Roma, 07/10/2021

GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296

LOTTO 1

RELAZIONE TECNICA

Indice

Indice delle Figure

Indice delle Tabelle

1. PREMESSA

Il Raggruppamento Temporaneo di Impresa (RTI) ritiene di poter offrire alle Pubbliche Amministrazioni (PA) contraenti una soluzione completa e di elevatissimo livello, garantita dalla fornitura di prodotti innovativi best in class, dalla professionalità e competenze delle risorse disponibili e da una consolidata capacità metodologica ed organizzativa delle aziende raggruppande. Le soluzioni proposte rispondono ai requisiti stabiliti dal Capitolato Tecnico di gara, che si intendono tutti rispettati e accettati compreso quanto specificato nelle risposte alle domande di chiarimento.
Il costituendo RTI è composto da **TIM** quale mandataria, **AlmavivA, KPMG, Netgroup** e **ReeVo** quali mandanti.

2. PRESENTAZIONE E DESCRIZIONE OFFERENTE

Di seguito si riportano i dati identificativi dei soggetti muniti dei necessari poteri che sottoscrivono l'offerta.

TIM	Riferimenti: Codice Fiscale: Documento:	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Tabella 1 – Dati identificativi dei soggetti muniti di poteri di firma

Di seguito si riportano le descrizioni delle aziende.

TIM – Gruppo leader in Italia e in Brasile nel settore ICT, sviluppa infrastrutture fisse, mobili, cloud e datacenter e offre servizi e prodotti per le comunicazioni e l'intrattenimento, ponendosi all'avanguardia delle tecnologie digitali. Il gruppo si avvale di factory specializzate che offrono soluzioni digitali integrate per cittadini, imprese e PA: **Noovle** è la cloud company di TIM, **Olivetti** è il polo digitale con focus sullo sviluppo di soluzioni IoT, **Telsy** opera nel settore della Cyber Security e **Sparkle** implementa infrastrutture e servizi internazionali. Nello sviluppo del business il gruppo ha fatto propri gli obiettivi di tutela dell'ambiente e di inclusione sociale. In particolare, il progetto Operazione Risorgimento Digitale promuove la diffusione di competenze digitali utili per lo sviluppo del Paese, mentre Fondazione TIM sostiene progetti di alto interesse sociale. Al 31 Dicembre 2020 l'organico complessivo dell'azienda è di 52.333 dipendenti di cui 42.667 in Italia. I principali dati economico-finanziari relativi al 2020 sono: ✓**investimenti industriali** per 3,4 miliardi di euro, ✓**ricavi** per 15,8 miliardi di euro ed ✓**EBITDA** di 6,7 miliardi di euro. TIM vanta una pluriennale esperienza maturata sulla gestione di convenzioni e accordi quadro nella PA: ✓**Reti Locali**; ✓**Videosorveglianza**; ✓**Telefonia Mobile**; ✓**Centrali Telefoniche**; ✓**Contratto Quadro SPC Cloud Lotto 1**.

KPMG – Da oltre 60 anni in Italia, il Network KPMG è ricompreso tra le più importanti piattaforme di servizi professionali attive nel nostro Paese. Il Network è presente in Italia con **4 entità**, **25 uffici** e **4.370 persone**. Tale capillarità territoriale consente di cogliere in maniera immediata le opportunità e le esigenze delle economie del territorio, interpretando nel modo più autentico la struttura portante dell'economia nazionale. La struttura Information Risk Management di KPMG offre una rara combinazione, di competenze tecnologiche e di una profonda conoscenza del mercato, con professionisti che aiutano le aziende a proteggere il business da eventuali attacchi, stando al ritmo e alla velocità con cui operano i cyber criminali.

NETGROUP – Azienda leader nell'innovazione e nella trasformazione digitale in ambito ICT, opera da oltre 25 anni sul mercato italiano della Pubblica Amministrazione e dell'Industria. La competenza sulle tematiche ICT, una vision improntata alla ricerca dell'innovazione, nonché la forte focalizzazione sui temi trasversalmente legati alla security, guidano Netgroup in un processo di aggiornamento continuo del know-how, con particolare riferimento all'ambito Cyber Security, mediante l'acquisizione di competenze e partnership tecnico/commerciali con i più innovativi esponenti del settore, per il continuo potenziamento del portafoglio di servizi e prodotti offerti. I servizi Cyber Security sono oggi erogati per primarie realtà nazionali e internazionali in ambito PA e Industria. I valori guida cui l'azienda si ispira sono: capacità tecnologiche e orientamento all'**innovazione**; metodologie di lavoro **agile**; **flessibilità** organizzativa; sistemi di **qualità** (ISO 9001), di gestione del **servizio** (ISO 20000), di gestione della **sicurezza delle informazioni** (ISO 27001) e di gestione **ambientale** (ISO 14001); **skill e competenze** elevate in ambito security**; infrastrutture organizzative e logistiche** disponibili su tutto il territorio nazionale; **complementarità delle competenze**.

ALMAVIVA – Ha progettato, realizzato e gestito alcuni dei più significativi sistemi per la PA, per Banche e Assicurazioni, Agricoltura, Trasporti e Logistica, Sanità. La professionalità delle risorse AlmavivA è attestata dalle numerose certificazioni di sicurezza vendor independent e sulle principali tecnologie di mercato oltre che sulla conduzione dei progetti (ITIL v4, PMI, IFPUG, Prince2, Cobit5, Togaf). Tutti i servizi sono certificati ISO 9001:2015, ISO 27001:2013, ISO 20000, ISO 22301, ISO 50001 e AQAP 2110/AQAP 160, ISO/IEC 25010:2011, ISO/IEC TS 25011: 2017, UNI ISO/IEC 25012:2014, ISO/IEC 25022:2016, ISO/IEC 25023:2016, UNI CEI ISO/IEC 25024:2016. AlmavivA adotta nuove modalità di ingaggio e valorizzazione delle risorse, che prevedono un rapporto strategico, sistemico e integrato con le migliori Università, i progetti di ricerca più sfidanti, le Academy e gli Hackaton su tutto il territorio nazionale. Il **Centro di Competenza Sicurezza ICT di AlmavivA** è una struttura dedicata e specializzata nell'erogazione di servizi di gestione e servizi professionali specialistici in ambito Sicurezza informatica. Il SOC assicura una continua prevenzione dei rischi e delle minacce che possono pregiudicare la qualità dei servizi erogati ai clienti e garantisce il mantenimento di un elevato livello di Sicurezza con un approccio **security e privacy "by-design" e "by-default"**.

AlmavivA è mandataria del RTI aggiudicatario del **Contratto Quadro per i servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni.** In questo ambito, nel contesto dell'erogazione dei servizi contrattuali, assicura attraverso il proprio SOC la **sicurezza del Centro Servizi, certificato ISO27001,** svolgendo le attività di installazione, setup, delivery e conduzione delle soluzioni di sicurezza per la **protezione di portali web di primaria importanza in ambito nazionale ed internazionale** quali ad esempio: il sito della presidenza italiana del G20 del 2020, il sito Italia Expo Dubai 2020, il portale istituzionale dell'AIFA, il sito dell'Agenzia Nazionale del Turismo Italia.it, il Portale del Nuovo preventivatore IVASS.

REEVO – PMI innovativa fondata nel 2003, è il cloud provider italiano focalizzato sui servizi di Cyber Security e archiviazione che consente alle aziende e alle Amministrazioni di proteggere e custodire il vero patrimonio aziendale rappresentato dai dati. Reevo, oltre a custodire i dati attraverso risorse e piattaforme tecnologiche, analizza le minacce, le vulnerabilità e i rischi dei servizi del cloud e delle reti clienti al fine di proteggerli da attacchi esterni ed interni. Infine, Reevo dispone di Centri di Competenza distribuiti sul territorio nazionale specializzati nella ricerca di soluzioni innovative specializzate sulla Cyber Security.

3. STRUTTURA ORGANIZZATIVA

3.1. MODALITÀ ORGANIZZATIVE *PER LA GESTIONE DELL'ACCORDO QUADRO E DEI CONTRATTI ESECUTIVI*

Il RTI intende adottare un **approccio unitario** *e* **integrato** al governo e all'esecuzione della fornitura, in grado di far corrispondere le potenzialità dei nuovi servizi con le esigenze delle Amministrazioni e di *accompagnare* queste ultime all'utilizzo efficiente dei nuovi servizi. La costituzione del RTI consente alle aziende raggruppande di **sfruttare i rispettivi punti di forza** nell'ambito di un **modello operativo unico**, che prevede funzioni di **governo centrale** della fornitura, per la gestione dell'Accordo Quadro (AQ) e per il supporto a Consip/AgID, e funzioni di governo dei Contratti Esecutivi (CE) stipulati con le singole PA. Nell'ambito del modello organizzativo proposto, particolare rilevanza è assunta dal **Comitato di Governance RTI**, costituito dai responsabili di tutte le aziende raggruppande, cui spetta il ruolo di *uniformare gli approcci e le modalità operative* delle diverse aziende, garantendo l'adozione di un modello operativo comune nell'erogazione dei servizi e assicurando il monitoraggio continuo delle performance dei servizi e del livello di soddisfazione delle PA.

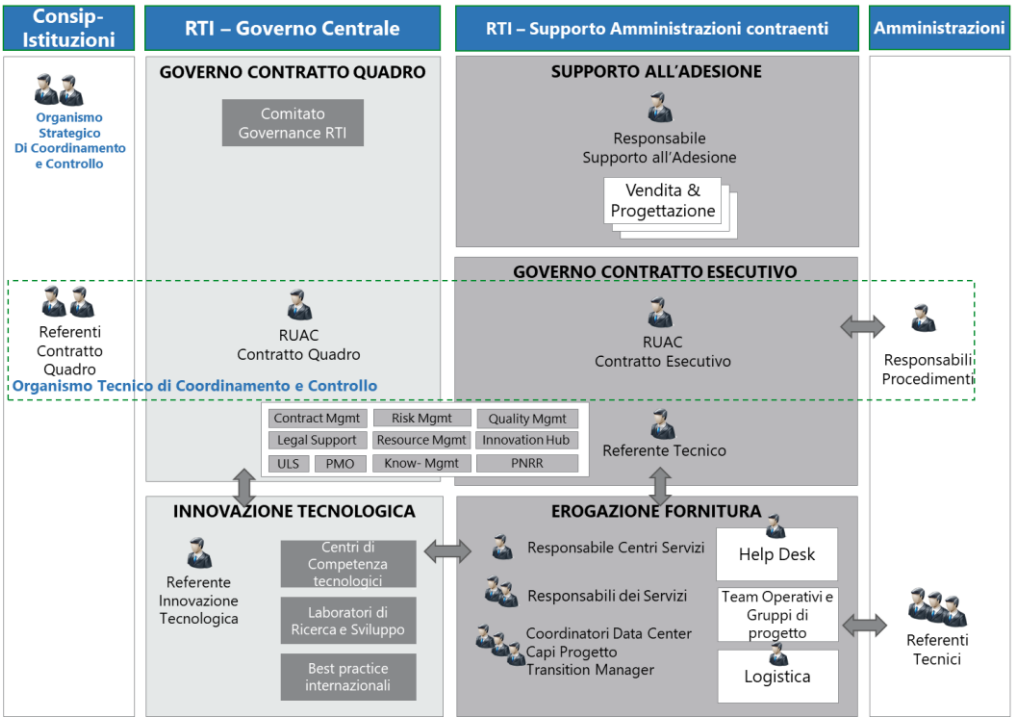

Figura 1 – Figure di riferimento nel modello organizzativo

Governo dei contratti

In conformità con i requisiti di Capitolato, il modello proposto prevede un **Responsabile Unico delle Attività Contrattuali** (**RUAC**), in relazione diretta con Consip/AgID, per le tematiche legate all'AQ, che sarà il Rappresentante del RTI nell'Organismo Tecnico di Coordinamento e Controllo. Nel modello è inoltre presente un **Responsabile Unico delle Attività Contrattuali** per ogni Contratto Esecutivo che gestisce i rapporti con la PA contraente e garantisce supporto all'Organismo Tecnico di Coordinamento e Controllo. I RUAC sono supportati dalle funzioni di staff, descritte di seguito:

Ruolo	Responsabilità
Contract Management	Funzione di supporto per tutti gli aspetti dei contratti e della loro corretta esecuzione. Svolge attività di verifica della copertura contrattuale e delle performance e fornisce supporto anche alle strutture di produzione nell'interpretazione delle clausole contrattuali.
Risk Management	Supporta l'intera organizzazione del RTI in tutti gli aspetti di valutazione del rischio. Effettua periodicamente un'analisi dei rischi sugli aspetti operativi dei servizi forniti e valuta le necessarie azioni di mitigazione.
Quality Management	Produce i Piani di Qualità Generale dell'AQ e Specifici di contratto e li modifica a fronte delle richieste di Consip/AgID/Amministrazioni contraenti. Esegue e coordina le verifiche di qualità secondo i piani approvati. Supporta Consip nelle verifiche ispettive sulla fornitura. Supporta i RUAC nelle analisi dei dati relativi a SLA, rilievi e penali e concorda azioni di mitigazione con le strutture operative.
Regulatory Support	Riferimento per gli aspetti legati alla valutazione e risoluzione di potenziali problemi di carattere legale introdotti dall'adozione dei servizi di sicurezza, tipicamente: leggi internazionali (Unione Europea), regolamenti comunitari, normative e giurisprudenza sulle tematiche dei servizi.
Resource Management	Identifica con le strutture operative delle aziende raggruppande i requisiti della fornitura in termini di risorse e profili professionali, coordinando le attività di selezione e di skill inventory. Collabora con i responsabili delle diverse unità di produzione per la definizione e l'aggiornamento continuo del Piano delle Risorse e dei Piani di Formazione.
Program Management Office (PMO)	Collabora con i RUAC per rappresentare in un quadro di riferimento unico l'andamento della fornitura in termini di volumi e di impegni (Piani Operativi). Fornisce consulenza e supporto al RUAC dei Contratti Esecutivi per le attività amministrative della fornitura (es. budget, fatturazione).
Unità Locale di Sicurezza (ULS)	Riferimento unico per tutti gli aspetti legati alla sicurezza. Recepisce le politiche di sicurezza di Consip/AgID e delle PA, identifica le misure che implementano tali politiche, diffonde tali misure lungo la filiera operativa e ne monitora l'applicazione. È owner della documentazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) secondo lo standard ISO 27001. Produce i Piani della Sicurezza per i diversi Centri Servizi e successive modifiche.
Funzione di Knowledge AQ & Content Management del Portale	Struttura a supporto del RUAC di AQ e dei RUAC di CE, che assicura: ✓la valorizzazione, diffusione, replicabilità e riuso delle lesson learned, success stories e best practice acquisite nell'AQ e nella pluriennale esperienza del RTI in materia di Risk Management, Cyber Security, Security Awareness, Sicurezza Informatica, etc.; ✓gestione editoriale dei contenuti e aggiornamento del Portale della Fornitura.

Funzione di "Innovation Hub"	Struttura a supporto del RUAC di AQ e dei RUAC di CE, ha funzione di coordinamento del processo "Innovation management" (cfr. cap.17), affianca le PA nella qualificazione dei "bisogni di innovazione". Inoltre, individua e ingaggia, in fase di attivazione, sul singolo CE le strutture dell'Ecosistema dell'Innovazione del RTI più idonee, per assicurare la migliore risposta in termini di soluzioni innovative e a valore aggiunto incrementando la consapevolezza delle PA in materia di Sicurezza (es. competence center, tech-labs, incubatori e acceleratori di innovazione).
Funzione di "Funding Innovation e PNRR"	Struttura a supporto del RUAC di AQ e dei RUAC di CE, affianca le PA che intendono aderire all'AQ nella valutazione delle fonti di finanziamento dei progetti e investimenti da effettuare in materia di innovazione di processi di gestione della sicurezza (es. PNRR, fondi comunitari e nazionali, venture capital pubblico-privato).

Tabella 2 – Funzioni di staff

Supporto all'adesione

Il RTI intende promuovere l'adesione ai servizi attraverso attività condotte sia centralmente sia sul territorio, organizzate in fasi. A sostegno delle campagne di comunicazione, e come canale informativo on-line, il RTI utilizzerà l'Area Comunicazione del *Portale della Fornitura* (cfr. cap.16), allo scopo di: ✓creare e diffondere materiale informativo; ✓facilitare il contatto diretto con le PA sul territorio attraverso strumenti di pianificazione; ✓pubblicare materiale multimediale illustrativo sulle modalità di adesione all'iniziativa.

Il supporto all'adesione è affidato alle forze di Vendita e Progettazione del RTI la cui capillare diffusione sul territorio consente di raggiungere la totalità delle PA.

Nella figura a lato sono evidenziate le fasi del supporto all'adesione, all'interno del processo complessivo di contrattualizzazione, e le macro-attività previste. La singola PA sarà pertanto in grado di individuare, con il supporto del RTI, gli indicatori di digitalizzazione più idonei al monitoraggio del raggiungimento degli obiettivi definiti nel Piano triennale e conseguentemente definire il Piano dei Fabbisogni.

Figura 2 – Fasi del Supporto all'Adesione

Innovazione tecnologica

Il RTI ritiene che abbia una particolare rilevanza il costante aggiornamento tecnologico per mantenere il sistema di sicurezza delle PA allineato alle evoluzioni continue delle minacce. Pertanto, nel modello organizzativo proposto, il RTI prevede la figura di un **Referente per l'Innovazione Tecnologica** che, nella sua funzione, avrà la responsabilità di informare periodicamente Consip e le PA contraenti sull'evoluzione tecnologica dei servizi, ed eventualmente supportare le valutazioni dei comitati di coordinamento e controllo tecnico e strategico (cfr. cap.17).

Inoltre, il RTI propone un **Ecosistema dell'Innovazione** a supporto dei Team operativi, articolato come segue:

- **Global Competence Center** interni al RTI: Centri che mettono a disposizione dei team di intervento conoscenze specialistiche, metodologie, soluzioni e tool innovativi, per migliorare qualità ed efficacia dei Servizi;
- **Tech-labs, Innovation Lab e Centri di ricerca e sviluppo**: Laboratori e centri di innovazione di ricerca e sviluppo di soluzioni innovative/prototipali per la trasformazione digitale della PA. Sono strutture interne al RTI e/o costituite in partnership con grandi centri di ricerca e poli universitari nazionali e internazionali;
- **Osservatori tematici, normativi e di Cyber Security Innovation** interni al RTI: presidiano su scala globale la frontiera dell'innovazione su temi di interesse della Fornitura (es. PNRR, Cyber Security in ambito pubblico, etc.);
- **Incubatori e acceleratori di innovazione** interni al RTI e/o con i quali le aziende del RTI collaborano stabilmente (es. partnership con incubatori di innovazione, università, etc.) che sostengono e accelerano la crescita di start-up e PMI innovative, con strumenti ad hoc (es. spazi fisici e digitali di co-working, business matching e networking, accesso a nuovi mercati e alla finanza agevolata). Tali strutture rappresentano un canale privilegiato per individuare e ingaggiare in tempo reale operatori specializzati per contribuire direttamente all'innovazione delle PA aderenti all'AQ in materia di Cyber Security;
- **Partnership IT**: Strutture interne al RTI che gestiscono e sviluppano collaborazioni con vendor di soluzioni tecnologiche leader di mercato che rappresentano piattaforme abilitanti all'adozione dei programmi di trasformazione della PA in materia di "gestione della sicurezza".

Erogazione dei servizi

Il modello organizzativo proposto dal RTI per l'erogazione dei servizi ha l'obiettivo di: ✓**individuare punti di responsabilità chiari e precisi**; ✓distribuire l'esecuzione dei servizi sui diversi gruppi di lavoro in modo da ottenere la **massima efficienza nell'operatività**; ✓presidiare i processi di servizio per monitorare e favorire l'applicazione delle best practice *e* dei requisiti di qualità.

La struttura di erogazione dei servizi prevede le seguenti figure-chiave:

- **Referente Tecnico** per ciascuna PA, che riporta al RUAC del CE, assume la responsabilità tecnica dell'esecuzione di tutti i servizi. Questa figura racchiude in sé le competenze di Service Management (ITIL), di Project Management (PMI/PMBoK) e di gestione della sicurezza (ISACA CISM). Il Responsabile Tecnico si interfaccia con i Referenti della PA per tutte le problematiche di natura tecnica afferenti al CE. Costituisce il punto di riferimento anche per gli aspetti organizzativi inerenti all'allocazione delle risorse dei Servizi Specialistici con il supporto della funzione di Resource Management.
- **Responsabile dei Centri Servizi** che assume la responsabilità dei servizi forniti da remoto dal Centro Servizi Virtuale del RTI.

In figura è rappresentato il modello organizzativo generale per l'erogazione dei CE che introduce le seguenti figure:

- **Transition Manager**: Pianifica e conduce il progetto di presa in carico dei servizi da parte delle strutture operative del RTI per le attività necessarie alla transizione. Concorda con i Responsabili dei singoli servizi le tempistiche e ne traccia l'avanzamento. Riferisce al Referente Tecnico e al RUAC del CE sullo stato delle attività, e si interfaccia direttamente con le funzioni tecniche dell'Amministrazione nelle sessioni di pianificazione e di stato avanzamento della transizione. Coordina le attività di phase out di fine fornitura;
- **Responsabili Servizi:** Uno per ciascun servizio o gruppo di servizi affini. Garantiscono la regolare erogazione del servizio coordinando le attività delle risorse assegnate al proprio gruppo di lavoro. In particolare, il Responsabile SOC coordina il team dedicato a supportare la gestione di incidenti e attacchi ostili in ambito dei servizi di sicurezza; supervisiona il processo di gestione degli incidenti, intervenendo direttamente nella gestione delle escalation verso l'Amministrazione nei casi particolarmente critici o complessi;

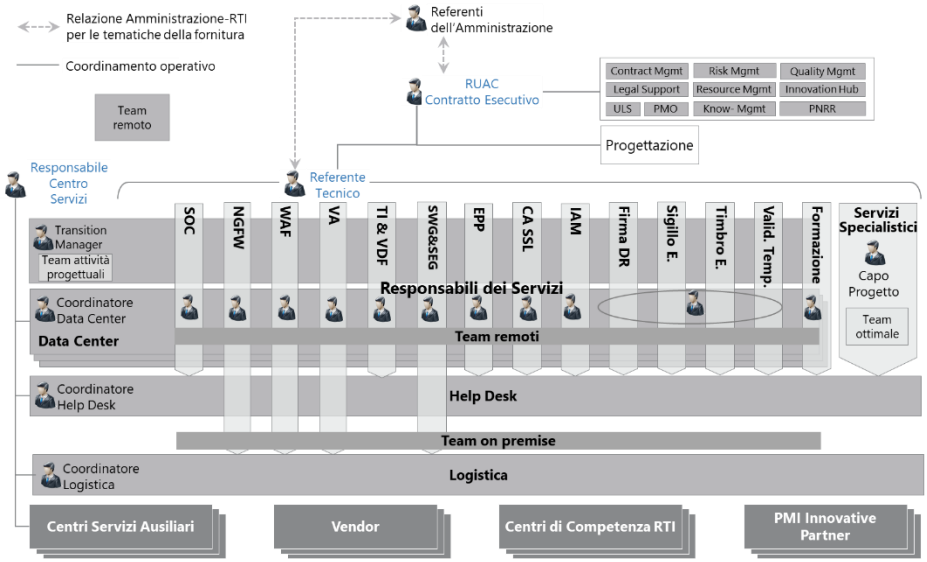

Figura 3 – Modello generale di erogazione dei servizi

- **Coordinatori Data Center**: Uno per ciascun Data Center (DC) utilizzato dal RTI per la fornitura (cfr. cap. 4), rispondono funzionalmente al Responsabile del Centro Servizi. Ogni coordinatore ha la responsabilità diretta del DC nel suo complesso: sicurezza, logistica, disponibilità degli spazi, funzionamento degli impianti, personale;
- **Coordinatore Help Desk**: Garantisce il buon funzionamento del servizio di Help Desk. Ha la responsabilità diretta del funzionamento degli strumenti, del personale, dei turni di lavoro.
- **Coordinatore Logistica**: Coordina e monitora le attività di stoccaggio e movimentazione dei materiali fra i centri logistici del RTI e la consegna dei materiali presso i punti di raccolta dei magazzini, sia in caso di nuove installazioni sia per il replacement degli apparati in caso di malfunzionamenti, supportando i tecnici preposti alla manutenzione al fine di garantire il soddisfacimento degli SLA.

Il modello è completato dalle entità di supporto, qui riepilogate: ✓**Centri Servizi Ausiliari**: Sono i Security Operation Center, i Network Operation Center e gli IT Operation Center previsti nell'organizzazione preposta all'erogazione dei servizi (cfr. cap. 4); ✓**Vendor**: Sono le aziende che producono le componenti tecnologiche HW-SW utilizzate nell'architettura di riferimento, e in particolare le strutture di supporto specifiche per i prodotti usati. Sono coinvolte nella risoluzione di problemi riscontrati sui prodotti, o in analisi e studi di fattibilità su nuovi modelli di servizio che richiedono funzionalità particolari; ✓**Centri di Competenza del RTI**: Forniscono risorse e competenze specialistiche su tematiche tecnologiche e di settore. Forniscono risorse aggiuntive da impiegare nella fornitura dei servizi per gestire eventuali picchi di lavoro; ✓**PMI Innovative/Partner**: Ecosistema di PMI innovative integrate nelle attività del RTI ed aziende terze comprese nel network di subfornitori delle aziende raggruppande, forniscono risorse specializzate a completamento di quelle messe in campo dal RTI.

3.2. DISTRIBUZIONE DELLE RESPONSABILITÀ FRA LE AZIENDE RAGGRUPPANDE

Il RTI mette a disposizione della PA capacità operative e soluzioni ampiamente consolidate presso primari clienti pubblici e privati che coprono tutti i servizi del presente AQ. Inoltre, il RTI vanta un notevole background relativamente alle procedure amministrative e ai processi interni della PA e ciò assicura la capacità di gestire forniture complesse e personalizzate in base ai diversi scenari, organizzativi e tecnologici, presenti nelle diverse Amministrazioni.

Organizzazione generale della fornitura

Le aziende raggruppande saranno organizzate secondo un modello univoco che comprende: ✓le strutture di *Account* che hanno la responsabilità dell'esecuzione dei contratti; ✓i *Centri di Competenza*, dove viene definito e implementato il portafoglio dei servizi; ✓le strutture di *Vendita* e *Prevendita*, che diffondono i servizi sul mercato; ✓i centri di *Delivery ed Operation*, che eseguono tutte le attività di attivazione ed erogazione dei servizi.
Le aziende raggruppande metteranno a disposizione del RTI le capacità delle proprie strutture per assicurare il successo della fornitura in tutte le sue componenti:

Area della fornitura	Struttura RTI	Caratteristiche
Governo AQ	Gestione Convenzioni	Struttura dedicata alla gestione del ciclo di vita delle convenzioni/AQ stipulati con Consip e ai relativi adempimenti contrattuali
Governo Contratti Esecutivi	Strutture RTI di Account	Organizzazioni dedicate alla gestione dei contratti di servizio nel settore pubblico, con focalizzazioni su PAC (incluso il settore Interforze) e su PAL
Supporto all'Adesione	Strutture RTI di Vendita e Progettazione	Strutture distribuite sul territorio (Nord-Ovest, Nord-Est, Centro, Sud) dedicate allo sviluppo del business.

Area della fornitura	Struttura RTI	Caratteristiche
Innovazione Tecnologica	Centri di Competenza RTI sulla Cyber Security	Startup Innovative e Centri di ricerca e sviluppo per la sperimentazione e la messa a punto di nuove tecnologie.
Erogazione Servizi	Strutture RTI di Delivery, Assurance ed Operation	Strutture distribuite, coinvolte nell'erogazione dei servizi oggetto di fornitura.

Tabella 3 – Strutture coinvolte nella fornitura

Sarà responsabilità del **Comitato di Governance RTI**: ✓nominare le **figure chiave** per il governo della fornitura, identificando i professionisti più qualificati per i ruoli di RUAC di AQ, RUAC di CE, Referente per l'Innovazione Tecnologica, Responsabile del Centro Servizi, Responsabili Tecnici; ✓assicurare il coinvolgimento dei **Centri di Competenza** nazionali e internazionali che si occupano delle tematiche di interesse per la fornitura; ✓assicurare la **disponibilità delle risorse** (Centro Servizi, Help Desk, Team Ottimali) necessarie all'erogazione dei servizi; ✓supervisionare l'andamento generale dell'iniziativa, il **livello di soddisfazione** delle Amministrazioni contraenti e valutare possibili evoluzioni.

Distribuzione delle responsabilità

Nella definizione del modello organizzativo per il governo e l'erogazione dei servizi, la decisione di costituire un RTI così composto nasce dalla volontà delle aziende raggruppande di sfruttare i rispettivi punti di forza in una logica di: ✓**complementarietà** nella ripartizione dei servizi con assegnazione di **ruoli e responsabilità** chiare e precise; ✓**flessibilità** nell'erogazione dei servizi grazie alla presenza di un Centro Servizi Virtuale unico, distribuito ed integrato tra le aziende del RTI in grado di erogare tutti i servizi della fornitura.

La complementarietà può essere declinata in termini di competenze tecniche ed organizzative ed in particolare la **complementarietà** di natura **organizzativa** garantisce: ✓una **governance solida,** sia a livello di Accordo Quadro sia di Contratti Esecutivi, grazie al ruolo di coordinamento svolto dalla mandataria TIM con il supporto delle mandanti, e all'adozione del **framework ITIL; ✓affidabilità**, **solidità** e **stabilità** grazie ad una presenza duratura e qualificata nel tempo delle risorse interne sugli ambiti oggetto del presente AQ.

