensione dell'orario di servizio: l'utente abilitato della PA inizia la navigazione con la selezione del Contratto di interesse, all'interno del quale è presente la sezione dedicata alla gestione delle richieste di estensione dell'orario di servizio. In tale sezione è possibile inserire la richiesta, dettagliandone le nuove tempistiche/esigenze, con possibilità di aggiungere note esplicative o di supporto. Tale richiesta, che può essere effettuata anche via posta elettronica ad apposito indirizzo dedicato, genererà un "documento di richiesta", visualizzabile ed approvabile nella sezione dedicata alla validazione dei documenti.

- **Funzionalità di accesso ai CV**: il RTI pubblicherà i CV delle risorse proposte, compresi i Referenti tecnici e i ruoli aggiuntivi offerti. L'utente abilitato della PA potrà visionare i CV che saranno resi disponibili secondo i vincoli temporali previsti da bando di gara, con la possibilità di procedere con la richiesta di colloquio, approvare la risorsa o ritenerla non idonea, nel caso in cui seguirà sostituzione e nuovo colloquio.

Area Monitoraggio e Collaborazione

L'area ha un duplice obiettivo: 1) fornire una visione d'insieme sull'andamento dell'AQ mostrando dati relativi a tutte le iniziative intraprese dalle PA aderenti, elaborati attraverso strumenti di analisi dei dati e reporting; 2) favorire lo scambio di esperienze e informazioni tra le PA, per confrontare i risultati ottenuti e condividere il know how acquisito, attraverso le soluzioni e gli strumenti di collaboration messi a disposizione dal Portale. Le attività in esecuzione sono monitorate al fine di individuare criticità, attivare contromisure opportune e rendicontare ai Referenti della PA l'andamento dei servizi. Le PA, nella configurazione ed esecuzione di un servizio, generano nuove esperienze e nuove conoscenze che vanno a costituire parte della loro proprietà intellettuale. Le **funzionalità di Yammer aiutano a consolidare e capitalizzare tali esperienze**, a favore del miglioramento continuo dei servizi. Qualsiasi dubbio durante la routine lavorativa può essere risolto in pochi click in quanto le risposte arriveranno direttamente dalle persone più competenti. Crea un canale di formazione informale: possono essere creati canali di interesse sui quali è possibile caricare le risorse utili per affrontare tematiche ricorrenti, per accedervi ogni qualvolta è necessario, da qualsiasi dispositivo. Le comunità sono un modo potente per consentire agli utenti di condividere approfondimenti e domande. I feed delle chat vengono creati ad hoc per ogni utente sulla base dell'utilizzo dell'AI per evidenziare gli argomenti più critici, le personalizzazioni dell'interfaccia in base al servizio di interesse, l'organizzazione di discussione ottimizzata e la rapida condivisione dei messaggi tramite l'applicazione mobile.



Area Osservatori

In tale area, messa a disposizione degli **Organismi di coordinamento e controllo,** è possibile consultare la reportistica e i dati relativi agli aspetti di **qualità** dei singoli Contratti Esecutivi. Dal punto di vista dell'analisi dei dati e disponibilità di reportistica, oltre a poter richiedere tramite un'apposita funzione presente in menu l'accesso a tutte le aree del portale, hanno infatti a disposizione una Homepage specificatamente realizzata che permette, in modo semplificato, l'accesso alle funzioni di cui necessitano. In particolare, **nella parte superiore della pagina,** trova posto la casella di ricerca che permette di individuare i servizi o le amministrazioni a seconda delle esigenze. All'interno della Homepage, nella parte superiore, vengono riepilogati i servizi sui quali sono state rilevate delle criticità nei parametri

di monitoraggio: tramite questa vista, l'utente può accedere direttamente alla scheda di dettaglio del servizio e rilevare le eventuali problematiche in corso. A seguire è presente una sezione di reportistica, che anticipa in maniera aggregata i dati relativi a tutti i Contratti, eseguiti e in esecuzione, all'interno dell'AQ e infine, nella parte sottostante, vengono elencate le amministrazioni e i progetti afferenti all'AQ in modo da permettere un rapido accesso alle schermate di dettaglio.