La **complementarietà** in termini di **competenze tecniche**, si esprime nella capacità di garantire conoscenze adeguate su tutti gli ambiti di gara attraverso la sinergia delle esperienze e delle competenze acquisite: ✓**TIM e AlmavivA** possiedono infrastrutture abilitanti per l'erogazione dei servizi di Cyber Security, processi consolidati e risorse competenti per la loro gestione; ✓**KPMG** e **Netgroup** erogano principalmente servizi di formazione e di supporto specialistico grazie alla disponibilità di personale certificato negli ambiti di servizio proposti e grazie agli accordi di collaborazione con istituti nazionali ed internazionali di formazione nell'ambito specifico della Cyber Security; ✓**ReeVo** fornisce un forte impulso innovativo negli ambiti di servizio applicabili.

La complementarietà delle competenze tecniche è garantita inoltre dalla copertura delle **partnership** con tutti i principali attori sul mercato della Cyber Security e dalla presenza dei **centri di competenza** all'interno dell'**Ecosistema dell'Innovazione** che costituiranno un polo integrato cui potranno attingere le strutture operative impegnate nell'erogazione dei servizi.

In tabella si riportano le certificazioni possedute dalle aziende del RTI:

Certificazioni vendor independent	TIM	ALMAVIVA	NETGROUP	KPMG	REEVO
Togaf 9			✓		
ITIL v3/4	✓	✓	✓	✓	✓
ISO 27001 Lead Auditor	✓	✓	✓	✓	✓
ISO 27001 Foundation			✓		
ISO 22301 Auditor		✓		✓	
ISO 27017					✓
ISO 27018					✓
ISO 27701					✓
ISAE 3402 Type2					✓
SSAE 18 Type2					✓
Certified Information Security Manager (CISM)	✓	✓	✓	✓	
Certified Information Systems Security Professional (CISSP)	✓	✓		✓	
Certified Information Privacy Professional / Europe (CIPP/E)			✓		
Certified Etical Hacker (CEH)	✓	✓		✓	
Cyber Security X Fundamentals (CSX-F)	✓	✓		✓	
Certified of Cloud Security Knowledge (CCSK)	✓	✓	✓		
Certified Information System Auditor (CISA)	✓	✓	✓	✓	
Certified in Risk and Information Systems Control (CRISC)		✓		✓	
Offensive Security Certified Professional (OSCP)		✓			
OSSTMM Professional Security Tester (OPST)		✓			

eLearnSecurity Certified Professional Penetration Tester (eCPPT Gold)		✓			
CompTIA Security+		✓			
CompTIA Cybersecurity Analyst (CySA+)		✓			
Advanced Cloud Security Auditing Course		✓			
Associate Business Continuity Professional		✓			
CDPSE Data Privacy Solutions Engineer		✓			
Certified Cyber Threat Intelligence Analyst		✓			
COBIT 5 Assessor		✓			
COBIT 5 Foundation		✓			✓
CSSLP - Certified Secure Software Lifecycle Professional		✓			
eJPT - Security Junior Penetration Tester		✓			
e-Security Administration v5		✓			
e-Security Agent building v5		✓			
e-Security Analysis v5		✓			
eWPT - Security Web Application Penetration Tester v1.0		✓			
GIAC Response and Industrial Defense - GRID		✓			
GIAC Certified Incident Handler (GCIH)	✓				
Certified Intrusion Analyst (GCIA)	✓				
GIAC Penetration Tester (GPEN)	✓				

Certificazioni vendor	TIM	AlmavivA	NETGROUP	KPMG	REEVO
Splunk	✓	✓			
IBM	✓	✓	✓		✓
Oracle	✓	✓	✓		
Fortinet	✓	✓	✓		
Checkpoint	✓	✓	✓		
PaloAlto	✓	✓			
CISCO	✓	✓	✓		✓
FireEye		✓	✓		
CrowdStrike		✓			
Forcepoint	✓	✓	✓		✓
Citrix	✓	✓	✓		✓
Skybox		✓			✓
McAfee	✓		✓		
Kaspersky	✓	✓	✓		
Broadcom (Symantec/CA)	✓	✓			
Cyberark		✓		✓	
RSA		✓	✓	✓	
Rapid7					
Tenable		✓			
TrendMicro	✓	✓	✓		
Microsoft	✓	✓	✓	✓	✓
Wallix		✓			
Symantec		✓			
CA(Computer Associate)		✓			
PenTera		✓			
Qualys		✓			

Verisign		✓			
Informatica		✓			
Google	✓	✓	✓		
AWS	✓	✓	✓		✓
Forescout					✓
Darktrace					✓
Watchguard					✓
Sophos					✓

Tabella 4 - Certificazioni del RTI

Il RTI, anche grazie alla ridondanza di competenze, è in grado di assicurare massima **flessibilità** per far fronte sempre e comunque a cambiamenti nel contesto normativo, organizzativo, tecnologico e funzionale di Consip e/o delle PA e per rispondere ad esigenze particolari e di picco che possano presentarsi nell'arco della durata contrattuale. Per questo motivo la ripartizione delle attività tra le Aziende del costituendo RTI tiene conto delle specifiche specializzazioni aziendali, ma prevede, anche, un coinvolgimento multiplo sui diversi servizi per facilitare la rimodulazione e l'adattamento dell'organizzazione all'interno del RTI stesso in determinati momenti di criticità. La ripartizione delle attività di ciascun CE tra le Aziende in RTI avverrà sulla base dei seguenti criteri:✓Ambito di servizio richiesto;✓Competenze specialistiche sulle tecnologie oggetto dei servizi previsti;✓Conoscenza pregressa dell'organizzazione e dei processi operativi delle Amministrazioni.
Per quanto attiene gli ambiti e l'erogazione dei servizi, nella tabella seguente si indicano le aziende coinvolte. Il comitato di Governance del RTI definirà, sulla base delle specificità del singolo contratto, l'effettiva ripartizione dei singoli servizi tra le aziende del RTI e definirà il Responsabile del Contratto Esecutivo.

Servizio / Azienda	Governance AQ	Governance CE	Innovazione	HD	L1.S1	L1.S2	L1.S3	L1.S4	L1.S5	L1.S6	L1.S7	L1.S8	L1.S9	L1.S10	L1.S11	L1.S12	L1.S13	L1.S14	L1.S15
TIM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AlmavivA		✓	✓				✓	✓	✓		✓		✓	✓					✓
KPMG			✓					✓	✓				✓						✓
Netgroup			✓		✓								✓						✓
ReeVo			✓																✓

Tabella 5 – Ripartizione dei servizi/ambiti

3.3. RISORSE E STRUTTURE AGGIUNTIVI PROPOSTI E MODALITÀ DI INTERAZIONE CON L'AMMINISTRAZIONE

Con riferimento al modello organizzativo descritto nei precedenti paragrafi, si evidenziano i **ruoli e le strutture aggiuntive** a supporto delle figure di responsabilità richieste espressamente nel Capitolato.

Ruoli Aggiuntivi	Strutture aggiuntive
Referente Innovazione Tecnologica; Responsabile Supporto all'Adesione; Responsabile Centro Servizi; Coordinatori Data Center; Coordinatore Help Desk; Responsabile Logistica; Responsabile per ogni servizio; Capi Progetto; Transition Manager	Contract Management; Risk Management; Quality Management; Regulatory Support; Resource Management; Program Management Office (PMO); Unità Locale di Sicurezza (ULS); Knowledge AQ & Content Management; Innovation Hub e PNRR

Tabella 6 – Ruoli e Strutture aggiuntive proposte dal RTI

Risorse aggiuntive

Oltre ai ruoli ed alle strutture sopra riportate il RTI rende disponibile il supporto dei propri centri di competenza e delle relative risorse che partecipano a laboratori oltre che a collaborazioni con il mondo accademico ed enti di ricerca.
In particolare, TIM ha avviato il programma **UniversiTIM** con lo scopo di creare un ecosistema con il mondo accademico finalizzato ad una collaborazione strutturata e organizzata negli stream della ricerca.
TIM collabora con l'Agenzia Europea dedicata alla Cyber Security (**ENISA**) sui seguenti ambiti: ✓**Threat Intelligence Platform**: sperimentazione con un apposito Pilot di metodi innovativi per l'individuazione e la gestione delle minacce tipiche del mondo Telco; ✓Meccanismi di protezione da attacchi di tipo **Distributed Denial of Service** (**DDoS**): sperimentazione di strumenti innovativi sviluppati all'interno del progetto per la definizione e condivisione di specifiche "firme" di attacco che possano essere utilizzate per istruire, anche in modo automatico, gli strumenti di protezione da tali attacchi (es. firewall); ✓Analisi delle minacce emergenti, in particolare rispetto ai nuovi scenari introdotti dal 5G.
La collaborazione di TIM con il Politecnico di Torino sul tema del **Quantum Computing** (**QC**) è focalizzata sullo studio di modelli di algoritmi di **Artificial Intelligence** e **Machine Learning** e analizza il tema della **Quantum Communication** nella sua molteplicità, con particolare attenzione al livello applicativo per la **crittografia quantistica**.

AlmavivA è partner principale dell'**Osservatorio Cyber Security & Data Protection** del Politecnico di Milano all'interno di diversi gruppi di lavoro, con particolare attenzione a trend di mercato e use case aziendali in ambito Privacy, ai modelli organizzativi e alle nuove competenze, all'offerta tecnologica, alla filiera di soluzioni e servizi di Sicurezza ICT, alle modalità di gestione del rischio cyber e ai temi di conformità normativa.

AlmavivA dispone di **laboratori**: ✓sull'applicazione di soluzioni di Web Application Firewall, in cui si approfondiscono con particolare attenzione gli aspetti applicativi della protezione dei servizi WEB esposti in rete in funzione della costante evoluzione delle minacce cibernetiche; ✓per il Mobile Security Assessment che permette, tramite dispositivi dedicati fisici con framework di sviluppo, l'emulazione di dispositivi mobili con sistema sia Android sia iOS, virtualizzando dunque l'accesso al sistema operativo senza le limitazioni imposte dai produttori.

TIM, AlmavivA e Netgroup fanno parte del **Centro di Competenza nazionale ad alta specializzazione per la Cyber Security CYBER 4.0**, finanziato dal Ministero dello Sviluppo Economico. Tale centro è espressione di un partenariato pubblico e privato, interdisciplinare e multi-attoriale, che copre un ampio spettro di competenze e favorisce lo sviluppo di una rete di collaborazioni qualificate e mira a sviluppare la competitività del sistema Paese offrendo, in particolare, alla Pubblica Amministrazione servizi di formazione e finanziando progetti di ricerca e innovazione per innalzare il livello di protezione dal rischio di attacchi cyber a sistemi, processi e asset strategici nazionali. Il RTI è anche impegnato nel selezionare, accelerando e co-creando idee, prodotti e servizi innovativi provenienti dal mondo delle startup. Ad esempio, il **TIM WCAP** (**Working Capital**) distribuito su cinque hub territoriali (Milano, Bologna, Roma, Napoli e Catania), favorisce una contaminazione tra le **startup**, i **produttori di tecnologia**, i principali **Atenei** ed i **Centri di Ricerca** italiani.

Modello di relazione con le Amministrazioni contraenti

Le figure di riferimento del RTI interagiscono con i referenti della PA contraente sulla base dei rispettivi ruoli e responsabilità. Il modello prevede un *numero ben delimitato di interfacce*, ciascuna in possesso delle conoscenze e dell'autorità specifica per il ruolo, allo scopo di **massimizzare l'efficienza** *e* **l'efficacia del governo della fornitura**.

Come rappresentato in figura, l'interazione fra RTI e PA passa principalmente per quattro figure o funzioni:

- **RUAC del CE** – per gli aspetti generali della fornitura e specificamente per gli aspetti contrattuali e amministrativi;
- **Responsabile Tecnico** – per tutto quanto riguarda l'andamento dei servizi e delle attività progettuali;
- **Capo Progetto** – per gli aspetti specifici riguardanti le attività dei servizi specialistici;
- **Help Desk** – per l'assistenza informativa, amministrativa e tecnica.

A questi si aggiunge l'interazione fra il **Transition Manager** del RTI e i Referenti dell'Amministrazione durante i soli periodi di presa in carico dei servizi e di phase out. Tutti i ruoli, le strutture e le risorse aggiuntive proposte dal RTI potranno essere coinvolti, per il tramite del Referente Tecnico, nei casi in cui le PA contraenti necessitino di un supporto su una tematica particolarmente complessa.

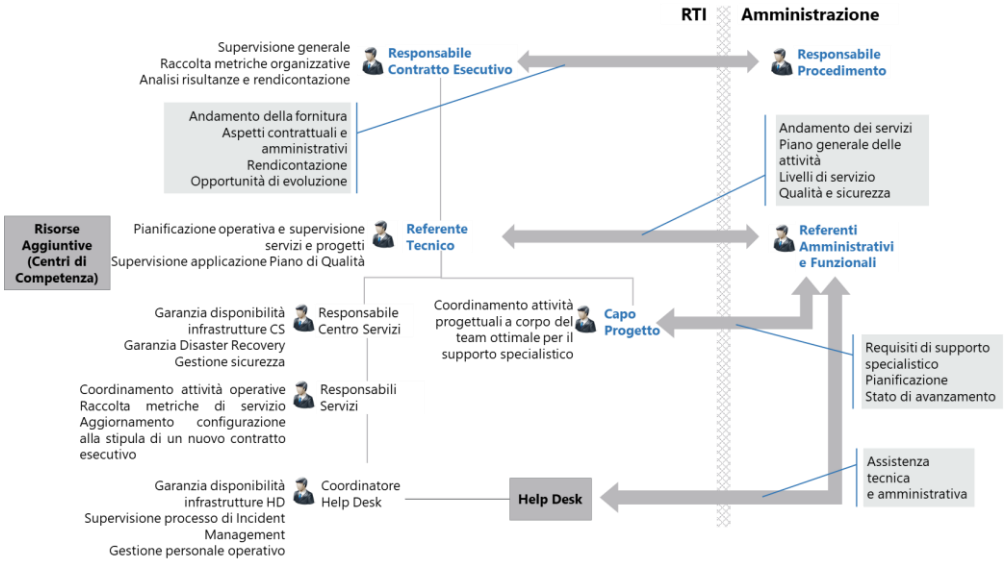

Figura 4 – Modello di relazione

4. PROPOSTA PROGETTUALE PER I "CENTRI SERVIZI"

Il RTI metterà a disposizione una soluzione organizzativa basata su un **Centro Servizi Virtuale**, distribuito su più **Data Center** (DC) e **Control Room** (CR), attivo e presidiato in modalità continuativa (H24x7) da personale qualificato e certificato e in grado di gestire i servizi contrattualizzati dalle Amministrazioni nell'ambito dell'AQ.

4.1. CARATTERISTICHE TECNOLOGICHE E MODALITÀ OPERATIVE DI FUNZIONAMENTO DEI CENTRI SERVIZI

Il Centro Servizi Virtuale è distribuito sul territorio nazionale ed organizzato sulle seguenti componenti:

- **Data Center,** dotati d'infrastrutture hardware/software con elevatissimi livelli di affidabilità, disponibilità e sicurezza dove sono ospitate le piattaforme per l'erogazione e la gestione dei servizi previsti nell'AQ;
- **Control Room,** costituite da personale altamente specializzato distribuito su più sedi per garantire la massima affidabilità e flessibilità nella gestione dei servizi previsti.

Dispone, inoltre, di una **piattaforma strumentale altamente integrata** che abilita i processi in maniera agile e ne garantisce la continuità operativa, attraverso i meccanismi di protezione dei DC e le tecnologie adottate a supporto dei processi di Disaster Recovery, e di **un'organizzazione di risorse capaci ed interconnesse digitalmente** in grado di sostenere il servizio anche in condizioni di picco o di indisponibilità di una o più CR grazie a tecniche di shadowing, multidisciplinarietà, training on the job, etc. La molteplicità di DC di cui dispone il RTI testimonia l'esperienza e la consolidata capacità operativa delle aziende raggruppande. Ricordando la modalità "managed" di erogazione dei servizi e la loro criticità, la soluzione scelta per il Centro Servizi è disegnata complessivamente sui 6 poli geografici riportati in tabella ed è in grado di offrire la massima flessibilità operativa e solidità all'intera fornitura. Al fine di garantire le Amministrazioni da eventuali picchi di lavoro, il RTI ha previsto di distribuire ogni servizio tra 2 DC Primari (Acilia e Casal Boccone) e 2 secondari di DR (Rozzano e Milano) ad eccezione dei servizi di Firma Digitale Remota, Sigillo Elettronico, Timbro Elettronico e Validazione Temporale Elettronica

Qualificata che sono erogati dalla sola mandataria attraverso l'utilizzo di un sito Primario (Pomezia) e un sito Secondario per la continuità operativa (Roma Oriolo) dedicati e certificati per i servizi fiduciari.

Nella tabella che segue è indicata l'ubicazione geografica dei DC che saranno utilizzati e l'azienda responsabile del loro funzionamento operativo.

Il modello di erogazione dei servizi prevede un'infrastruttura di erogazione dedicata alla PA all'interno di ciascuno dei DC, sia Primari che Secondari. **Tutti i Data Center sono certificati ISO/IEC 27001**.

Il monitoraggio e la gestione dei servizi richiesti in AQ sono erogati attraverso personale qualificato e certificato dislocato presso le seguenti Control Room (CR) del RTI:

- **Control Room Sud** distribuita sulle sedi di Bari - Piazzale Mater Ecclesiae 5 - e di Taranto – via Campania 11;
- **Control Room Centro** sulla sede di Roma – via di Scalo Prenestino 15.

Azienda	Città	Indirizzo
TIM	*Acilia*	Via di Macchia Palocco, 223 (RM)
	Rozzano	Viale Toscana, 3/5 (MI)
	Pomezia	SS148 Pontina km.29,100 (RM)
	Roma Oriolo	Via Oriolo Romano, 257 (RM)
ALMAVIVA	*Roma Casal Boccone*	Via di Casal Boccone, 188 (RM)
	Milano	Via dei Missaglia, 97 - ed. B4 (MI)

Tabella 7 – DC a disposizione del RTI

Tali CR operano ripartendosi le attività in funzione del carico di lavoro e delle specifiche competenze richieste in sede di ciascun contratto esecutivo. La scelta di separare fisicamente le CR dai Data Center è funzionale alla necessità di garantire la continuità operativa, disaccoppiando le infrastrutture a supporto dagli operatori che le gestiscono/utilizzano, minimizzando così gli impatti di eventuali fault di una delle sedi. Inoltre, i siti sono connessi fra loro attraverso la **VDCN** di TIM (Virtual Data Center Network), rete di trasmissione dati IP/MPLS ad altissima velocità (10 Gbps scalabili a multipli di 10) che abilita sia la connettività per l'erogazione dei servizi sia l'allineamento fra i DC del RTI. L'infrastruttura di routing ha una capacità di forwarding di 100 Gbps e rende tutto il modello di servizio *un unico grande centro "virtuale" di erogazione.* In conclusione, la soluzione consente di ottimizzare sia il traffico fra i sistemi, sia il traffico di gestione, specializzando l'erogazione di servizi in funzione della distribuzione delle risorse rispondendo pienamente ed efficacemente a possibili situazioni di indisponibilità e garantendo la *totale continuità del servizio*. Tutti i DC messi a disposizione dal RTI sono già collegati sia ad Internet, tramite due differenti Service Provider afferenti a due POP attraverso percorsi differenziati, sia alla rete **SPC**, il che li rende, dal punto di vista della rete, immediatamente disponibili ad erogare i servizi del presente AQ alle PA.

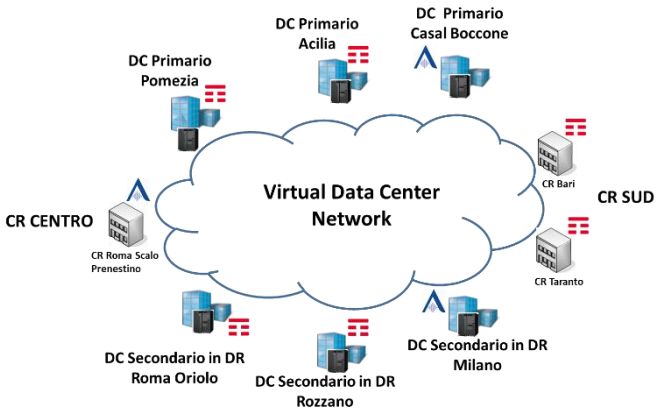

Figura 5 – Architettura Centro Servizi Virtuale

I Centri Servizi ausiliari

Il modello di servizio previsto dal RTI viene completato dai Centri Servizi ausiliari dislocati sul territorio italiano e focalizzati sulla gestione delle piattaforme tecnologiche e ai servizi infrastrutturali (backup, monitoraggio, disaster recovery, etc.) interne alle aziende del RTI. I Centri Servizi ausiliari disponibili sono:

- **Information Technology Operation Center (ITOC)** per la gestione sistemistica delle piattaforme e dei servizi infrastrutturali;
- **Network Operation Center (NOC)** per le attività di supervisione proattiva/reattiva della connettività dei DC;
- **Security Operation Center (SOC)** per le attività specialistiche volte ad assicurare una corretta gestione delle configurazioni dei sistemi di sicurezza fisica e logica dei DC e delle CR del RTI;
- **Data Center Services (DCS)** per le attività di monitoraggio, gestione e configurazione delle infrastrutture dei DC.

4.1.1. Sicurezza del Centro Servizi

Di seguito vengono descritte le misure di sicurezza distinte per ambito specifico (fisico, logico ed organizzativo) che il RTI intende mettere a disposizione dell'Amministrazione.

Sicurezza Fisica

Sistemi per il controllo accessi: presenti in tutti gli ambienti e strutture critiche con adeguato livello di sicurezza. Il RTI fornisce sia tecniche di Anti pass-back, che prevengono potenziali abusi nell'utilizzo dei badge personali, sia di Anti piggy-backing, che evitano l'accesso fraudolento mediante accodamento al passaggio di un utente autorizzato. Oltre al sistema di riconoscimento tradizionale, mediante un badge personale, il RTI prevede l'inserimento di un badge biometrico, attraverso un Badge MIFARE® contenente l'impronta digitale dell'assegnatario. Inoltre, il RTI garantisce l'**antintrusione** mediante un muro di cinta sormontato da barre di acciaio, con accessi carrai controllati da un servizio di guardiania armata del Comprensorio che opera h24, 7 giorni su 7 e da un sistema antintrusione perimetrale a microonde e raggi infrarossi. In aggiunta, il RTI prevede un sistema di videosorveglianza evoluto controllato dal servizio di guardiania operante H24 7/7. In particolare, il DC di Acilia, certificato Tier IV, è dotato di un sistema di sicurezza perimetrale con rilevamento automatico delle intrusioni, geolocalizzazione e tracking degli intrusi con Radar Navtech e telecamere termiche intelligenti Sightlogix integrate con la piattaforma di Video Management. Tale piattaforma è in grado di garantire la sicurezza su aree molto ampie, in qualsiasi condizione ambientale, e di rilevare una persona fino a 1000m di raggio, un veicolo fino a 2000m di raggio e di fornirne la posizione GPS seguendone i movimenti su una mappa con tracking automatico.

Rack: Gli apparati sono alloggiati in rack normalmente accessibili attraverso l'utilizzo di chiavi. In alcuni casi è prevista la messa in sicurezza dei rack (o delle **Cage**), attraverso l'impiego di sistemi biometrici di controllo accessi. È possibile inoltre allestire **Suite** delimitate da pareti grigliate accessibili tramite badge al solo personale autorizzato.

Continuità elettrica: il RTI garantisce la disponibilità di stazioni di trasformazione dell'energia elettrica dedicate alimentate da un consorzio di fornitori, da quadri elettrici ridondati, da gruppi di continuità (in ridondanza N+1) che entrano a regime in meno di un minuto in caso di black-out e da batterie di backup per la gestione del transitorio fino all'attivazione dei gruppi di continuità. Gli impianti elettrici (fino alla singola presa di alimentazione del rack) sono presidiati H24 per 365 giorni l'anno e controllati tramite un **Building Management System centralizzato**.

Rilevatori antifumo e antincendio: sono presenti, in tutti gli ambienti, rilevatori antifumo e antincendio con attivazione automatica dei relativi impianti di spegnimento degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. La rilevazione fumi è garantita da un impianto con sensori ottici posizionati sottopavimento, in ambiente e nel controsoffitto. Sono presenti anche mezzi estinguenti mobili e un impianto fisso ad idranti, ed un sistema di ricircolo dell'aria primaria che si aziona automaticamente in caso di allarme incendio.

Antiallagamento: sono presenti sonde in grado di rivelare la presenza di liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua e pompe elettriche in grado di convogliare e scaricare all'esterno perdite di acqua.

Sicurezza Logica

Ad ogni Amministrazione contraente, il RTI garantisce l'isolamento e la protezione dei dati. Le tematiche di gestione del rischio e della compliance vengono indirizzate attraverso:

- processi di Gestione della Sicurezza, che saranno descritti in dettaglio nel relativo Piano;
- corretta gestione dei profili di accesso di tipo amministrativo assegnati da specifica struttura organizzativa separata da quelle deputate alla gestione tecnica dei sistemi, in conformità al Provvedimento del Garante Privacy 1.6.2006;
- rispetto degli obblighi di legge previsti dal Testo Unico in materia di privacy – D.Lgs. 196/03;
- conformità agli standard internazionali di sicurezza e alle best practice richiamate anche dall'ISO27001 in materia di User Access Management;
- framework documentale interno per la descrizione di policy e linee guida di riferimento; nello specifico tutte le aziende del RTI utilizzano un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme allo standard ISO/IEC 27001, per assicurare la protezione, l'affidabilità, la riservatezza e l'integrità delle informazioni delle Amministrazioni, il patrimonio intellettuale, le attività e le informazioni affidate da terzi.
- conformità alle linee guida di riferimento emanate dagli enti internazionali che si occupano di sicurezza informatica, quali ad esempio il National Institute of Standards and Technology (NIST), la European Union Agency for Network and Information Security (ENISA).

I processi rispettano i principi generali stabiliti da tali norme, quali l'univocità degli identificativi personali, il minimo privilegio secondo le funzioni svolte, la tracciabilità delle operazioni, la separazione dei ruoli a livello funzionale o individuale, la riservatezza delle informazioni, la protezione di dati e sistemi attraverso meccanismi di segregazione a più livelli. In particolare, gli accessi ai sistemi da parte del personale tecnico vengono tracciati attraverso un sistema di Security Log Management e conservati secondo quanto previsto dalle normative correnti in materia di sicurezza.

Sicurezza Organizzativa

Al fine di garantire un'organizzazione dei Centri Servizi sicura ed efficace, il RTI prevede la condivisione di **Procedure di escalation a fronte di eventi di fault o anomalie** con impatto rilevante sull'operatività del DC. Una volta innescata la procedura di escalation, i responsabili operativi impegnati nella risoluzione del problema mantengono costantemente aggiornati i livelli superiori coinvolti. Le informazioni pervenute sono analizzate al fine di stabilire se il livello di criticità raggiunto è tale da richiedere il coinvolgimento dei Responsabili dei Centri Servizi. Sono previste anche **Procedure di backup & restore** specifiche per le piattaforme applicative installate presso i DC a supporto dell'erogazione dei servizi di AQ. Il RTI prevede, infine, un **Piano di Disaster Recovery.** Per questo motivo, il RTI ha individuato DC Secondari distanti più di 200Km dai Primari nei quali replicare infrastrutture e dati necessari a garantire la continuità operativa anche a fronte di eventi disastrosi che colpiscano una significativa area geografica. Il suddetto piano prevede:

- tecniche di ridondanza delle infrastrutture IT (connettività, sistemi elaborativi e sistemi di storage duplicati con tecniche di clusterizzazione, mirroring, virtualizzazione, etc.) che garantiscono un alto grado di resilienza all'insorgere di guasti;
- backup dei dati delle PA sia su infrastrutture di storage poste in ambienti separati dei DC con garanzia di elevata protezione fisica, sia su copie di sicurezza trasferite su altri DC del RTI sempre all'interno del territorio comunitario;
- replica asincrona tra gli storage dei siti di produzione e di DR.

4.2. CARATTERISTICHE INFRASTRUTTURALI E LOGISTICHE A SUPPORTO DELL'IMPATTO AMBIENTALE

Caratteristiche logistiche e infrastrutturali

I DC proposti dal RTI per la fornitura sono tutti **Tier III** ad eccezione del DC TIM di Acilia classificato **Tier IV**. Complessivamente dispongono di migliaia di metri quadri di sale sistemi e sale TLC. Le sale sistemi sono predisposte in modo modulare e consentono sia l'hosting "intensivo" dei sistemi sia la configurazione rapida di spazio ad-hoc. Sono presenti inoltre aree magazzino, sale ignifughe (Lampertz) per la conservazione di dati sensibili ed ambienti predisposti ad ufficio. In particolare, il DC di Acilia garantisce una disponibilità del 99,995% equivalente a 26 minuti di fermo ammissibili all'anno.