17 INNOVAZIONE

La attività svolta dal RTI nell'**identificazione di attori chiave per l'innovazione**, porta allo sviluppo di relazioni con realtà emergenti da acquisire e in cui investire per favorirne la crescita e includerne le competenze nella propria offerta di servizi e/o prodotti in un'ottica di miglioramento continuo del processo di innovazione. Forrester ha recentemente classificato Accenture quale leader assoluto per gli "Innovation Consulting Services" ed "Innovation Consulting Service Providers" (Current Offering in the Forrester Wave™: Innovation Consulting Services, Q2 2021), evidenziando soprattutto come il portfolio di servizi di innovazione fornisca una offerta completa ed un processo end-to-end che va dal disegno di strategie di innovazione fino alla prototipizzazione ed al deployment su larga scala di quanto ideato e realizzato. Volano dell'innovazione per il RTI, Accenture e Fastweb fanno della collaborazione con soggetti innovativi e con i principali player tecnologici uno dei pilastri della propria *value proposition* che viene continuamente alimentata dalle costanti interazioni con università e centri di ricerca, oltre che da significativi investimenti in strutture di innovazione interne tra cui i centri di ricerca multidisciplinari, gli Accenture Labs, il network di centri di ricerca e laboratori di sicurezza di Fastweb, i molteplici poli di innovazione tematici e Accenture Ventures, **intera struttura dedicata all'*Open Innovation***: attraverso un rigoroso processo di selezione e affiancamento, le migliori start up entrano nel virtuoso processo di innovazione che consente di portare ai clienti soluzioni nuove ed efficaci a problemi complessi; la struttura opera in 45 paesi, con oltre 35 partner prioritari (cui sono destinati i maggiori investimenti) distribuiti su 10 *innovation segments* di industria tra cui la **cybersecurity** ha un ruolo primario con **oltre 100 startup** in portfolio.

Relativamente a Fastweb, grazie al suo profilo internazionale, ha investito in oltre 70 aziende tecnologiche, di cui numerose in ambito Cyber Security, attraverso la struttura, denominata "Venture Capital", che si compone di numerose collaborazioni nell'ambito del panorama delle start up. In questo quadro di attenzione focalizzata sull'innovazione, e in linea con i modelli che Accenture e le altre aziende del RTI promuovono per favorire la crescita e il coinvolgimento sul mercato di PMI e start-up innovative, si innesta la partecipazione della PMI innovativa **Difesa e Analisi Sistemi** (DEAS) che proponiamo come partner in grado di integrare le specializzazioni presenti nelle sue strutture sul tema della gestione delle vulnerabilità, della *threat intelligence* e della protezione dei sistemi.

17.1 Soggetti coinvolti e le loro principali caratteristiche

DEAS – Difesa E Analisi Sistemi nasce con l'idea di creare in Italia un polo di Cybersecurity e offrire un supporto globale alle Istituzioni e alle grandi imprese italiane. L'obiettivo di DEAS è diventare un modello di riferimento di Ricerca e Sviluppo nel Sistema Paese utilizzando innovative infrastrutture tecnologiche e fornendo soluzioni integrate di AI e servizi di sicurezza conformi ai più alti standard del settore. DEAS si presenta al mercato quale soggetto abilitatore sia per attività di audit centrale idonea alla legge-perimetro 105/2019 (PSNC) e alla compliance richiesta dal Centro di valutazione e certificazione nazionale (CVCN), sia per attività cyber a sostegno delle misure minime AgID, nel rispetto degli standard qualitativi previsti per operatori della PA centrale e locale non incluse nel PSNC. L'apporto di DEAS al RTI è rappresentato non soltanto dalla sua esperienza nella progettazione di soluzioni innovative di IA/ML ed erogazione di servizi di compliance, con percorsi per l'ottimizzazione e l'hardening dei sistemi informativi secondo gli standard AgID, ma soprattutto dalle capacità di sviluppo e implementazione di soluzioni integrate di difesa (Database Security, Endpoint Protection, Vulnerability Assessment, Security Probing) per il rafforzamento delle infrastrutture perimetrali.