Soluzioni a supporto dell'impatto ambientale

I DC proposti dal RTI sono stati progettati, realizzati e gestiti ponendo attenzione ad aspetti ambientali che non si riducono alla sola efficienza energetica ma anche ad aspetti puramente volti al rispetto e alla tutela ambientale. TIM, così come tutto il RTI, ha un ruolo fondamentale nel contribuire allo sviluppo sostenibile ovvero al processo di cambiamento tale per cui lo sfruttamento delle risorse, la direzione degli investimenti, l'orientamento dello sviluppo tecnologico e i cambiamenti istituzionali siano orientati ad eliminare o a ridurre al minimo, ove ciò sia attuabile, gli impatti negativi sull'ecosistema generati dalle proprie attività. TIM si è dotata di un **Sistema di Gestione Ambientale** conforme alla norma **UNI EN ISO 14001** ottenendo la relativa certificazione. TIM ha inoltre ottenuto la certificazione del **Sistema di Gestione dell'Energia** in conformità con la norma **UNI EN 50001**. Nel 1996 TIM è stata uno dei fondatori del Corporate Responsibility Charter dell'ETNO; nel 2002 ha sottoscritto il Global Compact delle Nazioni Unite, che invita ad adottare un approccio responsabile favorendo lo sviluppo e la diffusione di tecnologie ecosostenibili; nel 2009 è stata tra i fondatori dell'iniziativa JAC (Joint Audit Cooperation) attraverso cui viene valutata la performance di sostenibilità dei fornitori strategici mediante audit di terze parti; nel 2015 ha aderito all'organizzazione

internazionale Global e-Sustainability Initiative che rappresenta il riferimento in merito alla sostenibilità nel settore specifico dell'ICT. Nel rispetto di tali impegni i DC di TIM sono gestiti nel segno dell'efficienza energetica e della sostenibilità ambientale che si traduce in: ✓sostituzione degli apparati più datati con nuovi meno energivori; ✓l'utilizzo di Evaporative Free Cooling, che garantisce una maggiore resilienza operativa; ✓DC costruiti e gestiti secondo principi "green" con le più avanzate tecniche di raffreddamento, ma anche soffitti e mura in grado di gestire al meglio la temperatura; ✓l'impiego di batterie agli ioni di litio al posto di quelle al piombo; ✓l'impiego di luci LED a basso consumo energetico etc. In particolare, all'interno del DC di Acilia, certificato Tier IV, l'impianto di refrigerazione è affiancato da un innovativo **sistema green** che immette all'interno aria fresca e disperde nel sottosuolo, a 30 mt di profondità, il calore in eccesso prodotto mediante un sofisticato impianto geotermico (**dispersori geotermici**), ed inoltre i servizi di alimentazione ausiliari del DC sono alimentati ad energia solare. Tali accorgimenti tecnologici innovativi consentono al DC di Acilia di raggiungere un livello di efficienza energetica PUE (**Power Usage Effectiveness**) pari a **1,3** riducendo significativamente la quantità di emissioni di gas. TIM pone grande attenzione anche all'aspetto ambientale di tutela del territorio su cui vengono realizzati i propri DC: dai sistemi di raccolta delle acque pluviali, al materiale drenante per il suolo su cui vengono costruiti, dalle vernici mangia-smog e battericide, a sistemi di illuminazione intelligenti, fino all'adozione di piccole famiglie di animali autoctoni per limitare l'impatto delle costruzioni sull'ambiente. I Data Center AlmavivA possiedono caratteristiche infrastrutturali che garantiscono elevati livelli di affidabilità, disponibilità e sicurezza dei servizi erogati, sono certificati ISO 27001, ISO 22301 per la Business Continuity, ISO 50001 per l'Efficienza Energetica e ISO 14001 per la Sostenibilità Ambientale.

Particolare attenzione è dedicata alla sostenibilità ambientale, perseguita attraverso l'accurato e costante controllo dei consumi elettrici, monitorati con l'indice di efficienza energetica **PUE** (**Power Usage Effectiveness**) paria **1,3**, e la riduzione delle emissioni di gas serra, attraverso l'utilizzo ad esempio di tecnologie di estinzione incendi innovative, il tutto monitorato con l'indicatore di sostenibilità **CUE** (**Carbon Usage Effectiveness**). La gestione efficiente dell'energia è testimoniata dalla certificazione ISO 50001 delle due sedi di Roma e della sede di Milano Missaglia.

4.3. HELP DESK – CARATTERISTICHE ORGANIZZATIVE, METODOLOGICHE, TECNICHE, DIMENSIONALI E FORMATIVE

La soluzione proposta dal RTI per il servizio di Help Desk (HD) deriva dall'esperienza maturata nel recente passato nella gestione di convenzioni e contratti quadro con AgID e Consip. Tutti gli aspetti del servizio, sia organizzativi sia tecnici, soddisfano i requisiti di gara e tengono conto delle best practice operative nel trattamento dei tipici casi d'uso nella PA.

Aspetti organizzativi e metodologici

Il servizio di Help Desk, erogato secondo la metodologia ITIL, è strutturato in modo da indirizzare adeguatamente le richieste di ogni singola Amministrazione contraente in modo specifico e contestualizzato. L'Help Desk è accessibile attraverso un'infrastruttura multicanale, in grado di gestire i contatti in modo unificato e omogeneo. I diversi canali di accesso disponibili sono integrati in un modello unico di trattamento, in cui le segnalazioni vengono indirizzate a diversi gruppi specializzati di operatori utilizzando politiche "intelligenti" di instradamento.

Il supporto fornito dall'HD si articola su due livelli logici, entrambi in grado di soddisfare:

1. richieste di tipo *informativo*, provenienti da PA che non hanno ancora aderito ai servizi dell'AQ;
2. richieste di tipo *amministrativo*, provenienti da PA già contraenti, su aspetti legati alla conduzione del contratto;
3. richieste di tipo *tecnico*, provenienti da PA contraenti che abbiano la necessità di avere sia un supporto sull'utilizzo dei servizi dell'AQ, sia di segnalare malfunzionamenti o eventuali incidenti di sicurezza.

Le richieste di tipo 1 sono disponibili a tutte le PA, mentre quelle di tipo 2 e 3 richiedono un *PIN di riconoscimento*, assegnato alle PA alla stipula del contratto.

L'**HD di 1° livello**: ✓assicura la comunicazione tempestiva ed efficace con i referenti delle PA; ✓riceve, registra le chiamate/e-mail dei referenti e comunica il codice identificativo del ticket; ✓assiste le PA per ciò che riguarda le attività propedeutiche alla sottoscrizione dei contratti; ✓classifica la richiesta fornendo direttamente una soluzione per i problemi non complessi o smista la richiesta al 2° livello; ✓controlla lo stato di avanzamento del ticket e informa il referente PA; ✓produce ed analizza le statistiche sugli interventi, per identificare i fabbisogni e definire azioni di prevenzione dei problemi.

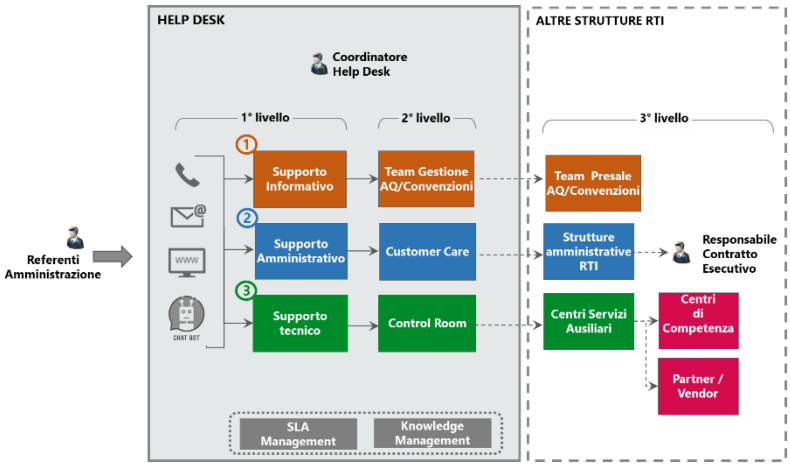

Figura 6 - Schema organizzativo generale dell'Help Desk

Le funzioni di ***2° livello*** dell'**HD** sono svolte da:

- **Team Gestione AQ/Convenzioni** che fornisce informazioni sull'AQ prima dell'adesione e supporto per compilare il Piano dei Fabbisogni;
- **Customer Care** che fornisce supporto su aspetti amministrativi dei contratti esecutivi stipulati;
- **Control Room** che fornisce assistenza ai referenti tecnici delle PA sulle segnalazioni di fault sui servizi acquisiti.

La struttura è completata da una funzione di **Knowledge Management**, che si fa carico di alimentare la Knowledge Base del servizio sulla base delle segnalazioni dei team operativi di supporto, secondo i meccanismi organizzativi e operativi descritti di seguito e da una funzione di **SLA Management** che monitora la qualità del servizio erogato rispetto ai livelli di servizio contrattualizzati, individuando situazioni potenzialmente critiche e identificando le azioni correttive intese ad assicurare che gli SLA vengano soddisfatti. Gli orari e le modalità di erogazione del servizio sono rispondenti ai requisiti di Capitolato.

Caratteristiche tecniche: infrastruttura tecnologica, modalità di accesso, strumenti a supporto

La soluzione infrastrutturale proposta dal RTI, per fornire il servizio di HD, è basata su un modello di servizio di tipo Hosted Contact Center (HCC) che utilizza le stesse funzionalità di Accoglienza e Routing Operatore dei Contact Center che TIM utilizza per fornire servizi di accoglienza ai propri Clienti. Le principali caratteristiche dell'infrastruttura sono: ✓**Scalabilità** che consente di inserire rapidamente nuove postazioni operatore che necessitano solo di un

PC e un telefono; ✓**Interoperabilità** che consente di integrare i diversi moduli che compongono l'infrastruttura anche con sistemi esterni grazie alla disponibilità di librerie e interfacce standard; ✓**Affidabilità**: garantita dalla replica delle componenti dell'infrastruttura per consentire la normale esecuzione del servizio in caso di fault.

L'infrastruttura di servizio si divide in 3 principali macro-blocchi:

- **Canali di accesso al servizio** di HD schematizzati nella figura 6:
  - **canale telefonico**, attraverso numero verde dedicato, con tre post-selezioni gestite tramite IVR per avere subito accesso all'operatore di 1° livello con le competenze richieste;
  - **canale e-mail** attraverso la configurazione di una casella e-mail dedicata e riservata all'AQ*;*
  - **canale web**, corrispondente alla funzionalità di self-ticketing accessibile attraverso il Portale della Fornitura, (cfr. Cap.16).

  Come **funzionalità aggiuntiva**, allo scopo di incrementare l'efficacia e l'efficienza dei servizi di HD per le PA contraenti, il RTI potrà rendere disponibile dal Portale della Fornitura, come ulteriore canale di accesso, una **ChatBot** che utilizza algoritmi di intelligenza artificiale per sostenere un dialogo strutturato con l'utente. Tale strumento si è dimostrato estremamente efficace in contesti analoghi come chiave di accesso per un'interazione rapida ed immediata degli utenti con il servizio di HD. La ChatBot incorpora funzioni di Machine Learning, dunque apprende dalle interazioni con gli utenti e dai comportamenti di quest'ultimi per fornire risposte rapide e precise, automatizzando quindi una serie di attività e offrendo un primo livello di assistenza.
- **Funzionalità Automatiche di Accoglienza (IVR)**, permette velocità e flessibilità nel disegno, messa in esercizio e gestione degli alberi di navigazione e dei contenuti vocali;
- **Motore di Routing Multicanale**, basato su tecnologia **Genesys**, che abilita il routing dei contatti in modalità Blending, ovvero combinando in automatico la distribuzione dei canali di accesso sincroni (Voce, Chatbot) con i canali asincroni (Mail, Web) in modo tale che l'operatore possa gestire contemporaneamente, ad esempio, sia il canale voce sia il canale mail.

Lo strumento principale utilizzato dagli operatori a supporto del servizio di HD è la **piattaforma ITSM BMC Remedy** che consente di definire i diversi processi ITIL secondo meccanismi di workflow, che ingaggiano le varie funzioni operative dell'organizzazione a seconda del trattamento richiesto, con meccanismi di escalation sui vari livelli in presenza di situazioni critiche. La piattaforma BMC Remedy: ✓supporta tutti i processi di acquisizione e gestione delle richieste e degli incidenti; ✓**consente la gestione centralizzata degli asset IT** e delle relative informazioni tecniche ed amministrative attraverso il modulo della suite BMC di **Asset & Configuration Management** e sulla base delle informazioni contenute nell'**Atrium CMDB**; ✓implementa la base di conoscenza della fornitura attraverso modalità multiple di classificazione e indicizzazione dei contenuti; ✓consente ai referenti di inserire richieste verso l'HD utilizzando il tool di **self ticketing** accessibile dal Portale della Fornitura anche per verificare lo stato delle richieste pendenti; ✓consente di distribuire, grazie al motore di workflow interno, le attività lungo l'organizzazione e monitorarne l'esecuzione, per massimizzare l'efficienza del processo.

Dimensionamento dei gruppi di supporto

Il gruppo di lavoro preposto al servizio di HD (1° e 2° livello) sarà **dimensionato in modo dinamico**, in funzione del numero delle PA contraenti e del volume complessivo dei servizi sottoscritti. Le ipotesi dimensionali utilizzate si basano sulle numerose esperienze maturate dal RTI in analoghi servizi di HD gestiti in altri Accordi Quadro/Convenzioni; mensilmente, tale dimensionamento sarà rivisto dal Responsabile dell'HD in funzione dei seguenti parametri:

- Profili di traffico:
  1. Numero di contatti al mese: ✓**60%** da canali sincroni (telefono, chatbot); ✓**40%** da canali asincroni (e-mail, web).
  2. Distribuzione percentuale dei contatti sui tre gruppi di supporto: ✓Informativo **5%**, ✓Amministrativo: **25%**, ✓Tecnico: **70%**.
  3. Distribuzione del traffico sulle diverse fasce orarie: ✓**89%** Lun-Ven dalle ore 08:30 alle ore 17:30; ✓**7%** Sabato dalle ore 08:30 alle ore 13:30; ✓**4%** Lun-Ven dalle ore 17:30 alle ore 08:30, il Sabato dalle ore 13:30 alle ore 24:00, la domenica e nei giorni festivi.
- Parametri di Servizio:
  1. Tempo massimo di attesa netto per il servizio telefonico: **60 secondi nel 95%** dei casi (cfr. indicatore di qualità HDCG);
  2. Tempo di presa in carico di una singola richiesta: **10 minuti nel 95%** dei casi, (cfr. indicatore di qualità HDPC);
  3. Tempo di risoluzione delle richieste da parte dell'HD: in funzione della priorità assegnate, **4 ore nel 98%**, **8 ore nel 96%**, **12 ore nel 94%** dei casi (cfr. indicatore di qualità HDTR);
  4. Numero di chiamate perse: **2%** del numero totale delle chiamate ricevute dall'HD;
  5. Tipologia e complessità dei servizi previsti;
  6. Numero di richieste la cui gestione è demandata all'Help Desk di secondo livello;
- **Tempi Medi di Servizio (TMS)**: sono stati infine stimati i TMS differenziati in base ai tre diversi gruppi di supporto ed in particolare, per i contatti telefonici, sono stati considerati i seguenti valori: ✓Informativo: TMS pari a **400 secondi**; ✓Amministrativo: TMS pari a **460 secondi**; ✓Tecnico: TMS pari a **540 secondi**.

I TMS indicati tengono conto sia del "*trattamento del contatto*" stesso (**TMC** + **ACW** = **T**empo **M**edio **C**onversazione + **A**fter **C**all **W**orking) sia del "*tempo di inattività*" (tempo di ready) dopo la chiusura del contatto. Le differenze riportate per i diversi gruppi tengono conto delle specificità delle richieste e dell'andamento del traffico offerto.

Sulla base delle ipotesi descritte in precedenza, utilizzando i classici modelli di teoria delle code (formula di Molina inversa per il calcolo dei serventi necessari), sarà definito il dimensionamento, in termini di FTE, delle risorse necessarie per il corretto funzionamento del servizio di HD. Inoltre, a maggior garanzia della capacità di gestire i picchi di traffico, si sottolinea che il modello organizzativo proposto dal RTI per la struttura di HD, prevede un **Gruppo Regia** che monitora in tempo reale la curva del traffico offerto agli operatori ed è quindi in grado di implementare politiche di bilanciamento adattativo del carico di lavoro sulle code di operatore in tempi estremamente ridotti, sfruttando le caratteristiche di scalabilità della infrastruttura tecnologica.

Aspetti Formativi

Gli operatori dell'HD verranno formati per acquisire competenze su: ✓*tecniche di interazione* – accoglienza, gestione contatto, modalità di ascolto e dialogo, etc.; ✓processo di *gestione della richiesta* e *utilizzo della piattaforma* di Trouble Ticketing; ✓*tematiche di base* della fornitura – per tutti gli operatori di 1° livello; ✓*tematiche specialistiche* della fornitura (contrattuali, amministrative, tecniche) – per gli operatori di 2° livello, differenziate per ciascun gruppo.
La formazione sarà continua sulla base delle esigenze espresse e della gap analysis rilevata. Gli operatori verranno sottoposti a *quick test periodici* per misurare il loro livello di competenza ed evidenziare la necessità di cicli di formazione ulteriore. Gli operatori disporranno di: ✓"*Call Guide*" per i vari tipi di problematiche, per rendere più efficace il contatto e risolvere più velocemente le richieste degli utenti; ✓un sistema di Knowledge Base alimentato in modo incrementale, in cui gli operatori dell'Help Desk potranno memorizzare soluzioni per risolvere richieste ricorrenti o ripetibili, (le cosiddette "one call solution"), e limitare i trasferimenti al 2° livello.

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

Il RTI vanta una solida esperienza nell'erogazione di servizi SOC, anche per ambienti critici della PA. Elevati livelli di efficienza ed efficacia delle Security Operations sono raggiunti tramite la specializzazione sulle tecnologie e sui vendor di cui il RTI è partner, che consente agli operatori del SOC di gestire gli incident di sicurezza con maggior precisione e rapidità. Il servizio è finalizzato al monitoraggio e alla gestione continua, adeguatamente alle dimensioni ed alla complessità del perimetro, delle minacce che insistono sulle infrastrutture e sui dispositivi della PA.

Per il Servizio "Security Operations Center" (SOC) e per tutti i Servizi ad esso connessi o relazionabili, il RTI garantisce alle PA contraenti pieno supporto lungo tutto il **ciclo di vita** del servizio (*Service Lifecycle*), dalla fase iniziale di *Assessment* alla fase finale di *Decommissioning & Handover*.

Ciclo di vita del servizio SOC
Il piano di gestione del ciclo di vita del servizio proposto dal RTI e ampiamente collaudato dalle aziende raggruppande, si articola in cinque fasi principali, come di seguito illustrato:

1. **Fase di Assessment**: il fornitore provvede a raccogliere tutti gli elementi necessari per dimensionare e configurare al meglio il Servizio offerto, sulla base delle specificità tecniche e amministrative della PA contraente. A tale scopo, il Fornitore condurrà due distinte attività di Assessment:
   - *Assessment dei requisiti di missione e normativi*: sono raccolti e analizzati sia i requisiti derivanti dalla *mission* specifica della PA contraente, sia i requisiti derivanti dal quadro normativo generale e particolare in cui essa si trova ad operare. Le informazioni raccolte in questa fase contribuiscono a definire i criteri di *Incident Response* in base ai quali si dovrà, ad esempio, favorire la continuità nell'erogazione dei servizi IT coinvolti rispetto alla raccolta di evidenze forensi, o viceversa.
   - *Assessment dei requisiti tecnologici e architetturali*: sono raccolti e analizzati sia i requisiti derivanti dall'architettura generale del *landscape* IT della PA contraente (modelli di dispiegamento e modelli di servizio adottati, tipologia e capacità delle interconnessioni di rete, etc.), sia i requisiti derivanti dalle specifiche tecnologie impiegate (famiglie di sistemi operativi, tipologie di gestori di basi di dati, etc.). Le informazioni raccolte in questa fase contribuiscono a definire i metodi e le procedure più opportune per l'acquisizione degli eventi e per le attività di investigazione, contenimento e ripristino in caso di Incidente.
2. **Fase di Caratterizzazione**: il fornitore provvede a caratterizzare il Servizio SOC in funzione dei requisiti raccolti nella precedente fase di Assessment, definendo o adeguando opportunamente le policy, le procedure e i playbook di analisi e di risposta agli Incidenti per una data PA contraente, in base alle sue specificità. Questa fase prevede le seguenti sotto-fasi:
   - *Caratterizzazione organizzativa*: di concerto con il referente dell'Amministrazione contraente, i requisiti precedentemente raccolti vengono esaminati per determinare le priorità e gli obiettivi dell'Amministrazione e per confermare, ovvero adeguare, il modello di comunicazione e di cooperazione tra fornitore ed Amministrazione, unitamente a tutte le procedure da attivare in caso di Incidente sospetto o conclamato. In questa fase vengono identificate le potenziali frizioni organizzative e individuati i possibili rimedi.
   - *Caratterizzazione tecnica*: di concerto con il referente dell'Amministrazione contraente, le informazioni precedentemente acquisite vengono analizzate per determinare i metodi e le tecniche da adottare in sede di *onboarding*, nonché per definire le policy e le soglie da impiegare al fine di raggiungere il migliore equilibro tra efficacia nella *detection* e riduzione dei falsi positivi. In questa fase vengono intercettate le possibili limitazioni o incompatibilità tecniche e individuati i possibili workaround.
3. **Fase di Attivazione**: il fornitore provvede a eseguire quanto necessario per la corretta attivazione del Servizio, facendo sì che la successiva fase di piena operatività possa avviarsi nel rispetto delle esigenze e delle aspettative dell'Amministrazione contraente. La fase di Attivazione si suddivide in:
   - *Integrazione e Onboarding*: il fornitore provvede ad attivare l'interconnessione geografica tramite rete Internet e/o via rete SPC. Successivamente, con il supporto del referente dell'Amministrazione, il Fornitore procede con la fase di *onboarding* provvedendo alla configurazione delle componenti di inoltro degli eventi di sicurezza per gli apparati di sicurezza di proprietà della PA contraente, in modo da abilitare la raccolta continua degli eventi e delle informazioni di sicurezza. La fase di onboarding termina con l'applicazione delle policy e dei modelli SIEM e con la verifica e l'eventuale adeguamento delle procedure e dei playbook del SOAR, secondo quanto definito e approvato in sede di *Caratterizzazione Tecnica*.
   - *Collaudo e Accettazione*: di concerto con il referente dell'Amministrazione, il fornitore esegue il collaudo del Servizio allo scopo di confermare che sia stato configurato in accordo alle esigenze della PA e che operi secondo i livelli di performance attesi. La fase di collaudo prevede la verifica della piena raggiungibilità di tutti i nodi fisici e degli oggetti logici configurati, nonché la simulazione di un Incidente di sicurezza e della sua successiva gestione da parte di ciascun attore coinvolto, inclusi i referenti dell'Amministrazione. Eventuali eccezioni e non-conformità non sanabili in sede di collaudo saranno registrate e inserite nel documento di *User Acceptance*, unitamente al corrispondente piano di rimedio.
4. **Fase Operativa**: il fornitore assicura la quotidiana operatività del Servizio SOC secondo le buone pratiche di settore e in accordo ai dettami del Capitolato Tecnico, ai pertinenti Indicatori di Qualità e ai requisiti espressi dall'Amministrazione. La fase Operativa a sua volta si suddivide in:
   - *Event monitoring & Incident handling*: il Servizio SOC erogato dal fornitore presidia H24 l'identificazione e l'analisi degli eventi di sicurezza, assicurando il triage e la risposta agli Incidenti rilevati. In questa fase viene avviata, se prevista, un'interlocuzione d'urgenza con il referente dell'Amministrazione,

volta a confermare l'effettiva sussistenza dell'Incidente di sicurezza e a concertare il migliore corso di azione, al fine di rispettare le specifiche priorità della PA coinvolta (ad es. prediligendo la continuità del servizio IT interessato o il suo immediato ripristino rispetto alla preservazione delle evidenze forensi).

- *Incident containment & System recovery*: il personale del Servizio SOC, una volta confermato l'Incidente di sicurezza e stabilito l'opportuno corso d'azione, provvede a contenerne gli effetti (ad es. esfiltrazione dei dati, propagazione del codice malevolo, etc.) isolando, se necessario, i sistemi coinvolti. Laddove tecnicamente possibile, in assenza di vincoli di natura investigativa (preservazione delle evidenze di reato) e in accordo con l'Amministrazione, il personale del Servizio SOC provvede a supportare da remoto l'Amministrazione nel ripristinare l'integrità e la funzionalità dei sistemi colpiti, mediante l'eradicazione del codice malevolo e l'applicazione di misure di protezione temporanee (ad es. chiusura di determinate porte di comunicazione, blocco in scrittura su specifiche aree di sistema, disabilitazione di demoni/servizi di sistema non essenziali, etc.), ovvero mediante la sostituzione di un *workload* immutabile (istanze, container, etc.) ricorrendo alla corrispondente *master image*.
- *Digital forensic & Post-mortem analysis*: a valle dell'Incidente di sicurezza il personale del Servizio SOC provvede a identificare, acquisire e analizzare le evidenze forensi connesse all'Incidente di sicurezza occorso, avendo cura di preservare l'integrità della catena di custodia. Le evidenze così raccolte vengono successivamente trasmesse all'Amministrazione interessata per l'archiviazione, unitamente al *Report* sintetico e di dettaglio contenente, fra le altre informazioni, il risultato dell'analisi *Post-mortem* incluse le eventuali *Root Cause Analysis* e *Lesson Learned*, se identificate.

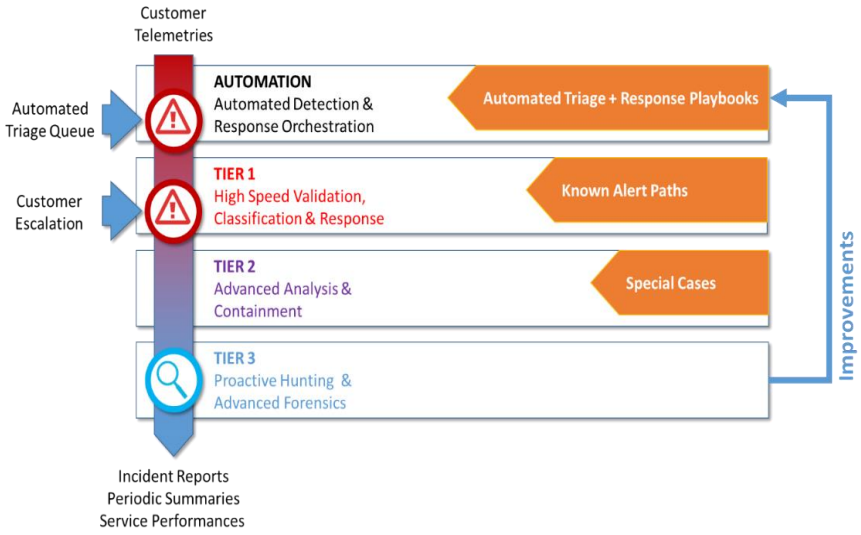

Figura 7 – Ciclo di gestione incidenti

5. **Fase di Terminazione**: al termine del contratto, il fornitore provvede a ripristinare la situazione originaria, rimuovendo tutti i componenti tecnici installati presso le sedi della PA. Del pari, si adopererà per trasferire alla medesima i registri di interesse e la conoscenza tecnica acquisita durante il periodo di erogazione del servizio, in modo da agevolare l'Amministrazione nel trasferimento del Servizio SOC ad altro gestore o presso le proprie strutture tecniche interne. Più nel dettaglio, la fase di Terminazione prevede le sotto-fasi di:

- *Decommissioning dei componenti tecnici*: salvo differente accordo con la PA, tutte gli eventuali componenti software (agent, connettori, API, etc.) e hardware (concentratori VPN, collettori di log, etc.) installati per abilitare l'erogazione del Servizio sono rimossi o ritirati dal Fornitore, il quale avrà cura di ripristinare contestualmente le condizioni originarie della rete della PA interessata.
- *Handover dei registri e della conoscenza*: tutti i registri creati in sede di attivazione del Servizio e aggiornati in itinere e tutta la conoscenza acquisita nel corso della sua erogazione saranno trasmessi all'Amministrazione in forma documentale, secondo un formato standard di comune fruizione. Il Fornitore presterà inoltre il proprio supporto all'Amministrazione affinché questa possa completare la propria transizione verso una differente gestione nel minor tempo e con la minore interruzione di servizio possibile.

Modello Operativo

Per poter conseguire il livello di efficienza necessario per assicurare continuità nel supportare i propri clienti in condizioni spesso di emergenza, il servizio SOC è organizzato su diversi livelli definiti come "tier", la cui differenziazione è legata alla capacità operativa e al grado di approfondimento e autonomia via via crescente per ogni livello.

Il processo di revisione continua delle situazioni di rischio, di approfondimento tecnico e classificazione di eventuali incidenti informatici di sicurezza e di gestione delle attività di incident response, in termini di supporto al contenimento e valutazione continua dello stato di efficacia dello stesso, viene integralmente gestito dal SOC. Questo sfrutta l'organizzazione a più livelli, le tecnologie e le best practice consolidate grazie alla continua esperienza maturata dal RTI in contesti complessi e su threat actor significativi. In particolare, il primo livello (**Tier 1**) è costituito da operatori in turnazione che si occupano principalmente del controllo e monitoraggio costante di anomalie di sicurezza o di fornire un'accoglienza specialistica di secondo livello (cfr. §4.3) in caso di richieste dell'Amministrazione. L'operatività del Tier 1 si estende alla prima classificazione di un eventuale incidente di sicurezza, all'apertura di un caso di analisi, alla gestione delle procedure di response codificate in funzione della classificazione effettuata e alla gestione dell'eventuale processo di escalation. Tale livello prevede quindi la gestione continuativa del servizio "proattivo" di monitoraggio della sicurezza del dominio dell'Amministrazione, al fine di:

- Gestire attività di triage autonome o approfondimenti richiesti dall'Amministrazione;
- Classificare eventuali minacce attive, validarne l'effettivo impatto e diffusione e avviare le procedure di escalation;
- Coordinare la prima fase di response per le attività di contenimento più idonee e misurarne l'efficacia.

Di seguito si riportano le funzioni gestite dal Tier 1 e le capacità del SOC espresse da questo livello: ✓Security Monitoring; ✓Customer Escalation Point of contact; ✓Threat Hunting; ✓Security Analysis (telemetrie); ✓Anomalies Categorization; ✓Triage (case management); ✓Preliminary Response (Incident Management di primo livello); ✓Incident Report; ✓Escalation al secondo livello.