Accenture è ad oggi il più grande player italiano in ambito cybersecurity per volumi di business e numero di risorse. Dispone in ambito cybersecurity di una fitta rete di **Cyber Fusion Centers (CFC)**, centri multidisciplinari di ricerca in cui professionisti cyber lavorano per monitorare la sicurezza e prevenire attacchi. Il **CFC di Napoli** è la principale struttura di tecnologia e innovazione nell'ambito della fornitura, sia a livello di AQ sia di CE, per offrire alle PA contraenti protezione e difesa, reattive e proattive, dalle minacce emergenti o esistenti. Il centro, cuore pulsante degli smart hub, è uno spazio di lavoro immersivo di oltre 600mq, che eroga servizi di Threat Intelligence, Managed Digital Identity, Managed Threat Operations, Managed Cloud Security, Digital Forensics ed Incident Response. Il CFC, che sfrutta la rete di strutture di innovazione su menzionate e il nutrito ecosistema di partnership tecnologiche, svolge il ruolo di collettore delle esperienze e del capitale, tangibile e intangibile, che esse mettono a disposizione. Il CFC di Napoli, inoltre, è il luogo in cui si concretizzano le iniziative di innovazione e formazione derivanti dalle collaborazioni di Accenture con gli atenei campani tra cui, le numerose attività di tesi specialistiche e la Cyberhackademy – corso di formazione basato su metodi di formazione innovativi voluto da Accenture e oggi alla sua seconda edizione in collaborazione con l'Università degli studi di Napoli Federico II.

Altre strutture **Accenture** coinvolte per apportare alla fornitura competenze in ambito PA e Cloud sono **a) Accenture Government Innovation Center** (**AGIC**), centro di Innovazione per la PA in cui le Amministrazioni possono conoscere le potenzialità dell'innovazione disponibile sul mercato e che fornisce uno spazio in cui sperimentare l'applicazione di nuove tecnologie e **b) Accenture Cloud Innovation Center** (**ACIC**) che offre competenze dedicate allo sviluppo e alla sperimentazione di soluzioni cloud con i partner tecnologici più rilevanti, per la prototipazione rapida di soluzioni *cloud-based* intrinsecamente sicure.

DEAS e Accenture forniscono al RTI i principali contributi di innovazione, descritti nel dettaglio al §17.2. Un fattivo supporto deriva, poi, dal contributo delle strutture di ricerca ed innovazione messe a disposizione dagli altri partner del RTI qui di seguito descritte.

Fincantieri NexTech è una società tecnologica di Fincantieri che sviluppa soluzioni nei settori della sicurezza e della protezione di informazione, rappresentando un **centro di competenza tecnologico del Gruppo**. Grazie alle esperienze nel settore militare e della sicurezza, alle competenze nell'analisi degli scenari operativi e alla capacità di realizzare sistemi complessi in "ambienti ostili", essa può supportare lo sviluppo e l'integrazione sia di soluzioni "legacy" - infrastrutture di campo basate su piattaforme tradizionali (SCADA) o su architettura SOA (Service Oriented Architecture) – e di erogare servizi SOC. Il contributo di **Fincantieri NexTech** in termini di innovazione deriva principalmente dalla collaborazione con le principali università e centri di ricerca, ad esempio grazie ai tre dottorati di ricerca finanziati in ambito cyber, e la partecipazione a progetti di ricerca nazionali e internazionali sui temi della sicurezza per ambienti militari e della difesa.

Fastweb è un MSSP (Managed Security Service Provider) ed eroga servizi di gestione operativa della sicurezza tramite il proprio SOC. Attraverso un **competence center e un osservatorio dedicati alla sicurezza,** da considerarsi integrati nella erogazione dei servizi connessi alla fornitura, Fastweb fornisce supporto ai servizi per adeguarsi in modo flessibile ed efficiente alle esigenze delle PA. Il principale contributo deriva da laboratori di sicurezza equipaggiati con **tecnologie all'avanguardia** per l'analisi di apparati embedded, strumentazioni di test e misura, centri dedicati a collaudi e prove tecniche per la certificazione di servizi e prodotti di sicurezza per la PA (es. Web Farm di **Roma** e **Milano**). Inoltre, Fastweb ha sviluppato un'infrastruttura IT, attraverso i propri Data Center distribuiti sul territorio