Il secondo livello del SOC (**Tier 2**) è costituito da un team di specialisti di sicurezza senior in grado di intervenire a seguito di una richiesta di ingaggio da parte del primo livello, mettendo a fattore comune le competenze relative alle minacce e vulnerabilità al momento riscontrate. Questo team conduce attività

di analisi approfondite che necessitano di competenze tecniche avanzate in termini di conoscenza del funzionamento delle contromisure presenti nel dominio sotto monitoraggio, delle tecniche e tattiche tipicamente utilizzate dagli attaccanti per comporre la kill-chain, delle tecniche di investigazione necessarie sulle telemetrie raccolte al fine di ricostruire l'effettiva situazione in corso ossia: ✓Sistemi impattati e catena degli eventi generata dall'attacco; ✓Presenza di artefatti all'interno dei sistemi e analisi preliminare per identificare eventuali componenti malevoli (APT); ✓Root cause che ha generato la catena di eventi osservata; ✓Identificazione e coordinamento di tattiche di contenimento "specifiche" in funzione della situazione ricostruita; ✓Coordinamento stakeholder per attività di response complesse; ✓Gestione della Knowledge Base (KB) interna e avvio attività di miglioramento dei processi di classificazione e response di primo livello; ✓Escalation al terzo livello.

Di seguito si riportano le funzioni gestite dal Tier 2 e le capacità del SOC espresse da questo livello: ✓In-depth Incident Investigation (Incident Management di secondo livello); ✓Security Analysis (telemetrie, contenuto sistemi, artefatti sospetti); ✓Response coordination; ✓Incident Containement; ✓Threat Intelligence (creazione indicatori a partire dai dati esecutivi degli incidenti gestiti); ✓Incident Report.

Il terzo livello del SOC (**Tier 3**) è costituito da team ad-hoc di specialisti per i processi di incident response avanzato e per tutti i servizi a valore aggiunto che richiedano competenze e capacità come il reverse engineering di eventuali artefatti, la ricerca continua di informazioni o indicatori per la Cyber Threat Intelligence o l'esecuzione di attività di ricerca continua di vulnerabilità esposte sul perimetro dell'Amministrazione. L'intervento del Tier 3 è basato su micro-team costruiti all'occorrenza che vengono assegnati ad un task specifico tra quelli sopra elencati, e generano report di dettaglio sensibili condivisi con l'Amministrazione.

Di seguito si riportano le funzioni gestite dal Tier 3 e le capacità del SOC espresse da questo livello: ✓Advanced Security Analysis (e.g. reverse engineering, attack attribution); ✓Threat Intelligence maintenance; ✓Continuous Vulnerability Assessment services.

5.1. SOLUZIONI TECNOLOGICHE PROPOSTE PER IL SOC

Il RTI propone per il Servizio SOC una soluzione integrata che consente agli analisti di rilevare rapidamente le anomalie di sicurezza, contestualizzarle e creare le condizioni per porre rapidamente in essere le necessarie azioni di contenimento.

Nella successiva figura sono schematizzate tutte le componenti funzionali che sottendono all'erogazione dei servizi di AQ con particolare riferimento a quelle necessarie per il Servizio SOC.

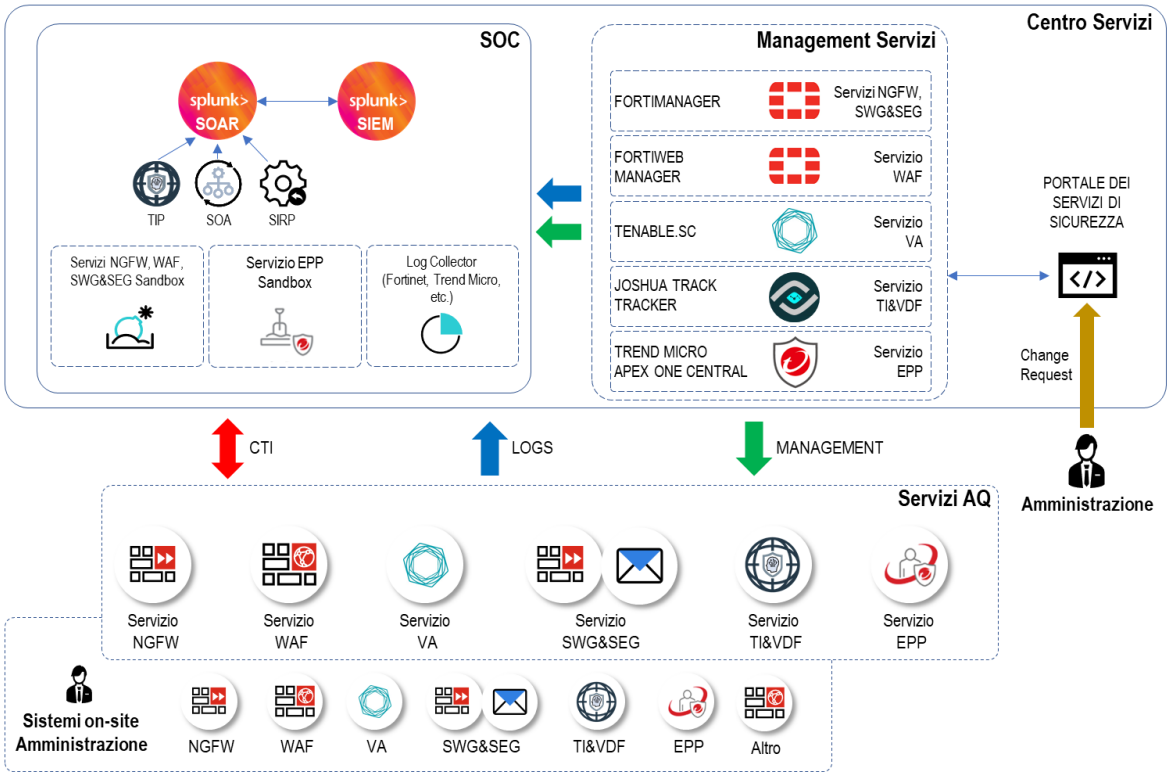

Figura 8 – Componenti funzionali del servizio SOC

La soluzione tecnologica prevista per il Servizio SOC è costituita dalle componenti SIEM e SOAR, Log Collector e le Sandbox previste in funzione del servizio erogato. Sono inoltre presenti le console di gestione per ciascuna delle tecnologie di erogazione dei servizi che interagiscono con la piattaforma SOC. Completa l'architettura il Portale dei Servizi di Sicurezza che consente alle Amministrazioni di richiedere change alle policy e modifiche alle configurazioni per i servizi proposti.

La progettazione di tutti i servizi previsti in AQ è stata effettuata in maniera sinergica ed integrata secondo una visione unitaria che è in grado di garantire la migliore postura di sicurezza dell'Amministrazione contraente. Ciascun servizio, pur ottimizzato per essere erogato anche singolarmente, esprime la massima potenzialità ed efficacia all'interno della visione integrata del proponente insieme con gli altri servizi di sicurezza. A questo riguardo si rappresenta di seguito lo schema dei flussi di interazione tra tutti i servizi dell'AQ che sono funzionali a tale visione progettuale descritti nel dettaglio nei capitoli successivi.

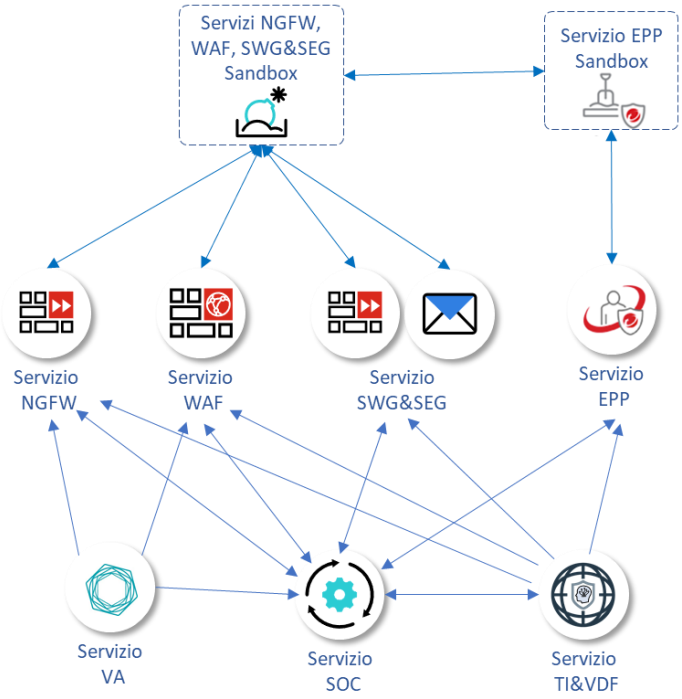

Figura 9 – Flussi di interazione

Per l'erogazione del Servizio SOC, il RTI si avvale di una piattaforma tecnologica leader di mercato: **Splunk Security Suite**. La piattaforma utilizza l'approccio "Data-to-Everything", gestendo efficacemente la raccolta di informazioni dagli asset IT della PA con il supporto di avanzati processi di intelligence, anche automatici, che consentono ai team di sicurezza di eseguire analisi statistiche, visive, comportamentali ed esplorative, identificare rapidamente un possibile incidente di sicurezza, velocizzando il processo decisionale e di individuazione della risposta più efficace, con la conseguente riduzione dei rischi per la PA.

La soluzione fornita dal RTI copre molteplici aree della Cyber Security, favorendo la collaborazione fra i vari team di sicurezza e supportando la corretta implementazione delle migliori pratiche per la protezione di infrastrutture e dispositivi. La piattaforma consente di attuare un flusso di lavoro completo, dalla raccolta dati fino all'invocazione delle azioni necessarie a contrastare le più disparate minacce, indirizzando efficacemente tutte le fasi della gestione delle informazioni e degli eventi di sicurezza.

La suite Splunk si compone di differenti elementi architetturali e servizi specializzati, volti ad ottenere un insieme completo e omogeneo di funzionalità di sicurezza integrate:

Figura 10 – Splunk DtE

Splunk Security Suite	
Splunk Enterprise	Una piattaforma di data-analytics potente e flessibile, in grado di gestire svariati scenari di analisi dei dati con finalità di sicurezza. Consente di monitorare e analizzare rapidamente i dati da qualsiasi fonte, alimentando le altre funzionalità di sicurezza.
Splunk Enterprise Security	Una soluzione di gestione delle informazioni e degli eventi di sicurezza (SIEM) che fornisce approfondimenti sui dati generati dagli endpoint e dalle tecnologie di sicurezza operanti sulla rete, nonché sulle informazioni relative a malware e vulnerabilità.
Splunk SOAR	Una piattaforma di orchestrazione, automazione e risposta agli eventi di sicurezza (SOAR) che si integra con le tecnologie di sicurezza esistenti per fornire uno strato di "tessuto connettivo" tra di esse, rendendole più intelligenti, più veloci e resilienti.
Splunk Applications	Applicazioni sviluppate da Splunk, dai suoi partner e dalla comunità per migliorare ed estendere le potenzialità della piattaforma, ad esempio l'App per la Compliance GDPR e per il MITRE ATT&CK Navigator.
Splunk Security Essentials	Un'applicazione che permette di esplorare nuovi casi d'uso e di distribuire indicatori di compromissione da Splunk Security Essentials a Splunk Enterprise e ai componenti Splunk SIEM e SOAR.
Splunk Enterprise Security Content Updates	Archivio di documentazione dettagliata sull'analisi della sicurezza, chiamato 'Analytic Stories', che supporta gli analisti nell'indagine e contrasto alle nuove minacce rilevate.

Tabella 8 – Suite Splunk

5.2. LIVELLO DI AUTOMAZIONE DEI PROCESSI DI MANAGEMENT, MODALITÀ E STRUMENTI DI CONTROLLO CENTRALIZZATO (CASE MANAGEMENT)

Il modello operativo del SOC proposto si basa sulle interazioni tra persone, tecnologie e processi, che operano tra loro secondo uno schema collaborativo ampiamente consolidato e riportato nella figura seguente, dove sono rappresentate le capacità che il SOC mette a disposizione delle PA e come queste ultime sono impiegate in funzione delle azioni, degli scambi informativi o delle necessità operative inerenti il mantenimento dell'integrità del livello di sicurezza della PA gestita. Ogni capacità è espressa integrando: ✓**strumenti di supporto** all'avanguardia per automatizzare l'operatività e normalizzare il processo di comunicazione verso le altre capacità del SOC; ✓**team di lavoro** organizzati su vari livelli (tier) formati per gestire le attività di identificazione di anomalie, validazione delle stesse e supporto alla response;✓**sistemi di comunicazione** adeguati a velocizzare le operazioni di scambio e supportare la creazione di una KB interna.

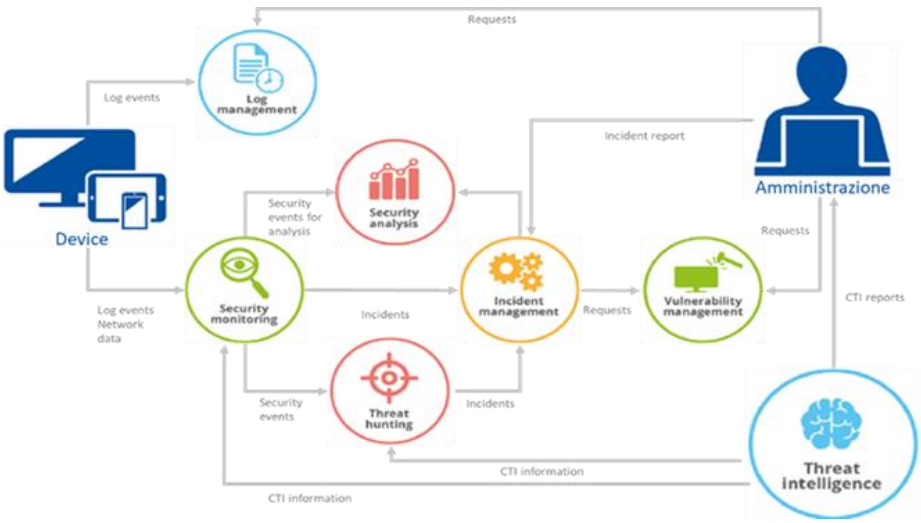

Figura 11 – Capacità del SOC

All'interno della suite Splunk le funzionalità di orchestrazione, automazione e risposta sono fornite dal componente **SOAR**, che integrano e potenziano le capability del SIEM della suite. Il SOAR supporta una vasta gamma di funzioni di sicurezza, tra cui la gestione degli eventi e dei casi, l'intelligence integrata per l'identificazione delle minacce e gli strumenti di collaborazione e di reporting. Permette inoltre agli analisti di sicurezza di lavorare in modo più efficace ed efficiente, automatizzando le attività ripetitive e velocizzando la gestione degli incidenti grazie al supporto all'automazione delle fasi di rilevamento, di indagine e di risposta alle minacce. Infine, consente di incrementare la produttività e di rafforzare al contempo il livello di difesa connettendo e coordinando flussi di lavoro complessi attraverso i team di sicurezza e gli strumenti da essi impiegati.

In particolare, Splunk SOAR consente di: ✓automatizzare sia il triage degli eventi sia le attività più ripetitive, in modo da permettere agli operatori SOC di focalizzarsi sulle attività di analisi che traggono maggiore valore dall'interazione umana; ✓investigare e rispondere agli incidenti di sicurezza con tempistiche di rilevamento (MTTD) e di risposta (MTTR) misurabili nell'ordine dei secondi o dei minuti invece che in ore, grazie all'uso di playbook che automatizzano le attività di sicurezza su una moltitudine di scenari. Il componente proposto orchestra i flussi di lavoro e la risposta agli incidenti integrandosi con altri strumenti di sicurezza; infatti supporta nativamente oltre 350 strumenti di terze parti e oltre 2.400 azioni automatizzate. Ciò non solo massimizza la velocità di investigazione e di risposta ma sblocca anche l'efficacia potenziale degli altri strumenti di sicurezza impiegati nel SOC.

Figura 12 – Dashboard Splunk SOAR

Automazione ed integrazione dei processi operativi e di management

Il RTI pone, alla base dell'efficacia del proprio modello operativo, l'automazione dei processi di management come elemento distintivo della soluzione proposta. Infatti, Splunk SOAR consente di attivare/gestire l'apertura manuale/automatica di casi di incidente e avviare il processo di orchestrazione e automazione della response mediante l'impiego di playbook specializzati, con sequenze di azioni di verifica aggiuntiva, di contenimento o di comunicazione programmate, in grado di rispondere in maniera adeguata all'incidente di sicurezza.

In caso di apertura di un case sulla piattaforma SOAR in maniera automatica/proattiva sarà generato e gestito il ticket sul sistema di trouble ticketing del RTI.

La soluzione SOAR proposta consente agli analisti di sfruttare l'automazione per accelerare la gestione degli incidenti e intraprendere azioni difensive in contemporanea su più sistemi di sicurezza, riducendo al minimo il cambio di contesto richiesto agli operatori, diminuendo l'eccessivo numero di avvisi e velocizzando la risposta agli incidenti.

Il livello di maturità della soluzione consente di gestire il processo di contestualizzazione e fusione con la threat intelligence direttamente in fase di acquisizione delle informazioni grezze, dettagliando tutta la base di conoscenza e non solo gli eventi sospetti. Questo approccio esalta la capacità di automazione delle attività di gestione e di organizzazione della risposta, in quanto i modelli di analisi possono beneficiare dell'integrazione con i dati aggiuntivi incrementando la capacità di interpretazione della situazione e di identificazione di comportamenti anomali anche complessi.

Il Servizio SOC dispone, pertanto, di capacità di contestualizzazione e di procedure tipiche di un SOAR, fondendole con le funzionalità di approfondimento e identificazione delle anomalie, consentendo una gestione dei playbook di intervento più efficace e indirizzata per: ✓gestire un processo "misto",

orchestrando procedure di contenimento iniziali in funzione del triage effettuato, insieme alla richiesta di azioni di intervento da parte degli operatori per ulteriori accertamenti o validazione dello scenario ricostruito; ✓automatizzare azioni rapide di primo contenimento indirizzate allo specifico scenario di attacco sintetizzato (ad es. sospendere utenze, mettere in quarantena endpoint, bloccare zone di rete); ✓automatizzare eventuali azioni di approfondimento su sistemi terzi prima di richiedere l'intervento dell'operatore (ad es. screenshot del contenuto associato ad una URL sospetta, sottomissione hash a Knowledge Base relativi ad artefatti malevoli, esecuzione triage su sistema EDR connesso, etc.); ✓tracciare in ogni momento lo stato di gestione di un incidente e tutte le entità "osservate" al fine di avere una visione completa di quanto accaduto, utile per le successive esecuzioni degli stessi playbook.

Modalità e strumenti di controllo centralizzati

Per facilitare la gestione delle attività di analisi e risposta agli incidenti, gli operatori possono contare su funzionalità di controllo centralizzato finalizzate alla gestione del processo di incident management. La piattaforma è in grado di aprire e gestire automaticamente i casi di analisi le cui informazioni provenienti dal triage automatico mappano i modelli predefiniti (playbook). L'analista può comunque prendere in carico il caso, assegnarlo ad un altro analista e seguirne l'evoluzione nel tempo. Un caso può essere aperto anche manualmente partendo da altri componenti di visualizzazione (dashboard, drill-down, grafico), utilizzando un template predefinito.

Un caso contiene un insieme di informazioni completo e coerente, quali, a titolo di esempio: ✓Il livello di gravità assegnatogli; ✓Il livello di triage specifico; ✓Il titolo breve; ✓Una serie di tag utili per la classificazione; ✓La descrizione dettagliata; ✓La data di apertura; ✓L'assegnatario; ✓L'elenco delle attività in corso e l'assegnatario di ciascuna attività; ✓L'elenco delle attività che devono essere eseguite per la risoluzione; ✓Un insieme di metriche misurate in funzione della situazione.

Per la fase di Incident Response è disponibile una serie di playbook già "strutturati" per ottimizzare l'efficacia delle soluzioni di sicurezza specificate in questa proposta, garantendo l'attivazione automatizzata delle funzioni di contenimento previste dalle varie piattaforme. Inoltre, è anche disponibile un set di playbook relativi alle principali tecnologie di mercato che possono essere attivati in funzione dello scenario di integrazione specifico di ciascuna PA, per incrementare sensibilmente la capacità di risposta del servizio. Infine, sono previsti una serie di playbook mirati a garantire la distribuzione delle informazioni operative consentendo l'allineamento della base di conoscenza sulle piattaforme interessate.

Nell'ambito dei processi a supporto della gestione degli incidenti, le attività possono essere assegnate a specifici analisti SOC e viene mantenuta una bozza delle attività svolte con la possibilità di allegare evidenze o bookmark di ricerche precedenti gestite su altri componenti grafici (dashboard, drill-down e grafici).

Per supportare al meglio l'automazione durante la fase di analisi, è possibile definire modelli di casi in grado di migliorare la produttività in base alla classificazione iniziale di un incidente. I modelli possono essere correlati a categorie di incidenti di sicurezza o a situazioni rischiose che possono essere considerate importanti per il dominio specifico. All'interno del modello solitamente sono definiti: ✓una serie di tag per la classificazione; ✓prefissi da utilizzare per titoli e descrizioni; ✓un elenco personalizzabile di attività da gestire; ✓un insieme di metriche che saranno valutate dagli analisti durante l'attività.

Per ogni caso viene gestito e visualizzato un log di tracciabilità che elenca tutte le azioni svolte dagli utenti e le attività ad esso correlate, riportando anche la durata di ogni operazione effettuata.

La piattaforma, infine, mostra una dashboard riepilogativa sullo stato dei casi gestiti (numeri e tempi di risoluzione).

5.3. CARATTERISTICHE TECNICHE DELLA SOLUZIONE SOFTWARE SIEM

L'elemento che distingue maggiormente la piattaforma Splunk, rispetto alle altre soluzioni SIEM, è la sua natura di piattaforma espressamente concepita per la data-analytics. Basandosi su un motore per l'analisi dei dati robusto e performante, il componente SIEM di Splunk consente di acquisire dati con volumi e velocità non raggiungibili dalle altre soluzioni concorrenti, nonché di effettuare attività di analisi e correlazione sia sui dati acquisiti in tempo reale sia sui dati storicizzati, anche a lungo termine. La soluzione Splunk, caratterizzandosi come SIEM 'analytics-driven', è nativamente predisposta per l'applicazione di metodi di machine learning, data science e statistica avanzata: ciò pone Splunk nelle condizioni di effettuare analisi predittive volte ad identificare in tempo reale l'occorrenza di eventi avversi. Nella seguente tabella è possibile trovare una comparazione delle caratteristiche della soluzione SIEM Splunk rispetto alle soluzioni SIEM tradizionali (non analytics-driven), alle soluzioni Open Source e ai nuovi competitor sul mercato. Il valore in colonna 'DIY' (Do It Yourself) indica una funzionalità implementabile solo tramite la scrittura e la successiva integrazione di codice ad-hoc.

	Splunk ES	SIEM Tradizionali	SIEM Open Source	Nuovi Competitor
1. Raccolta di log ed eventi	Sì	Sì	Sì	Sì
2. Applicazione in tempo reale delle regole di correlazione	Sì	Sì	DIY	Sì
3. Applicazione in tempo reale di metodi di analisi avanzata e di tecniche di *machine-learning*	Sì	Limitato	DIY	Sì
4. Analisi di dati storicizzati a lungo termine, anche con tecniche di *machine-learning*	Sì	Limitato	DIY	Limitato
5. Conservazione degli eventi a lungo termine	Sì	Limitato	Sì	Limitato
6. Ricerca e reportistica su dati normalizzati	Sì	Sì	Sì	Sì
7. Ricerca e reportistica su dati grezzi ('*raw data*')	Sì	Difficile	Sì	Difficile
8. Ingestione di dati di contesto per l'esecuzione di correlazioni e di analisi addizionali	Sì	Limitato	Sì	Limitato
9 Gestione di scenari non strettamente legati alla sicurezza	Sì	No	DIY	No

Tabella 9 – Confronto funzionalità SIEM

Splunk SIEM consente agli operatori del servizio SOC di effettuare un monitoraggio evoluto basato sulla capacità di aggregare dati significativi, provenienti da molteplici fonti, stabilendo in tempo reale analisi e correlazioni finalizzate a individuare comportamenti anomali, segnali critici e a generare allarmi, rispondendo alle esigenze di incident response, compliance e analisi forensi.
Il SIEM raccoglie i log e centralizza l'analisi degli eventi generati da applicazioni e sistemi in rete. Grazie alle funzionalità di machine learning, le attività di correlazione e monitoraggio sono potenziate, abilitando una security intelligence evoluta.
La soluzione proposta dal RTI supporta gli operatori del SOC nell'erogazione del servizio lungo le seguenti fasi:

1. COLLEZIONE. Raccolta dei log di sicurezza basilari e di altri eventi dall'ambiente informatico gestito. La raccolta dei log e degli eventi si esplica, al minimo, nei seguenti ambiti: ✓**Traffico di rete**, dai log di traffico generati da firewall *Fortinet, Cisco, Palo Alto, CheckPoint* e di altri vendor; ✓**Attività sugli endpoint**, inclusi gli eventi Windows, i system log Linux, i log auditd Linux, i system log MacOS; ✓**Sistemi di autenticazione**, per eventi Active Directory, log LDAP, eventi di Identity and Access Management (IAM) basati su cloud, eventi da autenticazione locale (NTLM, PAM, etc.); ✓**Traffico web**, inclusi i log generati da NGFW, WAF, SWG e Proxy Server prodotti da vendor quali *Fortinet, Cisco, Palo Alto, Websense, Bluecoat* e altri.
2. NORMALIZZAZIONE. Applicazione di una tassonomia di sicurezza standard e integrazione con ulteriori dati relativi ad asset e identità. Questa fase è volta ad assicurare che i dati raccolti nella precedente fase di Collezione siano conformi ad una tassonomia di sicurezza standard, ovvero che dati comuni quali, ad es., indirizzi IP, porte TCP, nome utente o nome macchina siano normalizzati e rappresentati attraverso una nomenclatura standard, indipendentemente dal dispositivo che ha generato o registrato l'evento. L'attività di normalizzazione migliora significativamente l'efficacia della correlazione specie con l'impiego di sorgenti diverse. La successiva integrazione con dati relativi ad asset e identità può avvenire interfacciando la piattaforma con sistemi di gestione degli asset IT (sistemi, reti, dispositivi e applicazioni) e con sistemi di gestione delle identità quali Microsoft Active Directory, OpenLDAP e altri sistemi IAM/SSO.
3. ESPANSIONE. Raccolta di ulteriori dati quali eventi di dettaglio sugli endpoint o metadati di rete, al fine di abilitare il rilevamento avanzato degli attacchi. Dati provenienti da fonti quali query DNS e ulteriori dati generati dagli endpoint ampliano le capacità di detection, consentendo un'efficace ricerca delle minacce eventualmente residenti all'interno della rete. Le fonti di dati impiegate in questo stadio includono almeno: ✓**La rete**, con metadati legati agli specifici protocolli di rete utilizzati, forniti da componenti specifici come *Splunk Stream* e *Bro*, accanto ai dati provenienti da query DNS e lease DHCP; ✓**Gli endpoint**, con la cattura dettagliata di attività quali creazione di processi, modifiche a file e a valori di registro, apertura di socket di rete, etc., consentita da tool specifici quali *Microsoft Sysmon*, *Osquery* e *Carbon Black Defense*.
4. ARRICCHIMENTO – Integrazione degli eventi e delle informazioni di sicurezza con fonti di Cyber Security Intelligence per una migliore comprensione del contesto e del potenziale impatto di un evento. In aggiunta all'espansione dei dati con elementi raccolti dalla rete e dagli endpoint, la piattaforma Splunk consente l'arricchimento dei dati con informazioni di intelligence provenienti da fonti interne ed esterne. Elementi di conoscenza contestuale e investigativa, unitamente a feed di threat-intelligence e fonti di open-source intelligence (OSINT), consentono di estrarre maggiore valore dai dati raccolti, in modo da consentire una più rapida e accurata identificazione degli eventi di sicurezza significativi e dei potenziali incidenti.
5. AUTOMAZIONE E ORCHESTRAZIONE – Conferimento di una capacità operativa di reazione agli incidenti di sicurezza coerente e ripetibile. Grazie al componente SOAR è possibile incrementare le capacità operative del SOC, consentendo una risposta agli incidenti di sicurezza più tempestiva e sistematica, un processo di investigazione più rapido, nonché una significativa riduzione dei danni conseguenti agli attacchi. Le fonti di dati impiegate in questo stadio includono eventi ad elevata accuratezza generati dalla piattaforma Splunk Enterprise.
6. RILEVAMENTO AVANZATO – Applicazione di meccanismi di rilevamento sofisticati, inclusi quelli basati sull'apprendimento automatico. Attraverso l'applicazione di metodi di **machine learning, data science e statistica avanzata** applicati al comportamento di utenti, dispositivi e applicazioni, viene abilitata la capacità di individuare entità avversarie, minacce sconosciute e agenti malevoli interni anche con tracce di attività molto ridotte. Le fonti di dati impiegate sono le medesime descritte nel precedente punto 3.

Figura 13 – Dashboard Splunk

Gli strumenti messi a disposizione dalla piattaforma Splunk presentano, inoltre, un'**interfaccia chiara ed intuitiva** che migliora l'interazione da parte degli analisti, nella rappresentazione degli esiti delle ricerche e delle correlazioni che avvengono analizzando set informativi anche non omogenei provenienti da più fonti di dati. Le correlazioni possono quindi riguardare eventi provenienti da qualsiasi dominio di sicurezza (accesso, identità, endpoint, rete), liste di asset, liste di identità, threat intelligence e altri dati nella piattaforma. I dataset risultanti possono essere ulteriormente trattati con un potente linguaggio di elaborazione ed attivare azioni in risposta adattativa a eventi che corrispondono alle condizioni di ricerca. Essendo la ricerca una delle attività che maggiormente caratterizza l'operatività degli analisti, la piattaforma mette a disposizione, oltre ad un nutrito numero di regole esistenti e template a supporto, anche delle procedure guidate grazie alle quali la creazione di regole viene resa semplice ed immediata.
Il SIEM analizza i registri raccolti per evidenziare eventi o comportamenti di interesse consentendo, ad esempio, di rilevare un accesso amministrativo al di fuori del normale orario di lavoro, quindi informazioni sull'host, sull'ID e altro ancora. Le informazioni contestuali raccolte rendono i **report estremamente più dettagliati** e permettono di ottimizzare i flussi di lavoro finalizzati alla risoluzione degli incidenti.