nazionale, che permette di erogare i più avanzati e complessi servizi a valore aggiunto (VAS) di cyber security. Fastweb dispone di una gamma completa e integrata di servizi di sicurezza, in modalità "on premise" e "as a service", in grado di soddisfare le esigenze di tutti i segmenti di mercato e di aziende di tutte le dimensioni, dalle start-up alle società di grandi dimensioni fino al settore pubblico. Con particolare riferimento ai servizi oggetto di gara, si citano a) **Fast Security 360°** che fornisce una difesa perimetrale completa e in tempo reale della rete aziendale da attacchi informatici, attraverso funzionalità implementate su apparati UTM (Unified Threat Management); b) **Fast KaleiDoS** per difendere le aziende e le PA dagli attacchi informatici DDoS (Distributed Denial of Service); c) **FAST Security Intelligence**, servizio di ricerca e Data Analytics, in grado di monitorare l'esposizione degli asset aziendali; d) **Fast Mail Security,** servizio di protezione della posta disponibile per Clienti con mail server ospitati on premises o con servizi di posta basati su infrastrutture di terze parti, e) **Fast Security - Advanced Protection** servizio che, utilizzando una tecnologia unica di analisi del traffico dell'endpoint, fornisce una protezione completa dagli attacchi APT, noti e non noti.

17.2 Ambito di intervento e valore aggiunto

Le strutture a supporto dell'innovazione proposte dal RTI sono parte integrante degli **smart hub,** sia a livello di AQ sia di singolo CE, e si focalizzano su ambiti di intervento specifici al fine di offrire valore aggiunto ai servizi oggetto della fornitura.

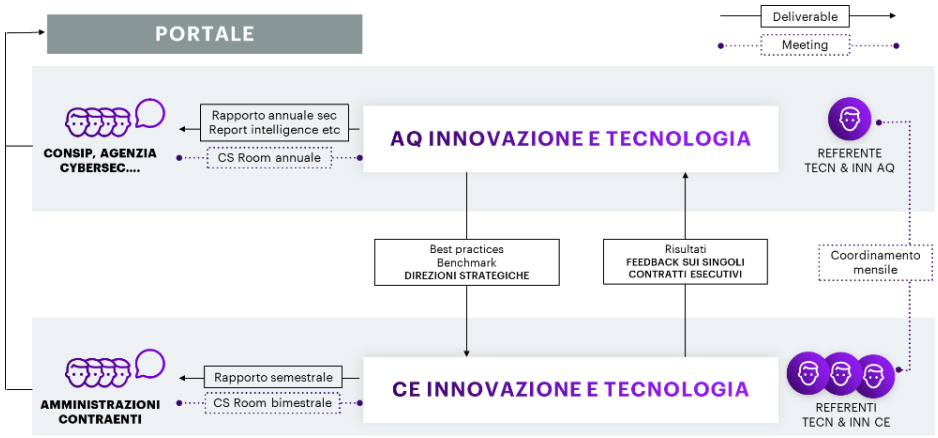
DEAS si propone per le attività di gestione continua delle vulnerabilità di sicurezza, Threat Intelligence & Vulnerability Data Feed e dei servizi di sicurezza specialistici. A tal fine, mette a disposizione competenze e tool sviluppati internamente per il rafforzamento della difesa perimetrale (**L1.S7** - Protezione degli end-point) e per lo sviluppo di soluzioni integrate di Cyber Threat Intelligence (**L1.S5** - Threat Intelligence & Vulnerability Data Feed). Essa dà valore aggiunto ai servizi oggetto della fornitura attraverso i seguenti asset innovativi:

- **DFC - Data Fusion Center (L1.S1, L1.S4)**, una piattaforma di Threat Awareness, disponibile in modalità as-a-service o stand-alone, che si configura come piattaforma di cybersecurity integrata con moduli IA/ML. Essa apporta alle tecnologie di Unified Threat Management (UTM) esistenti sul mercato la funzionalità innovativa di Situational Awareness, data dalla somma di più moduli integrati (Network Security Monitoring, Log Management Correlation, User Awareness, Network Awareness). DFC supporta le attività di Data Center Operations e Managed Security Services predisposte dal SOC per PA centrale, locale, e Grandi Aziende. Attraverso una gestione nativa degli incidenti (secondo le modalità CSIRT), DFC permette di gestire tutte le fasi operative del servizio SOC, agevolato da moduli di IA cognitiva e da molteplici e innovativi sistemi di visualizzazione grafica. In tal senso, le competenze di DEAS comprendono, nel complesso, un patrimonio operativo capace di garantire assistenza alle attività di cybersecurity del RTI (L1.S4 - Gestione continua delle vulnerabilità di sicurezza).
- **LVS - Laboratorio per la Valutazione della Sicurezza (L1.S15)**, struttura laboratoriale omologata OCSI (Organismo di Certificazione Sicurezza Informatica), per la ricerca e l'addestramento nelle pratiche aziendali collegate al disegno dei processi e delle operazioni di tool e soluzioni ICT. A supporto di un'innovazione rispondente al paradigma della security-by-design, il LVS è in grado di verificare gli obiettivi di sicurezza, la descrizione dell'ambiente in cui un oggetto di valutazione (ODV) è utilizzato, le minacce alle quali è soggetto, i requisiti funzionali e di fiducia, nonché la specifica delle funzioni di sicurezza.
- **Poligono cibernetico (L1.S9)**, infrastruttura hw/sw funzionale alla riproduzione di un ambiente operativo di simulazione di attacchi informatici e orchestrazione della risposta attraverso un training di gruppo basato su livelli diversi di automazione del Cyber Risk Management. Il Poligono abilita soluzioni di knowledge-transfer orizzontale e verticale capaci di integrare moduli didattici tradizionali con esperimenti coinvolgenti e una user-experience innovativa per la formazione di personale tecnico e non. Il Poligono supporta lo sviluppo di attività di apprendimento, in modo proattivo e interattivo, simulando ambienti reali, rendendo possibili attività di addestramento non sarebbero realizzabili su sistemi in produzione.
- **RaPToR, (L1.S7)**, la soluzione di endpoint protection, inclusa all'interno del "SPC Cloud L2 per i Servizi di Identità Digitale e Sicurezza Applicativa" che abilita misure avanzate anti-ransomware di Relevation, Response, Remediation secondo la logica R3 per endpoint (PC, dispositivi) e computer embedded (es. IoT).

Il **CFC Accenture** di Napoli rappresenta la struttura di riferimento per le attività di **tecnologia e innovazione.** Oltre a garantire una costante attività di **monitoraggio delle tecnologie emergenti**, esso è il principale attore nel garantire che le soluzioni proposte apportino nativamente valore aggiunto in termini di innovazione ai servizi oggetto della fornitura. In particolare, Accenture **propone i seguenti asset ed acceleratori** quali parte integrante del modello di erogazione dei servizi:

- **Next Generation Security Operation** (L1.S1, L1.S7, L1.S6, L1.S10) - il servizio di Next Generation Security operation descritto al §6 estende il concetto di **Security Orchestration and Response (SOAR)** a tutto il ciclo di vita della gestione degli incidenti, riducendo il tempo di rilevazione e risoluzione e garantendo consistenza in termini di risposta e scalabilità. Con l'evoluzione dell'Internet of Things è importante che gli strumenti e i processi del SOC possano adattarsi ad integrare anche i nuovi **device OT/IoT/IIoT all'interno degli scenari** di analisi. Accenture grazie alle recenti acquisizioni e agli investimenti in ambito OT ha realizzato piattaforme e acceleratori basati su algoritmi innovativi in grado di assicurare la stessa qualità del servizio nel caso di dispositivi connessi, per loro natura peculiari sia dal punto di vista tecnologico sia dei requisiti di sicurezza. Il servizio fa leva sulle principali tecnologie di mercato (es. Nozomi) in ambito OT per le quali Accenture vanta un robusto network di relazioni con i principali vendor e personale altamente qualificato.
- **Autonomous Identity** (L1.S10) - un approccio innovativo all'Identity & Access management, sviluppato da Accenture, che utilizza ML e AI per analizzare le caratteristiche degli accessi autorizzati e portare automazione nella autorizzazione, gestione e bonifica delle identità. Inoltre, esso consente di ridurre al minimo l'overprovisioning di risorse, riducendo automaticamente il rischio di accessi non autorizzati a risorse specifiche, e di realizzare il provisioning automatizzato e proattivo delle utenze (es. per nuovi utenti), riducendo il volume delle richieste di supporto e velocizzando significativamente il processo di on-boarding. La soluzione consente di incrementare la produttività con una diminuzione dei costi fino al 40% e di ridurre il rischio di accessi anomali fino al 30% con un alto grado di confidenza.
- **MultiCloud Security** (L1.S1, L1.S4, L1.S6) - Accenture ha implementato dal 2020 il programma "**Journey to Cloud**" ($3B di investimento globale) in cui la sicurezza è elemento fondante per mitigare i rischi associati alla migrazione e alle nuove minacce in cloud. Per il controllo delle misconfigurazioni in ambiente cloud, che ad oggi rappresentano la principale causa di attacco, Accenture ha sviluppato acceleratori in grado di apportare una riduzione massima dell'effort di remediation dell'85% ed una riduzione del 75% del 'time-to-compliance'. Attraverso l'uso di tecniche di hyperautomation, essi consentono l'esecuzione di controlli complessi nell'ordine di pochi minuti e abilitano controlli proattivi per bloccare l'occorrenza di potenziali incidenti in ambienti cloud pubblici, ibridi e privati indipendentemente dalla tecnologia.

17.3 Modalità organizzative del coinvolgimento



I soggetti del RTI deputati all'innovazione afferiscono all'ambito di competenza **Tecnologia e Innovazione** degli **Smart Hub**.

Secondo un modello operativo, coordinato dal **Referente Tecnologia e Innovazione,** essi operano sia a livello di AQ sia di CE garantendo un continuo allineamento in ottica di collaborazione, condivisione di conoscenza e *cross-fertilization* tra le PA a beneficio della sicurezza dell'intero sistema paese. A livello di AQ, il **Referente Tecnologia e Innovazione** coordina le attività della struttura ed è il punto di riferimento diretto per CONSIP e per tutti gli attori chiave coinvolti nelle decisioni strategiche per il paese. Per ogni CE, un **Referente Tecnologia e Innovazione** è a sua volta responsabile del coordinamento delle attività del singolo contratto e lavora in costante coordinamento con il **Referente Tecnologia e Innovazione** di AQ, oltre che con le PA contraenti. I referenti delle strutture di Tecnologia e Innovazione a livello di AQ e CE si coordinano mensilmente per un avanzamento sullo stato complessivo delle attività e per favorire lo scambio di informazioni, idee e risultati che alimentano il processo di innovazione. Per garantire il governo strategico e continuo delle iniziative di innovazione e il loro costante monitoraggio, è istituito un **presidio di steering**, denominato **Cybersecurity Room**, sia a livello AQ sia CE.

La **Cybersecurity Room di AQ** si configura come presidio di advisory strategica dedicato a Consip oltre che come presidio tematico-tecnologico costantemente attivo e osservatorio per la sicurezza nazionale a beneficio del sistema paese. Essa ha il compito di a) coordinare le Cybersecurity Room istituite a livello di CE, b) elaborare **rapporti annuali** sullo stato della sicurezza nella PA anche attingendo alle strutture di Cyber Threat Intelligence del RTI , c) elaborare le direzioni strategiche e di innovazione da diramare alle strutture dei singoli CE e d) recepire feedback dalle Cybersecurity room dei singoli CE al fine di elaborare best practices e lessons learned (es. materiale per la formazione in ambito cyber su nuove minacce). La Cybersecurity Room di AQ si riunisce con cadenza semestrale o su specifica richiesta del cliente e vede la partecipazione di almeno un esponente di ogni azienda del RTI, del Referente Tecnologia e Innovazione e di Referenti preposti all'innovazione identificati da Consip.