5.4. PROPOSTE INNOVATIVE PER IL CONTROLLO ED IL MIGLIORAMENTO CONTINUO DELLA QUALITÀ PERCEPITA DEL SERVIZIO.

Il RTI propone un servizio SOC basato su standard e best practice nazionali ed internazionali, quali SANS, NIST 800-61, CIS, MITRE ATT&CK, ispirato ai quattro "classici" stadi Predict-Prevent-Detect-Respond ed estendendone i contenuti ed i concetti ad una visione più ampia. Il principio che ispira il servizio è quello di far evolvere i modelli di gestione standard dei SOC, compenetrando tematiche tradizionali con il nuovo paradigma del rischio cyber, che prevede la gestione di minacce di tipo asimmetrico in cui, a prescindere dalla robustezza dei meccanismi di difesa adottati, permane sempre il rischio che un attacco abbia successo.

Il Servizio SOC nella sua interezza adotta un approccio olistico e focalizza l'attenzione costante sulle attività di governo, prevenzione e reazione tempestiva, anche e soprattutto nell'ottica del miglioramento continuo. A tal proposito, la soluzione proposta attraverso il modulo Splunk Dashboard Studio mette a disposizione della PA apposite viste integrate, sia sull'andamento generale dei servizi e sul loro funzionamento, sia sulla continua e reale erogazione a valore di questi. La proposizione, nello specifico, si concretizza in un **cruscotto unificato**, orientato ad illustrare lo stato della sicurezza dell'Amministrazione comparato in tempo reale con tutte le informazioni ricevute dal campo. In questo modo il Referente Tecnico della PA dispone di informazioni contestualizzate, sintetiche e di dettaglio, attraverso le quali poter avere contezza direttamente di quanto sta accadendo e dell'efficacia delle azioni intraprese.

Figura 14 – Cruscotto unificato

Al fine di alimentare il processo di **controllo e di miglioramento continuo della Qualità del Servizio**, con particolare riferimento alla qualità percepita dai soggetti fruitori, il sotto-processo di interazione e comunicazione con l'utilizzatore opererà in modalità '**closed-loop**', raccogliendo costantemente **feedback** a valle di una serie di interazioni ricorrenti appositamente selezionate. Il meccanismo proposto, atto a misurare e a incrementare il livello di **customer-satisfaction**, rappresenta una **innovazione di processo** ampiamente collaudata in diversi settori consumer (e-Commerce, e-Banking, servizi di Streaming multimediale, etc.) e qui applicata, per la prima volta, all'erogazione di servizi tecnici rivolti al mondo delle Pubbliche Amministrazioni.

La raccolta dei feedback potrà avvenire immediatamente a valle dell'interazione con il referente dell'Amministrazione o in qualsiasi momento successivo, eventualmente anche dopo la chiusura dell'incidente. Il feedback raccolto sarà di tipo quali-quantitativo, in modo da poter sia misurare il grado di soddisfazione generale per ciascuna categoria di interazione (o di deliverable) consumata, sia identificare in maniera circoscritta le specifiche aree di miglioramento.

Il modulo di feedback, concepito per garantire tanto l'intuitività e la rapidità della compilazione quanto la completezza delle informazioni acquisibili, sarà strutturato come di seguito:

1. **Indicatore generale di soddisfazione**, selezionabile in una scala da *1* a *5*, dove *1* rappresenta un elevato grado di insoddisfazione e *5* un elevato grado di soddisfazione;
2. **Elenco chiuso di voci selezionabili**, specifiche per ciascuna tipologia di interazione o di deliverable, cui attribuire una delle possibili valutazioni fra *Inferiore alle attese*, *Pari alle attese* o *Superiore alle attese*;
3. **Campo a testo libero**, volto alla raccolta degli eventuali suggerimenti per il perfezionamento dei moduli, delle procedure e dei processi, ovvero per la raccolta di eventuali encomi mirata a identificare le possibili aree di eccellenza da assumere a modello per il miglioramento dei servizi esistenti e per lo sviluppo di nuovi servizi.

Per agevolare la raccolta del feedback, al termine di ciascuna interazione contemplata dal processo di controllo e di miglioramento continuo, il referente dell'Amministrazione riceverà un messaggio di posta elettronica contenente il collegamento ipertestuale al form, specifico per l'Incidente in oggetto e per la tipologia di interazione (o di deliverable) oggetto di valutazione, unitamente alle informazioni e alle istruzioni necessarie per la corretta compilazione del modulo di feedback.

Nello specifico ambito del Servizio SOC, il RTI ha individuato in particolare tre aree di controllo e miglioramento, corrispondenti alle seguenti fasi e/o deliverable del Servizio:

a) Riduzione delle casistiche che richiedano, o comunque inneschino, un contatto con il referente dell'Amministrazione. Poiché non è infrequente che un sospetto Incidente di sicurezza possa occorrere anche al di fuori del comune orario di ufficio, è di fondamentale importanza che il contatto con il referente dell'Amministrazione avvenga solo quando effettivamente necessario. Ciò include non soltanto i possibili falsi positivi ma anche tutte quelle situazioni di deficit informativo, sia esso di natura procedurale o di natura circostanziale. In questa fase, il processo di controllo e di miglioramento continuo acquisirà i necessari input da parte del referente dell'Amministrazione e con questi alimenterà gli strumenti a disposizione degli analisti SOC.
b) Chiarezza e completezza della comunicazione in fase di primo contatto con il referente dell'Amministrazione all'atto dell'apertura dell'Incidente. Affinché il referente dell'Amministrazione possa acquisire tutte e sole le informazioni effettivamente rilevanti per supportare l'attività del SOC ovvero per intervenire in prima persona laddove opportuno, risulta di primaria importanza la definizione di un protocollo di comunicazione che consenta di veicolare, specie in sede di primo contatto, un set di informazioni il più possibile chiaro, completo e corretto. In questa fase, il processo di controllo e di miglioramento continuo acquisirà i necessari input da parte del referente dell'Amministrazione (ad es., possibili lacune nelle informazioni fornite, eventuale eccesso di informazioni non rilevanti, utilizzo di un gergalismo tecnico non comune ovvero eccessivo, etc.) che alimenterà gli strumenti a disposizione degli analisti SOC, con particolare riferimento alla Procedura di Comunicazione seguita nello specifico contesto e a ogni altra procedura attinente la comunicazione con gli stakeholder interni o esterni al RTI.

c) Fruibilità dei deliverable trasmessi al referente dell'Amministrazione, all'atto della chiusura dell'Incidente. Poiché i deliverable consegnati alle Amministrazioni contraenti possono essere destinati ad un'audience diversificata, comprendente anche stakeholder privi di adeguata preparazione tecnica, risulta fondamentale trovare un giusto equilibrio fra esaustività e rigore tecnico da un lato, e piena comprensibilità della reportistica da parte di figure non tecniche dall'altro. In questa fase, il processo di controllo e di miglioramento continuo acquisirà i necessari input da parte del referente dell'Amministrazione (ad es. utilizzo eccessivo di gergalismo tecnico, struttura della reportistica percepita come dispersiva, scarsa chiarezza nell'esposizione di Root Cause e Lesson Learned, eventuali indicazioni di Remediation troppo vaghe o scarsamente applicabili, etc.) e con questi alimenterà gli strumenti a disposizione degli analisti SOC, con particolare riferimento ai Template e alle Linee Guida per la redazione della Reportistica e ad ogni altro modello documentale attinente la trasmissione di informazioni agli stakeholder interni o esterni al RTI.

Infine, il servizio SOC proposto, anche attraverso consolidate **funzionalità di intelligenza artificiale e machine learning**, non solo è in grado di comprendere i fenomeni in accadimento, ma soprattutto fornisce comparazioni e suggerimenti in ottica di "**decision support system**", grazie a specifiche capacità di **predictive analytics**, fondamentali nell'ottica di prevenzione di eventi o incidenti.

6. PROPOSTA PROGETTUALE PER IL SERVIZIO "NEXT GENERATION FIREWALL"

Il servizio "Next Generation Firewall", proposto dal RTI, finalizzato a garantire la protezione di sistemi e rete da minacce esterne, viene fornito attraverso appliance **FortiGate** (hardware appliance o virtual appliance on premise) di **Fortinet**, un'avanzata tecnologia firewall con evoluti servizi di sicurezza multi-minaccia, erogati attraverso un'unica piattaforma integrata che consente di contrastare efficacemente attacchi e minacce informatiche, grazie anche alla semplicità di gestione e alla flessibilità di inserimento in una vasta gamma di scenari di implementazione.
La gestione del servizio viene effettuata attraverso il sistema di management centralizzato costituito dalle componenti **FortiManager** e **FortiAnalyzer**, attraverso VPN create su connettività INTERNET o SPC e terminate, lato Centro Servizi, sui concentratori attestati sull'infrastruttura di management del servizio. Il RTI vanta una consolidata partnership con il vendor ed ha una vasta e profonda esperienza nell'erogazione di servizi NGFW.
L'infrastruttura di erogazione del servizio di Next Generation Firewall si avvale delle componenti di seguito descritte:

- **Piattaforma di Gestione NGFW (FortiManager) –** Piattaforma centralizzata multitenant instanziata presso il Centro Servizi del RTI, utilizzata per la gestione del servizio NGFW. Consente la separazione logica delle PA contraenti in domini distinti (Tenant) garantendo la segregazione completa dei dati. Il FortiManager è una singola console di management che consente di gestire dispositivi Fortinet e fornire funzionalità di update manager centralizzato per tutti gli apparati gestiti. Si riassumono di seguito le caratteristiche principali: ✓Gestione centralizzata di oggetti e policy; ✓Capacità evolute di tracciamento delle revisioni; ✓Comparazione delle configurazioni e auditing delle attività effettuate dagli amministratori; ✓Gestione dei Workflows per una migliore implementazione dell'utilizzo multiutenza; ✓Gestione Centralizzata di SD-WAN, Reti Wireless e VPN; ✓Automazione: Gestione di templates and scripts per il provisioning di nuovi dispositivi o modifica degli esistenti; ✓API JSON o XML per l'interazione con sistemi di orchestrazione di terze parti; ✓Multitenancy e RBAC per una precisa definizione dei ruoli degli amministratori e del loro perimetro di gestione; ✓Software upgrades e security updates centralizzati per i dispositivi gestiti.
- **Log Collector (FortiAnalyzer)** – Piattaforma centralizzata multitenant instanziata presso il Centro Servizi del RTI, utilizzata per il logging e la reportistica del servizio NGFW. Il FortiAnalyzer è uno strumento che integra funzionalità di raccolta di log, analisi e reporting per tutti i dispositivi che compongono la Fortinet Security Fabric; offre capacità di analisi in un'unica piattaforma centralizzata in grado di svolgere ricerche forensi, anche tramite Indicatori di Compromissione (IOC), reportistica, data mining, event handling, archiving e visualizzazione unificata di tutti i log generati dagli apparati. Si riassumono di seguito le caratteristiche principali disponibili agli operatori ed analisti: ✓**FortiView**: consente una visualizzazione interattiva ed un monitoraggio in tempo reale degli eventi di sicurezza. In figura è rappresentata la capability di Threat Mapping che consente la visione grafica di come la minaccia si sviluppa per criticità, tempo, sorgente e destinazione; ✓**NOC&SOC Dashboard**: permette di costruire dashboard personalizzate utili agli ambienti di esercizio e di monitoring per governare la disponibilità delle risorse di rete e sicurezza; ✓**Event Manager**: permette di personalizzare la gestione degli allarmi in seguito ad eventi di sicurezza singoli e la correlazione degli stessi; contribuisce a ridurre lo sforzo di mantenere efficienti le policy di sicurezza grazie alla visibilità degli eventi e ad una rapida individuazione degli attacchi e delle minacce di sicurezza; ✓**Reporting avanzato** che consente di produrre report predefiniti e definirne di personalizzati con l'utilizzo di data set e query ad hoc in linguaggio SQL.
- **FortiSandbox** – Il componente FortiSandbox permette la detonazione anche dei malware di ultima generazione, costituisce parte integrante dell'architettura Fortinet Security Fabric ed utilizza tre modalità di intelligence sulle minacce per il rilevamento e la prevenzione degli Incidenti di sicurezza. In primis, il FortiSandbox utilizza l'intelligence globale sulle minacce emergenti, raccolta in tutto il mondo tramite i ricercatori dei FortiGuard Labs; in secondo luogo, esso condivide i dati di intelligence con altri prodotti Fortinet (WAF, SWG&SEG) o di altri vendor, incrementando l'efficacia dei diversi sistemi nella protezione del patrimonio informativo dell'Amministrazione; infine, aspetto più importante, FortiSandbox applica una forma di **intelligenza artificiale** vera e propria, che include l'analisi statica e comportamentale, al fine di migliorare l'efficacia del rilevamento delle minacce **Zero-day**. L'Artificial Intelligence (AI) è applicata durante l'intero processo di sandboxing, sia tramite analisi statica sia tramite analisi dinamica ad elevata interazione su molteplici sistemi operativi in parallelo. Le caratteristiche principali di un'analisi in Sandbox includono: ✓Motore Antimalware dinamico e aggiornamenti effettuati dai FortiGuard Labs, a cui può inviare query in tempo reale, permettendo così di rilevare in modo veloce minacce esistenti ed emergenti.

Figura 15 – Dashboard FortiManager e FortiAnalyzer

✓Emulazione di Codice: esegue in tempo reale una ispezione di tipo "lightweight sanboxing", con cui si riesce ad identificare tipologie di malware che utilizzano tecniche di evasione e/o si attivano solo in presenza di versioni software specifiche. ✓Ambiente virtuale completo (detonazione): fornisce un ambiente isolato per analizzare codice sospetto o ad alto rischio, permettendo di esplorare e verificare l'intero ciclo di vita della minaccia. ✓Visibilità avanzata: fornisce un quadro globale in una vasta gamma di reti, sistemi e attività di file classificati per livello di rischio, per migliorare la velocità di risposta agli incidenti. ✓Analisi Manuale: consente agli analisti di sottomettere manualmente campioni di malware per effettuare sandboxing virtuale senza la necessità di avere un dispositivo separato.

- **Appliance FortiGate Next Generation Firewall -** Gli apparati Next Generation Firewall permettono la visibilità completa del traffico attraverso la gestione di indirizzi IP, utenti e dispositivi con la possibilità di creare policy di sicurezza con una combinazione di questi fattori. L'ispezione del livello applicativo (Application Control feature), permette una accurata identificazione delle applicazioni che generano traffico all'interno della rete senza comprometterne le performance. Una volta individuato il traffico applicativo, è possibile controllare le applicazioni, bloccare quelle indesiderate, limitare e garantire la relativa banda (Traffic Shaping feature), attivare i profili di protezione antivirus/antimalware, IPS, DLP e le altre verifiche di sicurezza dettagliate precedentemente.

Nella tabella seguente si riportano le appliance proposte dal RTI per le diverse fasce:

Fasce	Fortinet appliance
Fascia 1: fino a 250 Mbps	FortiGate-40F
Fascia 2: fino a 2 Gbps	FortiGate-100F
Fascia 3: fino a 4 Gbps	FortiGate-400E
Fascia 4: fino a 7 Gbps	FortiGate-600E
Fascia 5: fino a 15 Gbps	FortiGate-2600F
Fascia 6: > 15 Gbps	FortiGate-3400E

Tabella 10 – Servizio Next Generation Firewall – Appliance on-premise

La soluzione proposta dal RTI garantisce: ✓funzionalità di firewalling avanzate (es. policy enforcement, statefull inspection, packet filtering, NAT, VPN client-to-site e site-to-site); ✓rilevamento e prevenzione delle intrusioni (IDS, IPS); ✓controllo delle applicazioni; ✓ispezione approfondita del traffico di rete con analisi delle intestazioni e del contenuto di ogni pacchetto; ✓visibilità del traffico crittografato con protezione da relative minacce tramite analisi del traffico HTTPS e altro traffico TLS/ SSL crittografato; ✓protezione e prevenzione delle vulnerabilità conosciute e virus (anti-malware, anti-spam e anti-botnet inspection); ✓QoS bandwith management; ✓trasmissione di eventi e log alla funzionalità di SIEM; ✓produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report).

Le scelte architetturali definite per l'implementazione, la definizione delle misure e delle regole di protezione e le modalità operative di gestione del servizio stesso derivano da una precisa strategia progettuale che consente al servizio di operare con la massima efficacia sia come singolo servizio sia, come meglio specificato nel seguito del presente capitolo, mediante l'**interazione in forte sinergia con gli altri servizi** della fornitura.

6.1. CARATTERISTICHE TECNOLOGICHE E PRESTAZIONALI MIGLIORATIVE

La soluzione tecnologica adottata dal RTI, oltre a garantire la disponibilità di tutti i requisiti minimi di Capitolato, si caratterizza per una serie di aspetti migliorativi che la pongono all'avanguardia nell'erogazione del servizio oggetto del presente paragrafo. In particolare:

- Funzionalità di firewalling avanzate con supporto dell'alta disponibilità, routing avanzato, SDWAN, proxy esplicito, bilanciamento dei server, ispezione di traffico crittografato dei protocolli SMTPS, FTPS, POP3S, IMAPS etc., DLP, gestione del traffico IPv6, DoS Policy, Traffic Shaping;
- Nell'ambito della funzionalità IPS è possibile creare **signature personalizzate** ed è previsto il **software bypass** in caso di fault del suo motore. L'aggiornamento del servizio è continuo e garantito dai laboratori FortiGuard, centro di intelligence Fortinet;
- La funzionalità di controllo delle applicazioni (Application Control) consente di ottimizzare l'utilizzo della banda di rete fornendo **priorità alle applicazioni più critiche** ed il controllo è organizzato in categorie dinamiche, gestite e aggiornate costantemente;
- L'ispezione del traffico di rete garantisce l'analisi sia dell'header (intestazione) sia del payload (contenuto) di ogni pacchetto e può essere effettuata in due modalità: **Flow mode** per un'analisi in tempo reale "packet by packet" e **Proxy mode** per un'analisi di tipo "Store and Forward".
- Adozione del modello di difesa "**Kill chain**" mediante la combinazione **in tempo reale** di servizi di sicurezza che includono anche il **DNS e Web Filtering**.
- **Granularità delle policy legate al QoS**, mediante traffic shaping che permette di applicare politiche anche in base all'applicazione o alle categorie di URL Filtering.
- Invio dei log sia in formato proprietario per il log collector di Fortinet (FortiAnalyzer del Centro Servizi) sia in formato standard syslog con la possibilità di inoltro **fino a 4 log collector/SIEM** diversi.
- Funzionalità di ricerche forensi e IoC, data mining, event handling, archiving, dashboard NOC/SOC personalizzabili.

Con riferimento alle performance, si evidenzia che tutti gli apparati FortiGate, sfruttando le potenzialità offerte dal sistema operativo proprietario FortiOS e la potenza dei processori ASIC proprietari, sono in grado di elaborare in hardware le principali funzionalità di network security e ispezione dei contenuti garantendo elevate prestazioni ed affidabilità. In tabella si evidenzia il miglioramento delle performance in termini di throughput rispetto ai requisiti minimi.

Fasce	NGFW Throughput migliorativi
Fascia 1: fino a 250 Mbps	800 Mbps **(+220%)**
Fascia 2: fino a 2 Gbps	2 Gbps
Fascia 3: fino a 4 Gbps	6 Gbps (**+50%**)

Fascia 4: fino a 7 Gbps	9,5 Gbps (+**36%**)
Fascia 5: fino a 15 Gbps	19 Gbps (+**27%**)
Fascia 6: > 15 Gbps	34 Gbps (+**127%**)

Tabella 11 - Throughput migliorativi per il servizio NGFW

6.2. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il servizio NGFW viene erogato dal Centro Servizi del RTI. Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**) conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT** (**SGS-IT**) conforme allo standard ISO/IEC 20000-1 e dall'implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

Organizzazione del servizio

L'organizzazione del servizio NGFW si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- *acquisizione* del know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione, e delle relative modalità operative, linee guida e metodologie in uso presso l'Amministrazione;
- predisposizione e configurazione del servizio e delle relative piattaforme di management:
  - Il *NGFW Team* attiva il Tenant dedicato all'Amministrazione su ciascuna delle piattaforme di gestione del servizio (FortiManager e FortiAnalyzer);
  - Il *Team on-premise* esegue l'installazione delle componenti previste on-site secondo il piano condiviso con l'Amministrazione. Gli apparati NGFW saranno resi raggiungibili, presi in carico dal sistema di management e configurati da remoto. Il servizio sarà predisposto sulla base di quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano;
  - se necessario, il *Team on-premise* ed il *NGFW Team* gestiscono il processo di migrazione secondo quanto stabilito nel piano di migrazione.

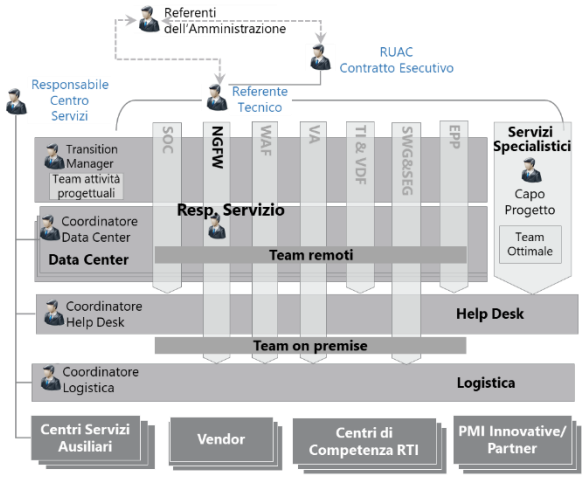

Figura 16 – Organizzazione Servizio NGFW

Erogazione del servizio:

- *Monitoraggio della disponibilità*: gli operatori dell'Help Desk di 2° livello monitorano il servizio attraverso la console (FortiManager) e gestiscono gli allarmi o in autonomia o coinvolgendo le strutture specialistiche di 3° livello.
- *Richieste di modifica delle configurazioni*: L'Amministrazione potrà richiedere l'aggiornamento delle policy di sicurezza utilizzando il portale dei servizi di sicurezza o mediante l'apertura di un ticket (cfr. § 4.3). La richiesta sarà presa in carico dal NGFW team che, una volta effettuate le necessarie attività, provvederà al collaudo della modifica congiuntamente con il personale preposto dell'Amministrazione.
- *Reporting* La reportistica permette di verificare la conformità agli standard scelti e il livello di protezione delle applicazioni. Prevede report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.
- *Supporto alla gestione incidenti*: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

Modalità di erogazione

La modalità di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓installazione di appliance dedicati fisici o virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione; ✓utilizzo di una istanza del servizio NGFW installata presso il Centro Servizi del RTI ed acceduta in modalità SaaS. L'architettura di default proposta dal RTI è quella on premise.

In fase di definizione del progetto esecutivo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione principali per la scelta dello scenario sono: ✓fascia di throughput richiesta; ✓tipologia dei servizi da proteggere, se cioè occorre proteggere servizi esposti su internet o servizi interni del cliente.

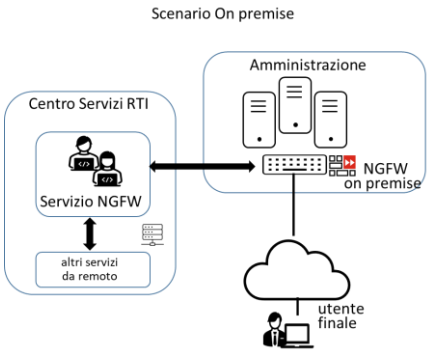

Figura 17 – Modalità di erogazione on premise

Interazione con gli altri servizi

Si riportano di seguito le interazioni principali del Servizio Next Generation Firewall verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: i log del servizio saranno inviati al servizio SOC per la registrazione, tracciatura e correlazione degli eventi, delle minacce e per l'allarmistica. La globalità degli eventi provenienti da domini tecnologici diversi, opportunamente cross

correlati ed orchestrati dal servizio SOC, non solo permettono il rilevamento precoce e proattivo di situazioni anomale, ma consentono anche di rendere particolarmente efficiente il processo di analisi abbreviando i tempi necessari all'individuazione delle azioni mirate al contenimento e alla successiva mitigazione di eventuali incidenti. Le soluzioni tecnologiche presenti nel SOC (SIEM, SOAR, etc.), contribuiranno alla rilevazione di attacchi sofisticati anche con il supporto di tecnologie di machine learning e threat intelligence (cfr. cap.5).

- **Interazione con il servizio Web Application Firewall L1.S3**: La FortiSandbox è a supporto dei servizi NGFW, WAF, SWG&SEG e, attraverso le capacità della Fortinet "Security Fabric", contribuisce alla realizzazione di una forte interazione tra questi servizi. Infatti, qualora la sandbox rilevi una minaccia a seguito di un'analisi eseguita su un file proveniente da uno dei tre servizi, essa produce e rende disponibile una nuova firma zero-day che sarà utilizzata dagli altri servizi per una migliore e più efficace mitigazione di future occorrenze dello stesso malware. Nello specifico, per il solo servizio WAF, in fase di configurazione delle regole, saranno armonizzate le policy che riguardano la protezione dagli attacchi da parte di IP con "bad reputation", oppure le funzionalità di blocco di eventuali indirizzi IP sulla base di geolocalizzazione. Ad esempio, per servizi web che dovranno essere fruiti da utenza presente solo nell'UE, sarà tipicamente impedito il collegamento da indirizzi IP extra UE.
- **Interazione con il servizio Gestione continua delle Vulnerabilità di Sicurezza L1.S4**: Le informazioni sulle vulnerabilità riscontrate saranno utilizzate dal NGFW Team per supportare il tuning delle funzionalità NIDS/NIPS per la riduzione dei falsi positivi.
- **Interazione con il servizio Threat Intelligence & Vulnerability Data Feed L1.S5**: gli IoC dei data feed intelligence sono condivisi con le piattaforme di gestione FortiAnalyzer (post-mortem) e con gli appliance FortiGate (real time) per la ricerca di eventi di compromissione.
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6**: l'interazione avviene secondo le stesse modalità descritte al precedente punto "Interazione con il servizio Web Application Firewall L1.S3".
- **Interazione con il servizio Protezione degli End Point L1.S13**: Qualora la FortiSandbox rilevi una minaccia zero-day, a seguito di un'analisi eseguita su un file proveniente dal servizio NGFW, e conseguentemente produce e rende disponibile una nuova firma/IoC, questa potrà essere utilizzata per alimentare la base di conoscenza della Trend Micro Sandbox Deep Discovery Analyzer (cfr. cap.13) al fine di consentire la protezione anche degli End-Point. Tale interazione è bidirezionale.

6.3. CAPACITÀ DI FORNIRE VISIBILITÀ E CONTROLLO DEGLI UTENTI PER CREARE POLICY, GENERARE REPORT ED ESEGUIRE INDAGINI FORENSI

Il servizio NGFW dispone di una funzionalità avanzate legata alla **User Identity** che consente al RTI di fornire un elevato livello di visibilità ed un granulare controllo degli utenti. L'autenticazione è un processo necessario a confermare l'identità di un utente per garantire che abbia accesso solo alle risorse a cui è autorizzato ad accedere. L'autenticazione degli utenti dell'Amministrazione avviene attraverso l'integrazione diretta con i sistemi esistenti presso l'Amministrazione (ad esempio LDAP, RADIUS, TACACS+, AD o POP3). In questo caso l'appliance FortiGate invia le credenziali immesse dall'utente al server esterno in modalità cifrata ed il server esterno risponde indicando se le credenziali fornite sono valide o meno. In ambiente Microsoft Active Directory è inoltre possibile configurare strategie di SSO per permettere l'autenticazione trasparente senza impatti sulla user-experience.

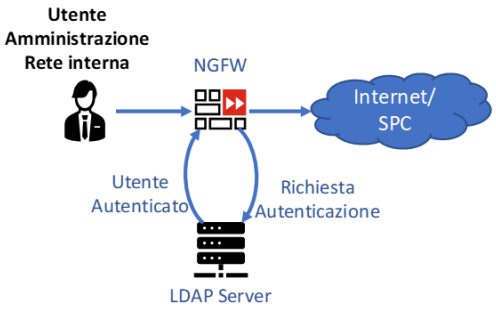

Figura 18 – Interazione NGFW-LDAP

Una volta introdotta la configurazione della **user identity** è possibile la **configurazione di policy specifiche associate a utenti e/o gruppi** al fine di applicare controlli mirati e gestirne le autorizzazioni. Inoltre, il campo "user" consente la generazione di **report specifici relativi agli utenti** ed arricchisce ogni log di traffico con l'informazione relativa all'utente che lo ha generato. Tali log

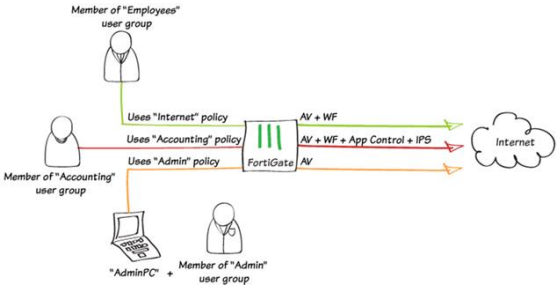

Figura 19 – Esempio di Policy per User

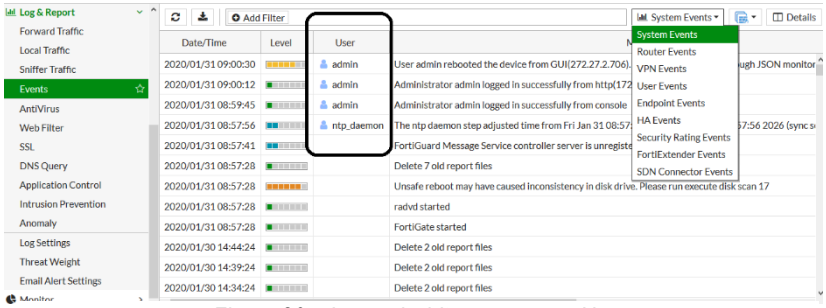

Figura 20 – Log arricchito con campo User

racchiudono quindi tutte le informazioni necessarie all'esecuzione di eventuali **indagini forensi** a seguito di incidenti informatici. Utilizzando la componente dedicata FortiAnalyzer del sistema di gestione, oltre alla capacità di memorizzare i log per un periodo di almeno sei mesi, è garantita l'applicazione della pseudoanonimizzazione dei dati secondo la normativa GDPR. I dati raccolti vengono trattati garantendo cifratura, integrità e non alterabilità; gli apparati NGFW inviano i log al FortiAnalyzer con protocollo proprietario che sfrutta la crittografia TLS/SSL, quindi il trasferimento dei log è cifrato dalla sorgente al log collector (FortiAnalyzer). Il dato viene immagazzinato in un file reso non modificabile in base a politiche di natura dimensionale oppure temporale. Al file così creato, viene applicato un hash (log checksum) per cui sarà possibile verificarne l'integrità al momento in cui sarà necessario importarlo per una eventuale ricerca forense.

7. PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL"

Il servizio di Web Application Firewall (WAF) ha come obiettivo principale quello di proteggere le applicazioni Web esposte su Internet da attacchi specifici al protocollo HTTP/HTTPS e relative anomalie allo stack applicativo, come ad esempio: SQL Injection, Cross-site Scripting (XSS), accesso illegale alle risorse e bot malevoli. L'approccio completo alla protezione delle applicazioni web prevede varie opzioni come la validazione dei metodi HTTP permessi, l'API protection, la firma/criptazione dei cookies e la gestione di meccanismi di accesso alle URL riservate tramite definizione di regole 'custom' specifiche.

Il servizio WAF permette la capacità di controllo degli attacchi **DoS/DDoS** in particolare a livello applicativo (livello 7 ISO/OSI) ed il motore di riconoscimento di tali attacchi è in grado di analizzare le connessioni e permette di controllare le seguenti condizioni: ✓Le richieste HTTP per sorgente; ✓Limitare il numero massimo di connessioni TCP per sessione HTTP attraverso il cookie di sessione; ✓Limitare il numero di richieste HTTP per secondo, per sessione, per URL; ✓Limitare il numero di connessioni TCP per client; ✓Riconoscere se il client è effettivamente un internet browser (real browser enforcement) effettuando sfide al client attraverso javascript.
È inoltre disponibile la possibilità di analizzare la nazione di origine del DDoS e di imporre blocchi sulla stessa.
Il servizio WAF, proposto dal RTI, sarà erogato attraverso il prodotto **FortiWeb** (hardware appliance o virtual appliance on premise) di **Fortinet**. La gestione del servizio viene effettuata mediante la console di management centralizzata **FortiWeb Manager**, attraverso VPN create su connettività INTERNET o SPC e terminate, lato Centro Servizi, sui concentratori attestati sull'infrastruttura di management del servizio.
L'infrastruttura di erogazione del servizio di Web Application Firewall si avvale delle componenti di seguito descritte:

- **FortiWeb Manager:** FortiWeb Manager è una console web che consente di gestire centralmente più dispositivi FortiWeb in remoto. Gli amministratori possono controllare i propri dispositivi (eventualmente, raggruppati logicamente), gestire job e licenze, effettuare upgrade di firmware e signature, controllare rapidamente i vari log e monitorare le statistiche sulle minacce in tempo reale.
- **FortiSandbox** – Il componente FortiSandbox costituisce parte integrante dell'architettura Fortinet Security Fabric e utilizza tre modalità di intelligence sulle minacce per il rilevamento e la prevenzione degli Incidenti di sicurezza (cfr. cap.6).
- **Repository di utenze e dati**: conserva le informazioni più rilevanti (contatti referenti, IP, FQDN, template usato nella configurazione, etc.) relative alle applicazioni di cui sia stato effettuato il provisioning.
- **Appliance FortiWeb Web Application Firewall**: Gli apparati Web Application Firewall rappresentano un elemento chiave nella realizzazione di una piattaforma di sicurezza che, insieme agli altri servizi costituisce un ecosistema di sicurezza "collaborativa" che permette di correlare le informazioni di security tra i diversi servizi
  Nella tabella seguente si riportano le appliance proposte dal RTI per le diverse fasce:

Fasce	Fortinet appliance
Fascia 1: fino a 500 Mbps	FortiWeb-600E
Fascia 2: fino a 5 Gbps	FortiWeb-2000F
Fascia 3: fino a 10 Gbps	FortiWeb-3000F

Tabella 12 – Appliance e throughput previste per il servizio WAF

Il RTI vanta una vasta e profonda esperienza nella erogazione di servizi WAF, in particolare nel comparto della Pubblica Amministrazione. AlmavivA, aggiudicataria in qualità di mandataria dell'accordo quadro SPC Lotto 3 e Lotto 4 ha realizzato e attualmente gestisce presso il proprio Centro Servizi il servizio WAF per importanti portali di primarie amministrazioni centrali, quali MAECI (portale ItalyExpoDubai), portale istituzionale AIFA, Dipartimento della funzione pubblica, IVASS, Consip, MIUR, Presidenza Consiglio dei Ministri (portale G20 e inPA-Portale del Reclutamento) e locali quali Regione Calabria, Campania, Sardegna, Sicilia, Provincia di Como, Comune di Roma e Palermo. Il RTI ha quindi una profonda conoscenza ed esperienza con la tecnologia scelta per questa fornitura oltre ad una consolidata partnership con il vendor. Oltre a rispettare pienamente i requisiti del Capitolato, il servizio WAF proposto dal RTI presenta una serie di caratteristiche tecnologiche e prestazionali migliorative come meglio descritto nel seguito. Tale servizio è caratterizzato dall'utilizzo di un approccio strutturato e integrato con i servizi oggetto di fornitura e **fortemente orientato agli aspetti della sicurezza applicativa WEB** e non solo alla protezione infrastrutturale e di rete. Le scelte architetturali per l'implementazione del servizio, la definizione delle misure e delle regole di protezione e le modalità operative di gestione del servizio stesso discendono da una precisa strategia progettuale. Quest'ultima, infatti, come illustrato in figura, tiene conto dei requisiti e vincoli di sicurezza del cliente e degli scenari delle minacce alle applicazioni che sono in continua evoluzione. A questo riguardo il servizio è progettato per operare con la massima efficacia sia come singolo servizio che, come meglio specificato nel seguito del presente capitolo, mediante l'**interazione in forte sinergia con gli altri servizi** della fornitura.

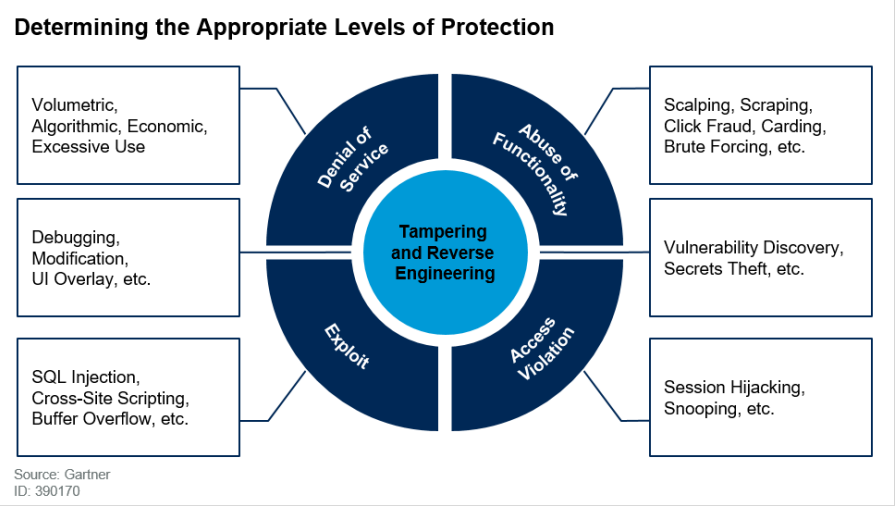

Figura 21 – Decision Point for Deploying WAFs for Application Protection, Gartner 2019

7.1. CARATTERISTICHE TECNOLOGICHE E PRESTAZIONALI MIGLIORATIVE

La soluzione tecnologica adottata dal RTI, oltre a garantire la disponibilità di tutte le funzionalità richieste da Capitolato Tecnico, si caratterizza per una serie di aspetti migliorativi che la pongono all'avanguardia nella erogazione del servizio oggetto del presente paragrafo, in particolare, sotto i punti di vista di:

- **Innovatività e resilienza**: ✓è fornito il riconoscimento evoluto dei Good-Bot dei motori di ricerca noti (es. Google, Yahoo, etc.) e dei Bad-Robots (scanners, crawlers, spiders). Un cruscotto mostra, a livello statistico la ripartizione del traffico tra utenti reali e robot; ✓sono disponibili funzionalità per la prevenzione dalla fuga di diverse tipologie di dato (es. lista directory, dati relativi alla disponibilità e agli errori delle applicazioni, codice sorgente

ASP/JSP, carte di credito); ✓è fornito il supporto alla georeferenziazione degli IP con possibilità di blocco a livello geografico ed analisi dei log basata su dati geografici e il blocco per IP reputation basata sulla categorizzazione del servizio di intelligence Fortinet fornita tramite FortiGuard; ✓è gestita la prevenzione da attacchi brute-force login: la funzionalità tiene traccia della velocità con cui ciascun indirizzo IP sorgente effettua richieste per URL specifici; se l'indirizzo IP di origine supera la soglia, il WAF penalizza l'indirizzo IP di origine bloccando le richieste aggiuntive per il periodo di tempo indicato in configurazione; ✓sono presenti funzioni di offloading dell'autenticazione così da impedire l'accesso ai server da parte di client non autenticati; sono incluse anche funzionalità di supporto al Single Sign-On (sono supportati meccanismi di autenticazione attraverso protocollo LDAP e Active Directory, RADIUS ed NTLM); ✓il livello del log degli eventi è molto dettagliato ed è consentito l'oscuramento di dati sensibili quali password e altre informazioni personali (GDPR); ✓è prevista la verifica della conformità alle HTTP RFC al fine di verificare l'eventuale codice malevolo contenuto nelle connessioni; ✓è disponibile una funzione di protezione dal Web Defacement.

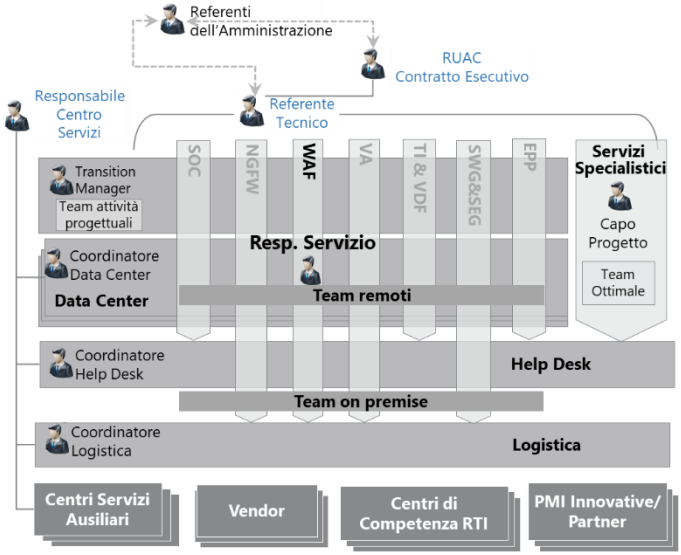

Figura 22 – Organizzazione del servizio

- **Configurabilità**: ✓è possibile definire regole e firme personalizzate, così da garantire l'aderenza a contesti diversi e prevenire falsi positivi; ✓è disponibile la possibilità di gestire eccezioni a vari livelli al fine di eliminare blocchi indesiderati. Le eccezioni per le firme creano dei log a disposizione per analisi da parte degli amministratori; ✓è possibile intervenire con regole di rewrite e reindirizzamento sul flusso http. Ad esempio, è possibile reindirizzare in https il traffico http, restituire pagine in response custom a fronte di particolari condizioni configurabili, modificare alcuni contenuti della response http.
- **Prestazioni e robustezza**: ✓gli apparati FortiWeb previsti offrono prestazioni migliorative in termini di throughput nell'ambito della fornitura in fascia 1, che risulta superiore del 50%, ed in fascia 3 (cfr. 7.3); ✓sono supportate architetture in alta disponibilità secondo due modalità: Active/Passive e Active/Active; ✓possono essere definite regole di compressione e caching in modo molto granulare, così da poter decidere quali siano le risorse cui applicare le funzionalità in oggetto e poter escludere tutti gli oggetti dinamici e, comunque, quelli che non possono essere elaborati attraverso caching e/o compressione.

Nella tabella successiva si evidenzia il miglioramento delle performance in termini di throughput

Fasce	WAF Throughput migliorativi
Fascia 1: fino a 500 Mbps	750 Mbps (+**50%**)
Fascia 2: fino a 5 Gbps	5 Gbps (in linea)
Fascia 3: > di 5 Gbps	10 Gbps (+**100%**)

Tabella 13 – Throughput migliorativi per il servizio WAF

7.2. PROTEZIONE DA EXPLOIT ZERO-DAY, INFEZIONI DA MALWARE E VULNERABILITÀ

Il servizio WAF implementa un modello di protezione ibrido che applica sia meccanismi negativi (blocco di ciò che è conosciuto come malevolo in base a signature) che positivi (è possibile definire il traffico autorizzato e bloccare quello non autorizzato, quindi anche gli attacchi zero-day). La protezione da zero-day è realizzata mediante funzionalità di input validation e parameter validation che bloccano eventuali richieste malformate.

Sono, inoltre, disponibili controlli di tipo sintattico, non basati su pattern, volti a prevenire attacchi di tipo XSS o SQL Injection.

Sono fornite anche funzionalità di machine learning volte a rilevare automaticamente traffico web pericoloso e attacchi provenienti da Bot.

Il modello di *rilevamento delle anomalie* osserva URL, parametri e metodi delle sessioni HTTP e/o HTTPS verso i server Web protetti e utilizza un meccanismo di apprendimento automatico per rilevare il traffico anomalo. Per riconoscere una richiesta come legittima o come potenziale attacco, esegue le seguenti azioni in automatico:

1. Acquisisce e raccoglie input, quali ad esempio i parametri delle URL o i metodi utilizzati, e crea un modello matematico che descrive il corretto utilizzo dei servizi protetti;
2. Rileva eventuali anomalie rispetto al modello precedente e le confronta con modelli pre-costruiti che descrivono le tipologie di minacce conosciute;
3. Rileva eventuali attacchi in base alla correlazione in tempo reale di entrambi i modelli.

L'utilizzo di questa tecnologia, resa disponibile dal FortiWeb, consente di indirizzare attacchi di tipo zero-day con una minimizzazione di falsi positivi.

Il modello di *rilevamento dei bot*, invece, osserva e traccia i comportamenti degli utenti su diverse dimensioni, ad esempio: quante volte le richieste HTTP vengono generate dall'utente, se le richieste utilizzano versioni HTTP illegali, se la richiesta recupera risorse JSON/XML, etc.

A differenza dei meccanismi tradizionali per il rilevamento dei bot, il sistema basato su intelligenza artificiale consente di evitare l'operazione manuale di tuning delle soglie per distinguere le attività lecite da quelle illecite.

Va evidenziato che sul WAF FortiWeb è disponibile, inoltre, una funzione nativa di scansione sugli allegati finalizzata ad individuare virus, malware e grayware sulla base di signature presenti in un database aggiornato automaticamente attraverso una connessione ai laboratori di intelligence FortiGuard.

Infine, il servizio di WAF FortiWeb può utilizzare le funzioni di Forti-Sandbox al fine di migliorare ulteriormente le capacità di identificazione di Zero-Day.

7.3. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il servizio WAF proposto dal RTI viene erogato dal Centro Servizi del Fornitore. Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT (SGS-IT)** conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

Organizzazione del servizio

L'organizzazione del servizio WAF, suddiviso per fasi:

Presa in carico del servizio

- *Acquisizione*, attraverso il *Team on-premise* (cfr. § 4), *di know how relativo al contesto*: il responsabile del servizio WAF invia un documento template al Referente dell'Amministrazione affinché, per ogni applicazione web da integrare, siano fornite le informazioni di base che innescano il processo: responsabile/referente dell'applicazione, IP/FQDN cui risponde ogni applicazione.
- *Predisposizione e configurazione del servizio e delle relative piattaforme di management*: il *WAF Team* procede alla configurazione di base dell'apparato dopo averne assicurato la raggiungibilità da remoto. Questo comporta, oltre alla definizionecoordinatore delle utenze amministrative necessarie, la configurazione di policy standard di base e di policy template rispondenti alle principali casistiche delle applicazioni web da integrare (ad esempio portali CMS, servizi Web, applicazioni transazionali autenticate e non, applicazioni con architetture a microservizi) da utilizzare a modello per le singole integrazioni di applicazioni, l'integrazione del sistema SIEM di riferimento per l'esportazione degli eventi relativi alle applicazioni ed alle operazioni di configurazione effettuate dagli amministratori WAF. Il *Team on-premise* gestisce l'installazione delle componenti previste on-site secondo il piano di installazione condiviso con l'Amministrazione. Gli apparati WAF saranno resi raggiungibili, presi in carico dal sistema di management e configurati da remoto. Il servizio sarà predisposto sulla base di quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano.
- *Migrazione*: nel caso che l'Amministrazione chieda al Fornitore di subentrare da una precedente installazione WAF propria o di terza parte, il Team on-premise e il WAF Team predispongono un processo di verifica delle configurazioni implementate allo scopo di appurarne l'efficacia (si rende utile, allo scopo, il servizio di Gestione continua delle vulnerabilità di sicurezza), la necessità di ottimizzazione prestazionale, la possibilità di integrazione con gli altri servizi. È possibile prevedere una migrazione su apparati proposti dal RTI.

Erogazione del servizio:

- *Provisioning di una configurazione aggiuntiva*: il responsabile del servizio WAF intervista il referente della applicazione usando un formulario (checklist) mirato a stilare le caratteristiche funzionali, architetturali e dimensionali dell'applicazione in oggetto. Tali caratteristiche saranno analizzate al fine di definire una proposta di configurazione che sarà trasmessa al referente. In funzione delle caratteristiche delle policy di sicurezza individuate e approvate dal referente, sarà proposto un processo graduale di attivazione in modalità 'prevent' delle regole. Alcune di esse, infatti, necessiteranno di un periodo di monitoraggio (operato sia tramite le dashboard del WAF stesso, sia tramite alert e report del SIEM) durante il quale saranno configurate in modalità 'detect'. Tale periodo di osservazione, potrà comportare l'affinamento delle stesse a seguito di osservazione (e convalida da parte del referente applicativo) di falsi positivi. L'effettivo onboarding dell'applicazione su WAF comporterà l'interazione con altri servizi della fornitura descritti nel seguito.
- *Conduzione operativa e sistemistica della piattaforma*: ✓monitoraggio della disponibilità e delle prestazioni; ✓applicazione di patch sia a fronte di segnalazione del vendor che di manutenzione in seguito a malfunzionamenti.
- *Supporto alla gestione incidenti*: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓produzione di reportistica per l'Amministrazione, realizzata sulla base di una serie di template standard definiti in fase di progetto esecutivo. Se l'Amministrazione ha aderito al servizio SOC, la reportistica verrà prodotta mediante l'integrazione con il SIEM del Centro Servizi; ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

Modalità di erogazione

La modalità di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓installazione di appliance dedicati fisici o virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione; ✓utilizzo di una istanza del servizio WAF installata presso il Centro Servizi del RTI ed acceduta in modalità SaaS. L'architettura di default proposta dal RTI è quella on premise.

In fase di definizione del progetto esecutivo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono:

✓fascia di throughput richiesta; ✓tipologia dei servizi web da proteggere, se cioè occorre proteggere servizi esposti su internet o servizi interni del cliente; ✓numerosità delle web application da proteggere.

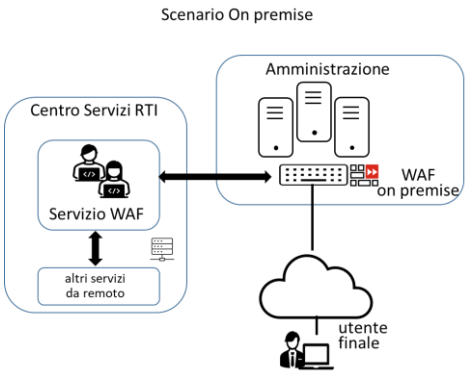

Figura 23 – Modalità di erogazione

Interazione con gli altri servizi

Si riportano di seguito le interazioni principali del Servizio Web Application Firewall verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Security Operation Center L1.S1".
- **Interazione con il servizio Next Generation Firewall L1.S2**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Web Application Firewall L1.S3".
- **Interazione con i servizi Gestione continua delle Vulnerabilità di Sicurezza L1.S4**: Le evidenze dei WAF saranno rese disponibili in maniera da consentire eventuali correlazioni, con un approccio olistico e a 360 gradi rispetto alla superficie di attacco.

  Dal servizio di gestione delle Vulnerabilità verranno recepite eventuali vulnerabilità di natura infrastrutturale e applicativa rilevate durante le scansioni periodiche al fine di implementare, in accordo con la PA, delle regole temporanee di mitigazione (virtual patching) nelle more della realizzazione di un piano di rientro definitivo da parte del personale incaricato dalla PA per la manutenzione correttiva/evolutiva. Inoltre, sarà possibile ridurre il numero dei falsi positivi grazie all'output del VA recepiti dal WAF.
- **Interazione con il servizio Threat Intelligence & Vulnerability Data Feed L1.S5**: L'interazione avviene tramite la FortiSandbox e consente di aumentare la base di conoscenza del servizio WAF per prevenire e mitigare gli incidenti di sicurezza, ad esempio, da malware zero-day.
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Web Application Firewall L1.S3".
- **Interazione con il servizio "Protezione degli End Point" L1.S13**: l'interazione avviene secondo le stesse modalità descritte nel paragrafo 6.2 al punto "Interazione con il servizio Protezione degli End Point L1.S13".

8. PROPOSTA PROGETTUALE PER IL SERVIZIO "WEB APPLICATION FIREWALL" - FUNZIONALITA' AGGIUNTIVE

Si conferma la disponibilità di funzioni di "Protezione dagli attacchi DDOS - Distributed Denial of Service" per il servizio WAF (cfr. cap.7).

9. PROPOSTA PROGETTUALE PER IL SERVIZIO "GESTIONE CONTINUA DELLE VULNERABILITA' DI SICUREZZA"

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

9.1. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI** conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale**)** dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT (SGS-IT)** conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

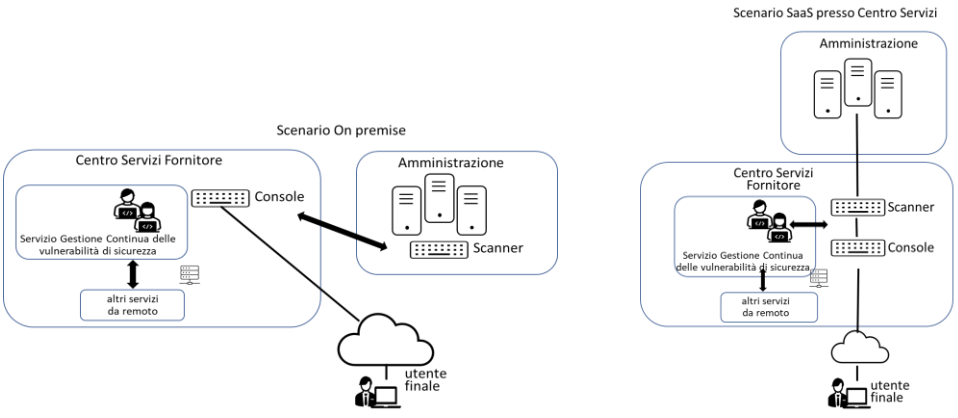

Figura 24 – Modelli di erogazione del servizio VA

Il **modello operativo** di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓installazione di appliance dedicati virtuali on premise presso la sede dell'Amministrazione o presso il cloud dell'Amministrazione, architettura di default proposta dal RTI in caso di IP privati; ✓utilizzo di una istanza del servizio installata presso il Centro Servizi del RTI, architettura di default proposta dal RTI in caso di IP pubblici.

In fase di definizione del Piano Operativo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono: ✓frequenza delle analisi richieste per il modello continuativo; ✓tipologia di esposizione dei target analizzati (reti private o pubbliche); ✓numerosità dei sistemi da analizzare.

L'organizzazione del servizio si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- **Manleva:** sarà richiesta la sottoscrizione di una manleva al fine di procedere con l'erogazione del servizio.
- **Referenti:** vengono definiti i referenti del servizio che potranno accedere ai risultati in tempo reale tramite dashboard, gestire le pianificazioni e le scansioni e ricevere i report.
- **Target:** si definiscono la lista degli IP dei sistemi che dovranno essere sottoposti ad analisi
- **Frequenza:** si definisce la frequenza con cui gli IP saranno analizzati

Erogazione del servizio:

- **Scansione**: vengono eseguite analisi e verifiche di sicurezza dei sistemi oggetto del servizio, senza soluzione di continuità e con la frequenza definita dalle PA.
- **Interruzione d'emergenza:** Le Amministrazioni potranno richiedere la sospensione delle analisi in caso di criticità.
- **Richieste di modifica della configurazione:** Le Amministrazioni potranno aggiornare le politiche di sicurezza utilizzando il portale dei servizi di sicurezza (in caso di contestuale acquisizione del servizio SOC) o mediante l'apertura di un ticket. La richiesta sarà presa in carico dal team specialistico che, una volta effettuate le necessarie attività, provvederà a darne comunicazione al referente dell'Amministrazione in funzione del canale di ingaggio.

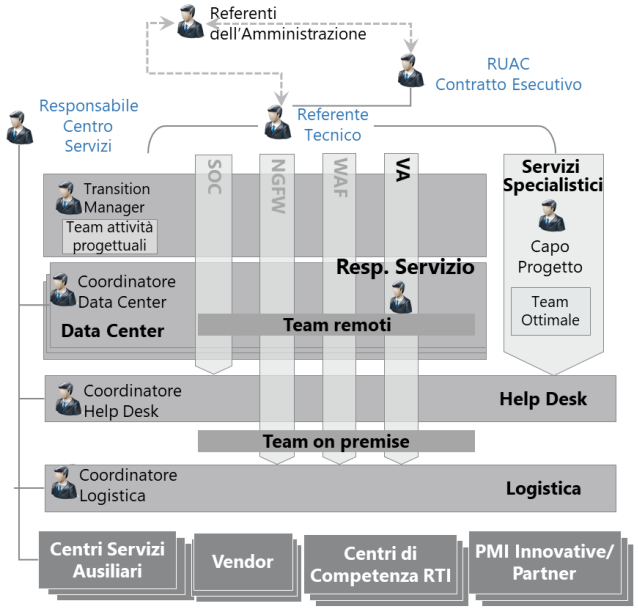

Figura 25 – Organizzazione del servizio VA

- **Reporting:** La reportistica permette di verificare il livello di sicurezza dei sistemi, riportando ogni vulnerabilità rilevata. La reportistica prevede report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), ad esempio evidenziando lo stato su base dello storico delle vulnerabilità, quali ad esempio vulnerabilità nuove e vulnerabilità sanate. La piattaforma offre un sistema di reporting basato su modelli che possono produrre report tecnici altamente dettagliati, scorecard sintetiche per i C-Level, VP-Level, D-Level, Manager, Technical SME-Level (es: CISO, CTO, CIO, DPO, etc.). Tutti gli elementi grafici o testuali possono essere selezionati singolarmente (es. solo le vulnerabilità critiche) ed ordinati. È possibile pianificare la generazione dei report ed il reperimento in diversi formati, inclusi HTML, PDF, CSV e formati XML, inoltre via API possono essere generati e scaricati automaticamente. Tutti i dati delle scansioni, indipendentemente dalla sorgente, vengono memorizzati e consolidati in modo sicuro in un singolo database, gestito in conformità con le primarie compliance di settore (GDPR, PCI-DSS, HIPAA, HITECH, SOX, ISO, GLBA, CobiT), all'interno del Centro Servizi. La reportistica sarà inviata automaticamente dal Centro Servizi, ai referenti del servizio, tramite e-mail, al termine di ogni singola scansione. Le Amministrazioni, come valore aggiunto, possono ottenere la reportistica anche accedendo alla Console nel Centro Servizi, in modo:
  - **Real time:** per visualizzare sia i risultati sia lo stato delle scansioni, in tempo reale, accedendo alla Dashboard interattiva
  - **On Demand**: per scaricare i risultati delle analisi completate

Il servizio è erogato in modalità SaaS dal Centro Servizi e può analizzare il livello di rischio sia di sistemi esposti su internet sia sistemi interni all'Amministrazione.

Nel caso di IP esposti su Internet, il servizio viene erogato tramite scanner abilitati al traffico Internet, tale configurazione non richiede l'uso di scanner dedicati per le Amministrazioni. Nel caso di IP privati delle Amministrazioni invece, ad ogni Amministrazione sarà messo a disposizione un proprio scanner virtuale su cui sarà applicata una configurazione VPN (Virtual Private Network) per consentire la raggiungibilità dal Centro Servizi.

Questa soluzione, quindi, consente di coniugare i benefici di una soluzione centralizzata (Console), con la scalabilità derivante da una soluzione multi-tenant.