La **Cybersecurity Room di CE** si configura come presidio di supporto operativo e tecnologico per le amministrazioni contraenti oltre che come osservatorio sulle nuove tecnologie. Essa ha il compito di a) recepire le istanze strategiche e gli obiettivi specifici stabiliti a livello di AQ, b) raccogliere e recepire feedback e criticità riscontrate durante l'operatività dei servizi in ambito, c) elaborare **rapporti semestrali** sulla sicurezza dei sistemi interni dell'Amministrazione Contraente che riepiloga le attività effettuate e lo stato dei servizi e d) avanzare proposte per migliorare la qualità dei servizi, suggerendo ad esempio l'introduzione di nuove tecnologie e/o di gradi crescenti di automazione. Essa si riunisce con cadenza bimestrale o all'occorrenza su specifica richiesta del cliente e vede la partecipazione di almeno un esponente di ogni azienda del RTI, del referente Tecnologia e Innovazione e di referenti preposti all'innovazione identificati dalle amministrazioni contraenti. Per ogni CE, il RTI s'impegna annualmente a fornire una POC su tecnologie innovative in collaborazione con partner tecnologici, la attivazione di una o più tesi di laurea e/o tirocini con uno o più atenei e l'organizzazione di una o più sessioni di co-creazione con le amministrazioni contraenti.

Al presidio di steering costituito dalle **Cybersecurity Room**, gli specialisti di alto profilo che fanno parte delle strutture di Tecnologia e Innovazione offrono un presidio operativo a supporto della esecuzione delle attività ordinarie. Essi interagiscono con il cliente sia in modalità **proattiva**, facendosi promotori di proposte innovative quali progetti finalizzati alla realizzazione di POC, prototipi per l'attivazione di nuove soluzioni o evoluzione di quelle in uso anche attraverso seminari e workshop, sia **reattiva**, rispondendo a specifiche richieste che richiedono disegno, progettazione e/o implementazione di soluzioni innovative sia in termini tecnologici (facendo leva sui partner di ecosistema) sia di modelli e metodologie (facendo leva su partner accademici e centri di competenza), anche attraverso sessioni di co-creazione per fornire risposte tempestive aderenti ai requisiti. In caso di modalità reattiva, il RTI si impegna ad attivare la struttura entro **due settimane** dalla ricezione della richiesta della PA, sia a livello di AQ sia di CE.I **rapporti prodotti e gli output delle Cybersecurity Room**, sia di AQ sia di CE, contribuiranno a popolare il Portale di Fornitura (cfr. §16), riportando ad esempio i trend sullo stato della sicurezza nella PA o lo stato della security o i trend di miglioramento della sicurezza osservati nel tempo per le singole Amministrazioni, nel rispetto della profilazione dei ruoli e preservando la confidenzialità dei dati condivisi.

18 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ - TIIS – Tempo di prima investigazione per incidenti di sicurezza

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico "Indicatori di qualità", il Raggruppamento s'impegna a garantire una riduzione dei valori di soglia previsti per l'indicatore TIIS secondo le indicazioni di seguito riportate:

Gravità Alta, TIIS <=2 ore solari e Gravità Media, TIIS <=4 ore solari.

19 MIGLIORAMENTO SOGLIE INDICATORI DI QUALITÀ - TCIS – Tempo di primo contenimento per incidenti di sicurezza

Con riferimento a quanto indicato nell'Appendice 1 al Capitolato Tecnico "Indicatori di qualità", il Raggruppamento s'impegna a garantire una riduzione dei valori di soglia previsti per l'indicatore TCIS secondo le indicazioni di seguito riportate:

Gravità Alta, TCIS <=6 ore solari e Gravità Media, TCIS <=10 ore solari.

20 ASSUNZIONE DELLE RISORSE PROFESSIONALI

Rispetto al complesso delle assunzioni necessarie per ogni contratto esecutivo finanziato, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC, e fermo restando il rispetto del requisito necessario di cui al Capitolato tecnico generale al par. 7.1 il Raggruppamento si impegna ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione di ciascun contratto esecutivo o per la realizzazione di attività ad essi connessi o strumentali, nella seguente misura: **>35%.**