Il servizio sarà basato sulla piattaforma Tenable.sc, la miglior piattaforma disponibile oggi sul mercato per rilevare e gestire le vulnerabilità, indicata nella The Forrester Wave™ come Leader di Vulnerability Risk Management, con la miglior strategia e la miglior offerta oggi disponibile su scala mondiale. Caratteristiche fondamentali e distintive della piattaforma sono:

1. capacità di verificare più di 65.000 vulnerabilità;
2. capacità di rilasciare tempestivamente aggiornamenti mantenendo una copertura accurata nel rilevamento delle vulnerabilità. La Tenable.sc Research Organization produce aggiornamenti in 12-72 ore dalla divulgazione della vulnerabilità/data di pubblicazione del fornitore, ciò include vulnerabilità di alto profilo e avvisi di fornitori standard come Microsoft Patch Tuesday, CPU Oracle, avvisi di sicurezza della distribuzione Linux/Unix e altri;
3. Disponibilità della Predictive Prioritization, che consente di concentrare i propri sforzi in base alle vulnerabilità che è più probabile che vengano sfruttate, che avrebbero un impatto maggiore. La Predictive Prioritization combina dati provenienti da varie fonti, includendo lo standard CVSS, che in ogni caso è disponibile anche esplicitamente. Inoltre essa analizza oltre 111.000 vulnerabilità distinte ogni 24 ore per aggiornare costantemente il mutevole panorama delle minacce, riducendo del 97% il numero di vulnerabilità critiche e alte che le Amministrazioni dovranno correggere.

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

- **Scanner** – Software reso disponibile su sistema virtuale dell'Amministrazione e presente di default nel Centro Servizi, che esegue le verifiche di sicurezza sui dispositivi raggiungibili ed identificati come target, tramite comunicazioni basate su protocollo IP. La soluzione abilita le Amministrazioni a: ✓analizzare sia sistemi esposti su Internet sia sistemi interni; ✓eseguire ricerche di vulnerabilità sui propri sistemi senza soluzione di continuità.

- **Console** - Piattaforma centralizzata multi-tenant istanziata presso il Centro Servizi del RTI, utilizzata per la gestione del servizio. Consente la separazione logica delle PA contraenti in domini distinti (Tenant) garantendo la segregazione completa dei dati. È una singola console di management che consente di gestire dispositivi Scanner e fornire funzionalità di settings e update centralizzato per tutti gli apparati gestiti. Il modulo contiene la base dati con le configurazioni, l'asset inventory, le pianificazioni, i profili di analisi, la base di conoscenza delle vulnerabilità pubblicamente note su scala internazionale, la base dati delle verifiche possibile sui sistemi, il motore di generazione ed invio della reportistica, l'archivio dei risultati delle analisi eseguite, i feed ed i contenuti di Cyber Threat Intelligence per estendere la soluzione proposta con metodi di interoperabilità. Include una interfaccia web per gli utenti per consentire di interagire con la piattaforma, di visualizzare in tempo reale i risultati, lo stato delle scansioni, le pianificazioni e le configurazioni.

Monitoraggio e scansione degli asset

La soluzione implementa funzioni di network discovery, definizione di policy di compliance e auditing, asset inventory, gestione delle vulnerabilità, gestione dei certificati TLS/SSL, asset management, gestione delle credenziali per accessi ai sistemi, gestione di rete per scanner multipli, remediation tracking e integrazione con LDAP.

Per assicurare costantemente il monitoraggio degli asset, la piattaforma offre:

- un sistema integrato di calendarizzazione degli eventi tramite cui le Amministrazioni avranno la possibilità di pianificare le proprie scansioni sui propri sistemi;
- un sistema integrato di feed che consente di ricevere dati sempre aggiornati su scala internazionale, con dettagli tecnici relativi all'enumerazione e all'analisi di sistemi operativi, applicazioni, software, configurazioni, servizi, etc.

La piattaforma ha la capacità di eseguire scansioni multiple in parallelo sui diversi sistemi target, attraverso sia gli scanner posizionati presso le Amministrazioni, sia utilizzando gli scanner esposti su Internet.

La soluzione è in grado di scansionare un elevato numero di sistemi operativi, identificando le vulnerabilità esposte da software e servizi di apparati connessi alla rete, siano essi server, client, database, web application, application server, etc.

Il servizio ha la capacità di classificare i rischi individuando i livelli di gravità, tramite uno standard denominato Common Vulnerability Scoring System (CVSS), già calcolato per ogni vulnerabilità rilevata, con l'ultima versione disponibile, la versione 3.1.

Per una completa contestualizzazione delle minacce, quindi per una chiara interpretazione degli impatti associati alle vulnerabilità, la piattaforma fornirà i seguenti dettagli:

- CVSS Base: un valore da 1 a 10 in cui 10 rappresenta il livello più critico di una vulnerabilità
- CVSS Base Vector: una stringa che consente di conoscere gli impatti RID della vulnerabilità, quindi gli impatti che lo sfruttamento di tale vulnerabilità potranno avere su Riservatezza, Integrità e Disponibilità;
- CVSS Origin: l'ente accreditato che ha elaborato la contestualizzazione della vulnerabilità, prevalentemente ad opera del National Vulnerability Database, repository governativo statunitense dei dati delle vulnerabilità basati sullo standard del Security Content Automation Protocol.
- CVSS Date: la data di classificazione del rischio della vulnerabilità

La soluzione consente di creare Profili che contengono le istruzioni relative alla modalità operativa dell'attività di scansione; in particolare è possibile personalizzare il numero di porte (TCP, UDP), le vulnerabilità da ricercare o ignorare, gli apparati da utilizzare singolarmente o in combinazione per la scansione, il livello di performance desiderato (ovvero le impostazioni dei limiti alle performance per ridurre l'impatto sul network).

Interazione

Si riportano di seguito le interazioni principali del Servizio Gestione continua delle vulnerabilità di sicurezza verso gli altri servizi le cui modalità sono descritte nei paragrafi specificati in elenco: ✓**Interazione con il servizio "Security Operation Center" L1.S1**: (cfr. § 6.2); ✓**Interazione con il servizio Next Generation Firewall L1.S2** (cfr. § 6.2); ✓**Interazione con il servizio Web Application Firewall L1.S3**: (cfr. § 7.3).

9.2. DISPONIBILITÀ DI CRUSCOTTI DINAMICI CHE CONSENTANO DI MONITORARE LA SUPERFICIE VULNERABILE IN TEMPO REALE

Le dashboard della Console consentiranno di default il monitoraggio della superficie d'attacco indicata dal referente della PA, in tempo reale e in modalità interattiva.

La piattaforma offre inoltre la possibilità di organizzare e visualizzare le informazioni più rilevanti in funzione del destinatario. I cruscotti possono essere personalizzati, resi accessibili e condivisi con gli altri utenti autorizzati. Le dashboard consentono di visualizzare informazioni provenienti dalle diverse applicazioni in un'unica schermata, offrendo un framework omogeneo oltre che una visione olistica e generale della postura di sicurezza.

Le dashboard possono essere modificate anche tramite query che consentono di portare in evidenza politiche, standard e linee guida adottate dalle singole Amministrazioni, ciò consente una visualizzazione dei risultati allineata ai processi di manutenzione delle Amministrazioni.

Le dashboard rappresentano graficamente numerosi dati, tra cui: principali vulnerabilità rilevate, distribuzione delle vulnerabilità sui sistemi, variazione delle vulnerabilità nel tempo, i protocolli più

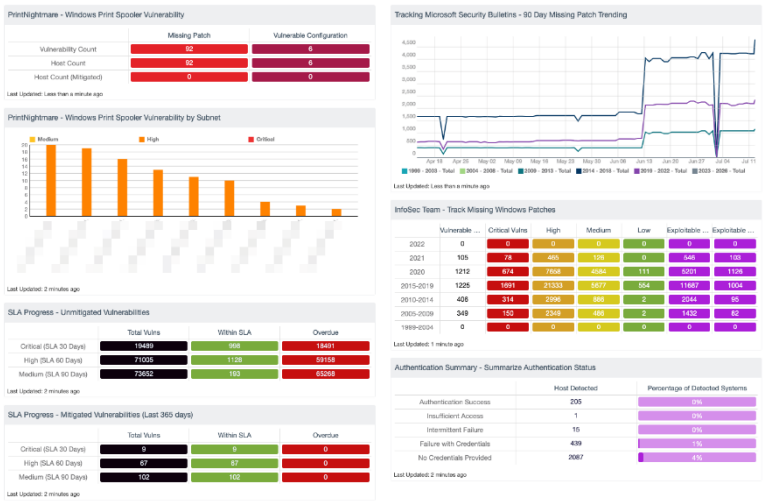

Figura 26 – Dashboard

vulnerabili, le vulnerabilità più frequenti, i software più vulnerabili, i sistemi operativi maggiormente impattati dalle vulnerabilità, i sistemi più vulnerabili, le remediation più importanti non ancora applicate, etc.
Tenable.sc fornisce di default oltre 400 dashboard personalizzabili e oltre 200 template di reportistica.

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

Il servizio predisposto dal RTI offre alle PA una soluzione end-to-end per definire, monitorare, analizzare e migliorare il proprio livello di sicurezza cyber complessivo secondo un approccio predittivo e di analisi di contesto, seguendo logiche cyber-intelligence driven ad ampio spettro. In aggiunta, sfruttando tecniche e strumenti di automazione, consente di definire un livello di rischio in maniera statica e di studiarne le evoluzioni nel corso del tempo, grazie ad un monitoring costante della security posture di una specifica Amministrazione. Il servizio consente di identificare e definire eventuali minacce esterne, accertare le proprie aree di vulnerabilità e i propri asset a rischio di esposizione e compromissione. Il servizio si basa su una **Threat Intelligence Platform** consolidata in ambito internazionale per la collaborazione dei **CSIRT** e l'Info Sharing, denominata **Joshua CybeRisk Vision™**. La soluzione è sviluppata a partire dal 2018 ed ha consentito negli ultimi due anni di enumerare, analizzare e contestualizzare gli asset e definire la postura delle Top 500 PMI in Italia. L'efficacia di tale soluzione è ampiamente osservabile nei contesti moderni che includono il Cloud Computing, in particolare nella capacità di rilevare i sistemi Shadow IT, sistemi al di fuori del governo di un'organizzazione.
Le Amministrazioni che adotteranno questo servizio potranno arricchire i propri apparati infrastrutturali tramite un flusso informativo con dati di minacce globali, forniti dai principali attori internazionali di Info Sharing. In aggiunta, si rendono disponibili in forma esclusiva dati su minacce afferenti sistemi informativi italiani, in particolare flussi contenenti dati sulle minacce attive ai danni della Pubblica Amministrazione.
Il servizio proposto facilita lo scambio e la condivisione di informazioni sulle minacce, Indicatori di Compromissione (IoC) su malware e attacchi mirati come ad esempio frodi finanziarie. La condivisione è basata su un modello distribuito contenente informazioni tecniche e non tecniche che possono essere condivise all'interno di organizzazioni private, semi-private o aperte. Lo scambio di tali informazioni porta a un rilevamento più rapido degli attacchi, riducendo il numero di falsi positivi, e producendo reportistica arricchita grazie a sistemi di automazione e all'ampio utilizzo di standard internazionali, completando il servizio con un sistema integrato di API ReST.
Tramite le informazioni aggiuntive di Intelligence, sarà possibile ricostruire preventivamente la Kill Chain e monitorare eventuali Tattiche, Tecniche e Procedure (TTP) introdotte dai Threat Actor per aggirare i controlli di sicurezza delle Amministrazioni e dei loro fornitori (supply-chain based). Tramite tale servizio saranno resi disponibili feed continuamente aggiornati, con dati di elevato valore e altamente affidabili in quanto prodotti principalmente su dati reali di attacchi rilevati e gestiti, contestualizzati su target italiani. Questo approccio supera qualitativamente le indicazioni globali dei provider internazionali, in particolare supera i data feed basati su sistemi esca non nazionali (Honeypot e Honeynet), che tuttavia sono presenti a completamento del catalogo offerto.
Il servizio genera automaticamente molteplici evidenze di rilevamento delle intrusioni; per esempio, nel caso di sistemi IDS (Intrusion Detection System) sono supportati Indicatori di Compromissione (IoC) basati su IP, domini, nomi di host, user agent, etc. e la generazione di elenchi hash per i valori MD5/SHA1 degli artefatti di file. Le funzionalità API del servizio consentono l'interfacciamento principalmente con strumenti di automazione proposti dal RTI per gli altri servizi in ambito o già in uso presso l'Amministrazione e prevedono una comunicazione di tipo machine to machine, tramite l'uso di opportune chiavi (token) al fine di semplificare il processo di autenticazione.
Elemento distintivo del servizio è la possibilità di ottenere, tramite **Joshua**, per ogni Amministrazione, specifici IoC di **Threat Analytics** per il proprio Sistema Informativo esposto su Internet, indicazioni di **Data Breach** presenti su GitHub, Pastebin o servizi FTP e SMB, gli **Info Leak** su Twitter, gli Asset della PA pubblicamente noti mediante **Postural Assessment**, gli account della specifica PA mediante **Theft Accounts**, minacce agli utenti della PA mediante **Web Malware Detection** sui principali siti della PA. Joshua, erogato nella modalità Threat Intelligence Data Feed, coniuga la capacità di ricercare codici di autenticazione, software, e-mail, dati GDPR rilevanti, etc., sui principali siti utilizzati da sviluppatori e Threat Actor, con la capacità di correlare gli elementi con i dati dello specifico Sistema Informativo esposto su Internet di una PA, **contestualizzando il subset informativo delle minacce**. Saranno infine utilizzate **tassonomie e schemi di classificazione** ben noti per supportare la classificazione standard utilizzata da ENISA, Europol, DHS, CSIRT o molte altre organizzazioni.

10.1. NUMEROSITÀ, TIPOLOGIE E CARATTERISTICHE DEI DATA FEED

Il servizio offre la disponibilità di feed gratuiti, a pagamento, e include Indicatori di Compromissione (IoC), bollettini di sicurezza informatica, e altre informazioni, sia da fonti aperte sia da fonti private.
I data feed sono classificati secondo il Traffic Light Protocol (TLP), un protocollo creato per facilitare una maggiore condivisione delle informazioni. TLP è un insieme di designazioni utilizzate per garantire che le informazioni sensibili siano condivise con il pubblico appropriato ed impiega quattro colori per indicare i limiti di condivisione previsti che devono essere applicati dai destinatari. Il catalogo proposto dispone di **80 data feed**, **classificati TLP: Amber, Green e White**. I dati sorgenti sono principalmente provenienti dal RTI, pertanto focalizzati su dati reali acquisiti su sistemi informativi e riguardante attacchi indirizzati a organizzazioni italiane e **pubbliche amministrazioni**. Sono comunque disponibili dati da sorgenti internazionali, appartenenti ad **enti promotori di Threat Intelligence Information Sharing**.
I Data Feed disponibili out-the-box nella piattaforma includono feed commerciali, con classificazione TLP:Amber e Green, forniti dalle sorgenti Joshua **CybeRiskVision** e **Kaspersky**. Di seguito si riporta il **Catalogo dei Data Feed**:

#	Sorgente	Tipologia		#	Sorgente	Tipologia
1	Kaspersky	Malicious URL		**41**	Blocklist.de	VOIP attack
2	Kaspersky	Phishing URL		**42**	COVID-19 Coalition	Temporary case
3	Joshua	Threat Analytics (Firewall)		**43**	SANS	Handler's Diary
4	Joshua	Threat Analytics (IDS)		**44**	SANS	Up and Coming Ports

5	Joshua	Threat Analytics (AEP)		**45**	SANS	Top 100 Source (NoBlacklist)
6	Joshua	Threat Analytics (Virus)		**46**	SANS	All Source IPs (NoBlacklist)
7	Joshua	Threat Analytics (Exploit)		**47**	SANS	Block List
8	Joshua	Data Breach: GitHub		**48**	US-CERT	All NCAS Products
9	Joshua	Data Breach: Pastebin		**49**	US-CERT	Alerts
10	Joshua	Data Breach (FTP)		**50**	US-CERT	Analysis Reports
11	Joshua	Data Breach (SMB)		**51**	US-CERT	Bulletins
12	Joshua	Info Leak: Twitter		**52**	US-CERT	Tips
13	Joshua	Postural Assessment		**53**	US-CERT	Current Activity
14	Joshua	Theft Accounts		**54**	ICS-CERT	Alerts
15	Joshua	Web Malware Detection		**55**	ICS-CERT	Advisories
16	Telsy/Odino	Network Activity IP		**56**	ICS-CERT	Announcements
17	Telsy/Odino	Network Activity Domini		**57**	malwaredomainlist	Virus
18	Telsy/Odino	Malware Hash		**58**	diamondfox_panels	ioc
19	Telsy/Odino	Detection Rules		**59**	firehol_level1	Network activity
20	Telsy/Odino	Network Activity IP		**60**	cinsscore.com	Network activity
21	CIRCL	All		**61**	alienvault.com	Network activity
22	The Botvrij.eu	All		**62**	Dataplane.org	SSH attack
23	EmergingThreats	Network activity		**63**	Dataplane.org	VOIP attack
24	Dan.me.uk	Tor exit nodes		**64**	Dataplane.org	Mail Server attack
25	Cybercrime	Malware online url		**65**	Dataplane.org	Network activity
26	Phishtank	Phishing url		**66**	Dataplane.org	Other
27	FeodoTracker	Network activity		**67**	Vxvalut	Virus
28	OpenPhish	Phishing url		**68**	Cybercrime-tracker	Virus
29	Bambenekconsulting	Network activity (IP)		**69**	Greensnow.co	Spam attack
30	Bambenekconsulting	Network activity (domain)		**70**	ZeroDot1	Mining
31	Abuse.ch	Malware online url		**71**	CyberCure	Network activity (ip)
32	Mirai Security	Network activity		**72**	CyberCure	Malware online url
33	Malshare	Virus		**73**	CyberCure	Virus
34	Benkow	Virus		**74**	Ipspamlist.com	Network activity
35	Abuse IPDB	Network activity		**75**	MalSilo	Malware online url
36	Blocklist.de	Network activity		**76**	MalSilo	Network activity (ip)
37	Blocklist.de	Spam attack		**77**	MalSilo	Network activity (domain)
38	Blocklist.de	FTP attack		**78**	Ipsum	Network activity (ip)
39	Blocklist.de	Mail Server attack		**79**	DigitalSide	All
40	Blocklist.de	SSH attack		**80**	eCrimeLabs	Metasploit CVE

Tabella 14 – Catalogo dei Data Feed

Il catalogo è **sottoposto periodicamente ad analisi di sovrapposizione** dei dati dei feed, ad oggi la duplicazione dei dati dei diversi data feed è **limitata all'1%.** Si evidenzia che la piattaforma consente un'estensione del catalogo dei data feed attraverso l'inserimento di nuovi flussi eventualmente già nella disponibilità delle Amministrazioni.

10.2. MODALITÀ E FREQUENZA DI AGGIORNAMENTO DEI DATA FEED

I data feed vengono aggiornati in due modalità: automatica e manuale, a seconda della tipologia di feed e delle sorgenti del dato. Nel caso di aggiornamento automatico, sistemi API interrogano e ricevono dati aggiornati da Organizzazioni Sorgenti di data sourcing, nazionali ed internazionali; un esempio è il flusso informativo delle Vulnerabilità note (2002-2021) che include anche la capacità di enumerare sistemi operativi, i software, gli aggiornamenti, arricchiti dai commenti ufficiali dei produttori. Nel caso di aggiornamento manuale, gli analisti del centro di competenza di Advanced Threat Hunting di Joshua CybeRisk Vision arricchiscono i data feed aumentandone i dettagli e la contestualizzazione, in modalità continuativa. La piattaforma prevede di default un aggiornamento della base dati ogni **trenta secondi**, tuttavia, attraverso un sistema parametrico, aggiornamenti con frequenze minori potranno essere implementati su richiesta della PA. Al fine di consentire un'efficiente configurazione dei data feed, implementando una ottimizzazione del consumo delle risorse di rete e di processamento, ogni Organizzazione Sorgente è caratterizzata da una periodicità di pubblicazione basata sulla frequenza degli eventi disponibili di una determinata tipologia di dato. Adottando un modello risk-based, i data feed sono aggiornati con frequenze dipendenti principalmente dal TLP. I data feed TLP: Amber proposti sono aggiornati e resi disponibili in **near real time**.

10.3. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT (SGS-IT)** conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management). Il **modello operativo** di erogazione del servizio prevede due possibili scenari architetturali di implementazione: ✓comunicazione tramite HTTPS API Gateway; ✓ comunicazione tramite TAXII server.

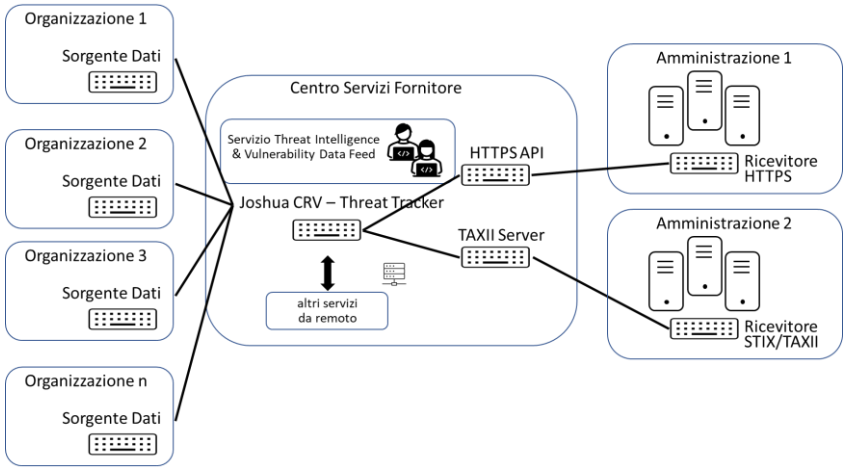

Figura 27 – Modalità di erogazione del servizio TI&VDF

In fase di definizione del Piano Operativo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono: ✓quantità di data feed sottoscritti; ✓tipologia di apparato candidato alla ricezione dei flussi dati.

L'organizzazione del servizio si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- **Catalogo:** ogni Amministrazione indicherà i singoli data feed che vorrà abilitare all'interno del flusso informativo che riceverà costantemente;
- **Modello di comunicazione:** ogni Amministrazione indicherà le modalità di ricezione del flusso informativo che riceverà costantemente. Tali modalità sono: HTTPS API Gateway o TAXII server;
- **Attack Surface Management:** ogni Amministrazione dichiarerà la superficie esposta del proprio Sistema Informativo al fine di sottoporla a monitoraggio passivo, tramite correlazione automatica degli IoC su fonti OSINT e CLOSINT, producendo anche segnali di allerta in caso di minaccia verso un proprio asset;
- **Token di accesso**: ogni Amministrazione avrà un token per accedere al flusso di dati afferenti i feed sottoscritti. Il token sarà generato dal RTI e fornito tramite comunicazione sicura (es: e-mail cifrata).

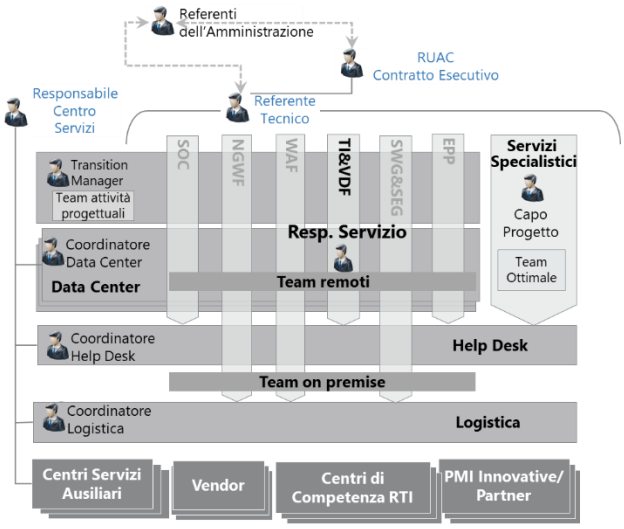

Figura 28 – Organizzazione del servizio TI&VDF

Erogazione del servizio:

- **Info Sharing**: il flusso dei dati richiesti sarà inviato dal Centro Servizi alle Amministrazioni, senza soluzione di continuità. Il flusso sarà disponibile in tempo reale ed includerà tutti i dati di una specifica sottoscrizione.
- **Modalità HTTPS API**: L'erogazione del servizio è prevista tramite API, quindi tramite rilascio da parte del Centro Servizi di un Token per autenticazioni machine to machine. Le API sono rese disponibili tramite protocollo HTTPS, implementando di default un canale di cifratura per una comunicazione sicura delle informazioni, disponibili nei principali formati (JSON, XML, CSV).
- **Modalità STIX/TAXII:** la comunicazione sarà diretta verso il TAXII server ed i dati saranno trasmessi in modo strutturato, nel formato STIX 2.0. Il modello TAXII previsto è **Source/subscriber**, pertanto il Centro Servizi si costituirà singola fonte di informazione per le Amministrazioni richiedenti.
- **Reporting**: Attraverso le API le Amministrazioni potranno generare report o raccogliere i dettagli tecnici di cui necessitano, come ad es. il numero di volte che una specifica minaccia è stata individuata nel mondo, gli URL contenenti codici dannosi e il comportamento tipico di un malware sul sistema dove è stato individuato. A tal proposito di seguito si riporta un estratto esemplificativo dei parametri delle API di ricerca: ✓returnFormat: indica il formato richiesto per i risultati della ricerca (json, xml, openioc, suricata, snort); ✓org: ricerca focalizzata per l'organizzazione che ha rilasciato uno specifico data feed; ✓from: eventi a partire da una determinata data; ✓to: eventi precedenti ad una determinata data; ✓withAttachments: consente di codificare gli allegati come nel caso di malware di esempio.

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

- **Joshua CybeRisk Vision – Threat Tracker:** Sistema centrale di raccolta dei dati, di correlazione e di condivisione. Tramite gli Indicatori di Compromissione sotto forma di eventi arricchiti di numerosi tag, determina gli attributi e li contestualizza per i Sistemi Informativi sottoposti a monitoraggio. Le sorgenti principali di tali indicatori sono le seguenti: ✓Feedback provenienti da una attività continua di ricerca approfondita da parte di analisti del settore; ✓Informazioni provenienti da fonti Aperte (OSINT) opportunamente verificate e certificate come attendibili; ✓Feedback da parte di tecnologie automatizzate dedicate alla ricerca e alla validazione di IoC; ✓Informazioni provenienti da fonti selezionate con le quali esiste una partnership; ✓Informazioni pubbliche relative a liste reputazionali di IP, Black List e output di sandbox.

Per ciascuna macrocategoria di sorgente è previsto uno step di analisi di attendibilità e verifica prima della definitiva pubblicazione dell'evento, con lo scopo di ridurre sensibilmente la possibilità di mettere in produzione dati che potrebbero generare anomalie degli allarmi di sicurezza o addirittura il blocco dei sistemi.

- **HTTPS API Gateway** – Abilita la comunicazione machine to machine per automatizzare la raccolta dei dati e le attività di reporting.
- **TAXII Server** - Abilita l'invio del flusso dati tramite il protocollo di comunicazione TAXII, le cui informazioni sono strutturate secondo il linguaggio **STIX 2.0** (e precedenti).

Interazioni

Si riportano di seguito le interazioni principali del Servizio Threat Intelligence & Vulnerability Data Feed verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: le informazioni gestite dal servizio Threat Intelligence & Vulnerability Data Feed sono inviate al servizio SOC in modalità machine to machine, per supportare il processo di prevenzione e gestione degli incidenti. Inoltre, il servizio SOC invia i data feed al servizio Threat Intelligence & Vulnerability Data Feed che, pertanto, arricchirà a sua volta il bacino informativo a disposizione delle Amministrazioni richiedenti tale servizio.
- **Interazione con il servizio Next Generation Firewall L1.S2:** (cfr. § 6.2 sezione Interazioni).
- **Interazione con il servizio Web Application Firewall L1.S3:** (cfr. § 7.3 sezione Interazioni).
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6:** (cfr. § 6.2 sezione Interazioni).
- **Interazione con il servizio Protezione degli End Point L1.S13**: il servizio di Threat Intelligence invia le segnalazioni (IoC) tramite l'utilizzo di API introducendo, di conseguenza, le protezioni per la rete dell'Amministrazione direttamente su dispositivi degli utenti.

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

Il servizio di protezione della navigazione Internet e della posta elettronica (di seguito anche SWG&SEG) proposto dal RTI, si avvale di soluzioni best in class di comprovata efficacia, basate su tecnologia **Fortinet**. Prevede un modello di erogazione composto da due sotto-servizi, uno dedicato alla protezione della navigazione Internet (SWG) ed uno dedicato alla protezione della posta elettronica (SEG).

Il servizio SWG viene erogato attraverso appliance **FortiGate** (hardware appliance o virtual appliance on premise) mentre il servizio SEG viene erogato in modalità SaaS dal Centro Servizi attraverso la soluzione **FortiMail**.

La gestione del servizio viene effettuata attraverso VPN create su connettività INTERNET o SPC e terminate, lato Centro Servizi, sui concentratori attestati sull'infrastruttura di management del servizio.

L'infrastruttura di management del servizio SWG&SEG si avvale delle componenti:

- **Management FortiManager –** Piattaforma centralizzata di gestione del servizio SWG, SEG e della Sandbox (cfr. cap. 4).
- **Logging&Reporting FortiAnalyzer** – Piattaforma centralizzata di logging e reportistica del servizio SWG&SEG (cfr. cap. 4).

L'infrastruttura di erogazione del servizio SWG&SEG si basa sui seguenti apparati:

- **SWG FortiGate** – Appliance in grado di proteggere le Amministrazioni dagli attacchi web grazie alle funzionalità di URL Filtering, alla visibilità e al controllo del traffico web crittografato tramite ispezione SSL e all'applicazione di policy granulari per le applicazioni web. Fortinet è il primo e unico fornitore di gateway di sicurezza ad avere ottenuto la certificazione VBWeb di Virus Bulletin per l'efficacia del web filtering.
  Il Secure Web Gateway mette a disposizione le necessarie funzionalità per proteggere la navigazione web. In particolare, è possibile configurare il servizio nelle modalità Transparent Proxy e di Explicit HTTP/HTTPS Proxy, SOCKS proxy. Tali apparati supportano molteplici modalità di autenticazione (Kerberos, NTLM, LDAP, captive portal, etc.) e protezione/filtering sia in ambito Web sia in ambito applicativo. L'Authentication Rule permette di applicare policy personalizzate per utenti/gruppi. È anche possibile definire se l'autenticazione deve essere fatta su base IP o su base sessione. Le proxy policy consentono di definire un controllo molto granulare delle applicazioni web utilizzando l'ispezione di particolari campi del pacchetto HTTP. Sulla proxy policy è quindi possibile applicare, oltre il web filtering che è il servizio principale, ulteriori controlli di sicurezza come **Application Control**, **Antivirus, IPS, DLP, File Filter, Video Filter, ICAP** per l'interfacciamento con ispezioni di terze parti, **SSL inspection** per estendere l'analisi al traffico cifrato come HTTPS.
- **FortiSandbox** – Il componente FortiSandbox supporta il servizio SWG&SEG per la detection di **malware Zero-Day** e/o **ransomware** e costituisce parte integrante dell'architettura Fortinet Security Fabric e utilizza tre modalità di intelligence sulle minacce per il rilevamento e la prevenzione degli Incidenti di sicurezza (cfr. cap. 6).
- **SEG FortiMail** – Il FortiMail è un potente secure email gateway in grado di proteggere la posta elettronica da una vasta tipologia di attacchi specifici tra cui **phishing**, **speal phishing**, **Business Email Compromise** (BEC), prevenendo la perdita di dati sensibili e coadiuvando il raggiungimento ed il mantenimento della conformità alle diverse compliance normative. Permette di scansionare il body delle mail per rilevare, riscrivere o bloccare eventuali URL che fanno riferimento a campagne di phishing e vengono rilevati attraverso la categorizzazione dei FortiGuard Labs o attraverso l'analisi avanzata in sandboxing. È possibile applicare un intero servizio di URL filter in modo da poter verificare anche ulteriori categorie a rischio Security.
  FortiMail combina funzionalità **antispam multilivello**, un potente motore **antimalware** e diverse funzionalità aggiuntive quali **Data Leak Prevention** (DLP), **Identity Based Encryption** (IBE), archivio mail e **anti-blocklisting** all'interno di un'unica soluzione integrata. La soluzione FortiMail è stata spesso oggetto del **premio VBSpam**, a testimonianza di un'altissima percentuale di rilevamento a fronte di un bassissimo numero di falsi positivi.

11.1. ORGANIZZAZIONE DEI SERVIZI, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI

Il servizio SWG&SEG proposto dal RTI viene erogato dal Centro Servizi del RTI. Il Servizio, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**) conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici

e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT** (**SGS-IT**) conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management).

Organizzazione del servizio

L'organizzazione del servizio SWG&SEG si sviluppa nelle fasi di seguito riportate.

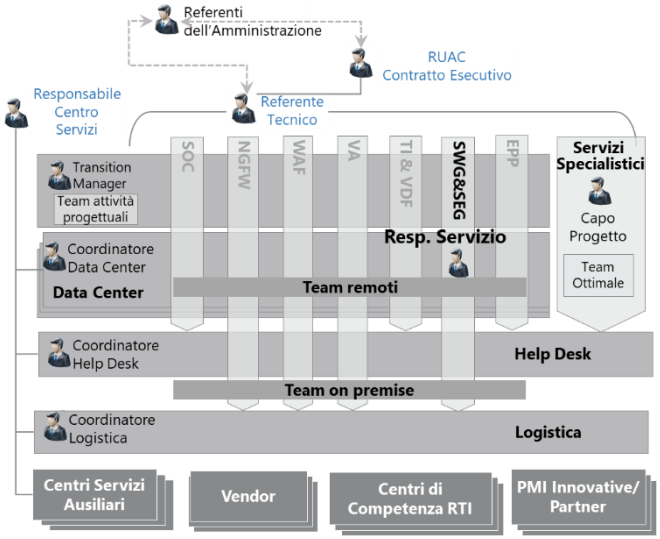

Figura 29 – Organizzazione del servizio SEG&SWG

Presa in carico del servizio:

- *acquisizione*, attraverso il *Team on-premise* (cfr. § 4), di know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione, delle relative modalità operative, delle linee guida e metodologie in uso presso l'Amministrazione;
- predisposizione e configurazione del servizio e delle relative piattaforme di management:
  - Il *SWG&SEG Team* attiva il servizio dedicato all'Amministrazione su ciascuna delle piattaforme di gestione del servizio descritte precedentemente. Attiva inoltre il servizio SEG (erogato dal Centro Servizi) secondo quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano;
  - Il *Team on-premise* gestisce l'installazione delle componenti previste on-site secondo il piano di installazione condiviso con l'Amministrazione. Gli apparati SWG saranno resi raggiungibili, presi in carico dal sistema di management e configurati da remoto. Il servizio sarà predisposto sulla base di quanto definito nel Piano Operativo in base a tutti i parametri che lo caratterizzano;
  - se necessario, il *Team on-premise* ed il SWG&SEG *Team* gestiscono il processo di migrazione secondo quanto stabilito nel piano di migrazione.

Erogazione del servizio:

- *Monitoraggio della disponibilità*: gli operatori dell'Help Desk di 2° livello monitorano il servizio attraverso la console gestiscono gli allarmi o in autonomia o coinvolgendo il supporto di 3° livello;
- *Richieste di modifica delle configurazioni*: L'Amministrazione potrà aggiornare le politiche di sicurezza utilizzando il portale dei servizi di sicurezza in modalità self-ticketing (in caso di contestuale acquisizione del servizio SOC) o mediante l'apertura di un ticket. La richiesta sarà preso in carico dal team specialistico SWG&SEG che, una volta effettuate le necessarie attività, provvederà al collaudo della modifica congiuntamente con il personale preposto dall'Amministrazione;
- *Reporting*: La reportistica permette di verificare la conformità agli standard scelti e il livello di protezione delle applicazioni. Prevede report personalizzabili di sintesi (executive summary) e di dettaglio (technical report), al fine di certificare la compliance a determinati standard o per consentire analisi sul livello di protezione delle applicazioni.
- *supporto alla gestione incidenti*: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

Modalità di erogazione

La soluzione verso un modello di erogazione composto da due sotto-servizi, uno dedicato alla protezione della navigazione Internet (SWG) ed uno dedicato alla protezione della posta elettronica (SEG).

La modalità di erogazione del servizio prevede due diversi scenari per entrambi i sotto-servizi in ambito: ✓installazione di appliance dedicati fisici o virtuali on premise presso la sede dell'Amministrazione o presso il proprio Virtual Private Cloud; ✓utilizzo di istanze del sotto-servizio installato presso il Centro Servizi del RTI ed acceduta in modalità SaaS. L'architettura di default proposta dal RTI è quella on premise per il sotto-servizio SWG e SaaS presso il Centro Servizi del RTI per il sotto-servizio SEG.

In fase di definizione del progetto esecutivo con la specifica Amministrazione contraente verrà definito e concordato quale sia lo **scenario più idoneo per la specifica Amministrazione** in questione. I criteri di valutazione per la scelta dello scenario sono: ✓numerosità di utenti; ✓dislocazione del mail server; ✓stima traffico generato.

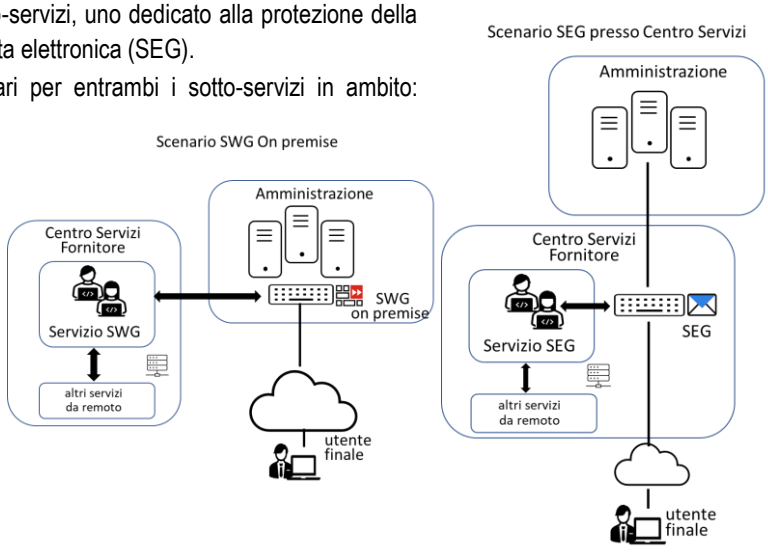

Figura 30 – Modalità di erogazione SEG&SWG

Interazioni

Si riportano di seguito le interazioni principali del Servizio Protezione Navigazione Internet e Posta Elettronica verso gli altri servizi: ✓**Interazione con il servizio Security Operation Center L1.S1**: (cfr. § 6.2 sezione interazioni); ✓**Interazione con il servizio Next Generation Firewall**

L1.S2: (cfr. § 6.2 sezione interazioni); ✓**Interazione con il servizio Web Application Firewall L1.S3**: (cfr. § 7.3 sezione interazioni); ✓**Interazione con il servizio Threat Intelligence & Vulnerability Data Feed L1.S5:** (cfr. § 6.2 sezione interazioni); ✓**Interazione con il servizio Protezione degli End Point L1.S13**: (cfr. § 6.2 sezione interazioni).

11.2. CAPACITÀ DEL SERVIZIO DI PROTEZIONE INTERNET DI "DEEP INSPECTION"

Il servizio di Protezione Navigazione Internet include funzionalità avanzate di Stateful Filtering e "Deep Inspection", che permettono di applicare feature di AV, Application Control e Web Filtering anche su comunicazioni protette da protocolli cifrati. Infatti, l'encryption SSL/TLS, utilizzata dal protocollo HTTPS per proteggere la sessione del client verso una web application, viene spesso sfruttata in maniera malevola per nascondere il payload (spesso malware, anche di tipo ransomware) all'interno del tunnel cifrato, bypassando il controllo del SWG. La funzionalità di SSL Deep Inspection consente di effettuare il parsing dei pacchetti transitanti in chiaro (ovvero decodificati) e quindi la possibilità di esaminare l'eventuale traffico malevolo o comportamenti malevoli pur conservando intatta la sicurezza della sessione di comunicazione.

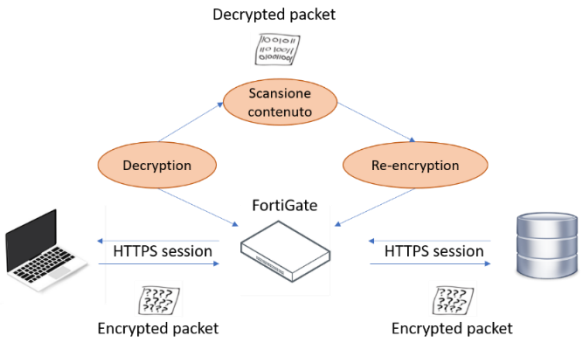

Figura 31 – Deep Inspection

Come si evince, il SWG Fortigate si pone in modalità proxy per poter effettuare la scansione avanzata, di tipo Store&Forward che, per una maggiore efficacia nella rilevazione dei malware, attende che il download del file sia completo prima di analizzarlo con gli engine di sicurezza. Tale operazione viene eseguita in real time direttamente in hardware, utilizzando dei processori ASIC ottimizzati, in modalità del tutto trasparente sia per il client che per il server (infatti, il SESSION ID, la tipologia di encryption etc., rimangono inalterati).

Gli engine di sicurezza utilizzano sia tecniche di scansioni malware "**Signature Based**", sia tecniche di **Sandboxing "Behaviour Based"**. Le tecniche di scansione "Signature Based" utilizzano la Suite di sicurezza AMP (Advance Malware Protection), specifica per la rilevazione Antimalware, che comprende le seguenti funzionalità:

- **Antivirus/AntiBotnet**: la funzionalità di Antivirus/Antimalware permette l'ispezione del traffico su base Signature e su base euristica, permettendo l'identificazione delle minacce più avanzate e l'identificazione di botnet e server Command&Control tipici di architetture di Distributed Denial-of-Service Attacks. Molto spesso i motori Antivirus basati su signatures, pur se queste sono costantemente aggiornate, sono poco efficaci quando i file malevoli vengono intenzionalmente modificati (per evitare di creare un malware ex-novo) con il solo scopo di alterarne la signature (questa pratica viene identificata come polimorfismo) allo scopo di eludere il controllo: la soluzione proposta dal RTI, basata sulla tecnologia Fortinet, utilizza il brevetto Compact Pattern Recognition Language che permette di rilevare un perimetro di polimorfismi da una signature base, rendendo più efficace l'utilizzo delle firme antimalware;
- **Mobile Security**: La funzionalità permette di protegge efficacemente i propri client dalle ultime minacce destinate a colpire in maniera specifica i device mobili, sempre più diffusi in contesti aziendali in linea con il fenomeno BYOD;
- **Virus Outbreak Protection**: questo servizio offre uno strato aggiuntivo di protezione mirato ai nuovi Malware appena nati e a fermare i rapidi attacchi virali, perché di solito occorrono almeno alcune ore per sviluppare e installare le firme; per questo scopo viene utilizzato in tempo reale il DB di checksum delle minacce appena rilevate prima che siano disponibili le firme AV;
- **Content Disarm and Reconstruction**: con questo servizio, il motore AV può rimuovere tutto il contenuto attivo in tempo reale rilasciando all'utente il file "disarmato", come ad esempio macro all'interno di file word oppure collegamenti ipertestuali all'interno di file pdf (le Macro contenute all'interno dei file Word, Excel, PowerPoint etc. rappresentano uno dei 5 modelli di trasmissione dei Virus più utilizzati).

Le tecniche di scansione di tipo "**Behaviour-based**" vengono invece effettuate attraverso la Appliance Sandbox. La Sandbox permette di massimizzare la protezione dalle minacce zero-day, APT, Ransomware (ad esempio Cryptolocker, WannaCry, CryptoWall, etc.). A differenza di altre soluzioni presenti sul mercato, la FortiSandbox è una soluzione basata su MITRE ATT&CK che sfrutta l'Intelligenza Artificiale (AI) e l'apprendimento automatico (Machine Learning - ML) per analisi statiche e dinamiche dei malware. FortiSandbox applica l'AI durante l'intero processo di sandboxing, miscelando analisi sia statica che dinamica per apprendere in modo adattivo i nuovi comportamenti del malware e migliorare l'efficacia del rilevamento delle minacce zero-day. La FortiSandbox permette la detonazione anche dei malware di ultima generazione che sono in grado di disattivarsi quando vengono eseguiti in un contesto virtuale e quindi eventualmente in un LAB specifico per l'analisi (ispezione dell'OUI dei Mac Address delle vNIC delle VM, verifica sui movimenti del mouse che se assenti denotano sicuramente una macchina di laboratorio senza presenza umana, verifica della presenza o meno di un'interfaccia di rete attiva). In funzione dello specifico profilo di sicurezza selezionato, il processo di scansione approfondita del codice terminerà validandone la non pericolosità oppure spostando il malware in quarantena, dandone opportuna comunicazione all'utente. Coerentemente con l'approccio Security Fabric la Sandbox mette a disposizione dei dispositivi connessi l'elenco dei file e delle URL malevole.

11.3. CAPACITÀ DEL SERVIZIO DI PROTEZIONE INTERNET DI DISCOVERY DI ACCESSI AD APPLICAZIONI IN CLOUD (SAAS)

In generale, un SWG operante in modalità 'stateful' lavora con policy/rules costruite sui primi 4 livelli del modello ISO/OSI. Ciò implica che la caratterizzazione del traffico da autorizzare o bloccare è legata principalmente al socket di sessione (IP sorgente, IP di destinazione, porta sorgente e porta di destinazione). Tuttavia, ad applicazioni fruite in Cloud in modalità SaaS (es. Microsoft Office 365), possono corrispondere un insieme piuttosto ampio di indirizzi IP, porte e protocolli da abilitare o bloccare per mezzo di un firewall perimetrale. In tale contesto, la difficoltà di gestione è legata non solo alla quantità dei parametri di rete considerati, che possono assumere simultaneamente decine o centinaia di valori differenti, ma anche alla loro variabilità: si pensi agli indirizzi IP che possono cambiare in base allo spostamento geografico degli ambienti Cloud del Vendor SaaS, all'acquisto o cessione di porzioni di subnet pubbliche, all'utilizzo di tecniche di NAT, etc.). Tale problematica, se non opportunamente indirizzata, potrebbe condurre ad un filtraggio del traffico solamente parziale, lasciando accessibili servizi SaaS che potrebbero rappresentare una possibile breccia di sicurezza, ampliando in conseguenza la possibile superficie di attacco. La soluzione proposta dal RTI supera tale problematica mediante l'impiego di un **Internet Service Database** costantemente aggiornato in maniera automatica e capace di gestire 1.500 applicazioni Cloud SaaS in termini di indirizzi IP, porte e protocolli utilizzati.

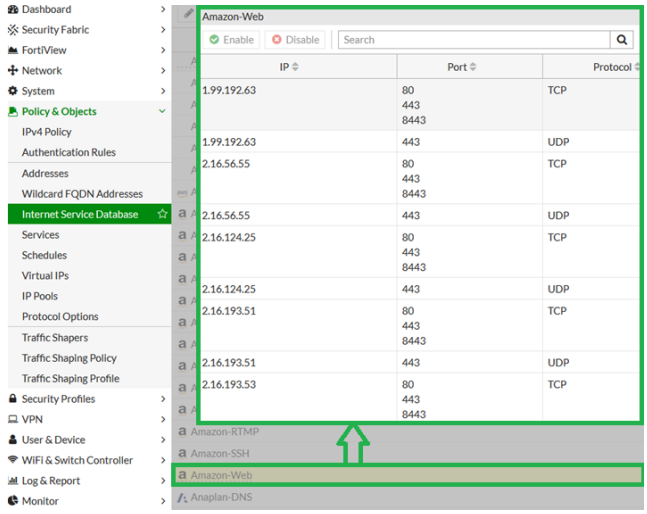

Figura 32 – ISDB

Attraverso l'utilizzo di questo Database è possibile effettuare la Discovery di accessi ad applicazioni in Cloud ed applicare un meccanismo di white/black-listing per consentire/impedire l'accesso ai soli servizi in Cloud censiti. Qualora un'applicazione in Cloud sia ritenuta non conforme alle policy aziendali è possibile negarne agli utenti l'accesso attraverso la definizione di una specifica Proxy Policy che ha, come campo destinazione, il servizio SaaS censito nell'Internet Service Database (ISDB).

È possibile, inoltre, consentire l'accesso all'applicazione SaaS prevedendo tuttavia controlli granulari delle Feature applicative utilizzabili dagli utenti. Le funzionalità avanzate di Application Control e Web Filtering, consentite dall'impiego dell'Internet Service Database, permettono di ottenere efficacemente delle Proxy Policy molto granulari, consentendo inoltre una caratterizzazione dei servizi e delle applicazioni sempre aggiornata. Tali policy possono essere applicate a degli host identificati mediante indirizzo IP oppure direttamente ad un'utenza di rete specifica (Layer 8 – Livello USER).

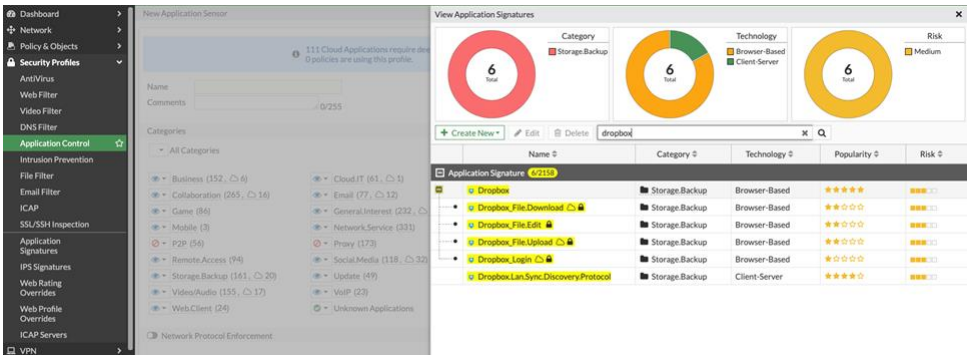

Figura 33 – Interfaccia SWG

Nella Proxy Policy relativa all'applicativo SaaS, è possibile applicare uno specifico profilo di "Application Control", per raffinare ulteriormente il filtering. Ad esempio, qualora un'Amministrazione abbia intenzione di filtrare l'accesso ad un servizio di file sharing SaaS, è possibile definire nel profilo di Application Control della relativa Proxy Policy, dei permessi specifici inerenti la gestione dei file per consentire o negare esplicitamente il download, l'editing o l'upload dei file.

Come menzionato precedentemente, Internet Service DB viene aggiornato automaticamente per cui si avrà, al momento della stesura di una Proxy Policy, la possibilità di utilizzare direttamente l'Internet Service già censito, oppure realizzare dei Custom Service andando a specificare i seguenti campi: ✓IP o IP Range; ✓Protocol Number; ✓Porta o Range di porte; ✓Reputation.

Infine, è possibile anche realizzare una Extension Internet Service che dia la possibilità di aggiungere o rimuovere IP address da un Predefined Internet Service, aggiungere o rimuovere porte etc.

12. PROPOSTA PROGETTUALE PER IL SERVIZIO "PROTEZIONE NAVIGAZIONE INTERNET E POSTA ELETTRONICA" - FUNZIONALITA' AGGIUNTIVE

Si conferma la presenza di "funzioni di protezione della posta anti-phishing e anti-ransomware" con riferimento al servizio di "protezione navigazione internet e posta elettronica" (cfr. cap.6, 11 e §11.2).

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

Il servizio di Protezione degli Endpoint ha la finalità di proteggere gli strumenti di lavoro del personale delle Pubbliche Amministrazioni da possibili attacchi informatici che possano sfruttare l'endpoint quale vettore preferenziale verso il Sistema Informativo della PA. Il RTI ha maturato una consolidata esperienza nell'erogazione di servizi di protezione degli endpoint sia nel comparto della Pubblica Amministrazione che nel mondo privato ed una profonda conoscenza ed esperienza sulla tecnologia Trend Micro proposta per questa fornitura, comprovata da numerose **certificazioni delle risorse** ed una **partnership di tipo GOLD.** La soluzione proposta dal RTI oltre a rispettare pienamente i requisiti del Capitolato, presenta una serie di caratteristiche tecnologiche e prestazionali migliorative come meglio descritto nel seguito. Specificatamente, per l'erogazione del servizio di protezione degli endpoint, il RTI adotta la tecnologia Trend Micro Apex One, una soluzione ideata per la protezione degli endpoint da molteplici virus quali ransomware, trojan e altri malware specifici, che consente anche di controllarne ed impedirne la diffusione all'interno della rete. Inoltre, la soluzione tecnologica Apex One di Trend Micro è leader

all'interno del Magic Quadrant di Gartner per le piattaforme di protezione degli endpoint nel 2021. Si evidenzia che come richiesto dal capitolato il servizio è erogato totalmente dal Centro Servizi del RTI senza la necessità di utilizzare componenti nel cloud del vendor.

Trend Micro, grazie alla "Zero Day Initiative", è il primo Vendor in assoluto in termini di ricerca di nuove vulnerabilità con migliaia di scoperte ogni anno. La tecnologia proposta beneficia di queste informazioni con significativo anticipo rispetto alla concorrenza e, grazie al Virtual Patching, è in grado di proteggere i dispositivi fin dal primo istante dalla scoperta senza dover attendere una patch ufficiale da parte del produttore.

A questo riguardo il servizio è progettato per operare con la massima efficacia sia come singolo servizio sia, come meglio specificato nel seguito del presente capitolo, mediante l'**interazione in forte sinergia con gli altri servizi** della fornitura.

Figura 34 – EPP Gartner Magic Quadrant

13.1. FUNZIONALITÀ AGGIUNTIVE E CARATTERISTICHE TECNOLOGICHE MIGLIORATIVE

Il servizio proposto dal RTI prevede l'utilizzo della piattaforma basata sulla tecnologia Trend Micro Apex One installata presso il Centro Servizi.

I componenti principali della soluzione sono:

- **Apex Central:** fornisce attraverso una console centralizza la visibilità ed il controllo per gestire, monitorare e creare policy di sicurezza. Attraverso l'uso di dashboard personalizzabili è inoltre possibile visualizzare e valutare in tempo reale lo stato di sicurezza degli endpoint dell'Amministrazione, rilevare eventuali utenti a rischio, identificare le minacce e rispondere agli incidenti. La visibilità può essere effettuare su base utente (eventualmente anche mediante integrazione con Active Directory) e consente di monitorare cosa accade sui dispositivi, permettendo così di accedere alle policy in maniera granulare e apportarvi modifiche.
- **Apex One Server**: la componente specifica destinata alla singola Amministrazione contraente che controlla operativamente i singoli agent installati sui rispettivi endpoint.
- **Security Agent:** agent installati su ciascun endpoint che permettono di eseguire le operazioni di controllo e verifica degli oggetti malevoli nonché di applicare localmente tutte le policy di sicurezza previste.
- **Deep Discovery Analyzer**: fornisce le funzionalità di sandbox per la *detonazione* degli oggetti potenzialmente malevoli.

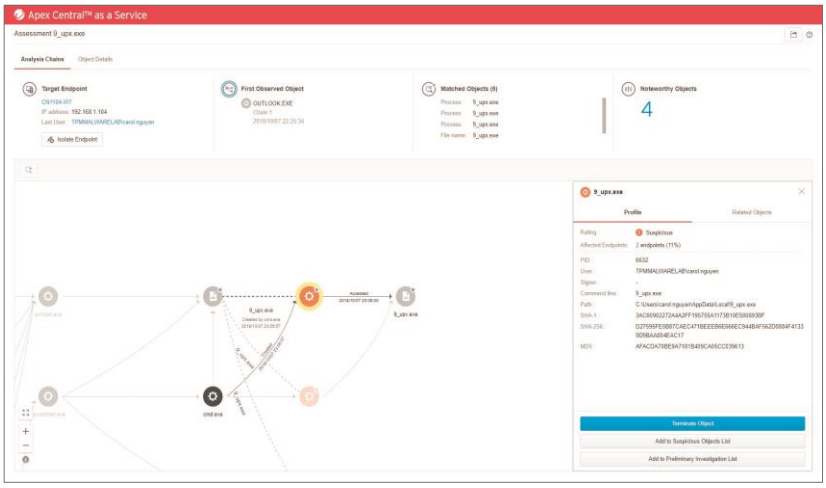

Figura 35 – Console di gestione Apex Central

La soluzione proposta dal RTI introduce alcuni elementi migliorativi rispetto ai requisiti minimi del Capitolato Tecnico che consentono di innalzare ulteriormente la postura di sicurezza degli endpoint dell'Amministrazione contraente.

Tutti gli endpoint vengono dotati di un agent in grado di erogare tutte le funzionalità messe a disposizione dalla tecnologia sinteticamente riportate nella figura seguente.

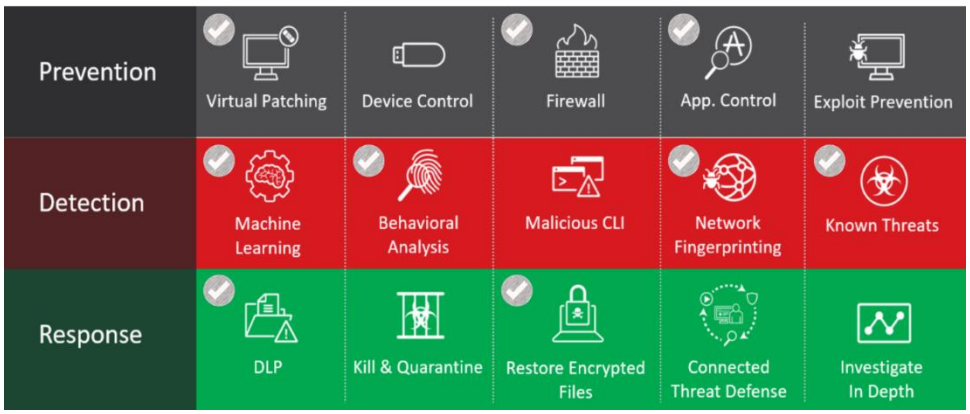

Figura 36 – Matrice delle funzionalità di Apex One

Le funzionalità che si caratterizzano come migliorative rispetto ai requisiti minimi sono evidenziate con una spunta nella figura e descritte di seguito:

- **Virtual Patching e Firewall**: La soluzione offre una protezione avanzata e preventiva degli endpoint mediante l'integrazione di patch virtuali a fronte di vulnerabilità note e sconosciute. Un motore dedicato monitora costantemente il traffico alla ricerca di eventuali attacchi zero-day e nuove vulnerabilità specifiche utilizzando i filtri del sistema di prevenzione dalle intrusioni (IPS) basato su host. In questo modo è possibile rilevare deviazioni del protocollo di rete o contenuti sospetti

che segnalano un attacco o violazioni dei criteri di sicurezza. Se vengono rilevate minacce, la soluzione impedisce che queste vulnerabilità vengano sfruttate grazie all'utilizzo di filtri prontamente distribuiti sugli agent che offrono una protezione completa prima che le patch possano essere distribuite o siano disponibili. Apex One detiene centinaia di regole IPS, regolarmente aggiornate tramite l'analisi dei laboratori di ricerca e della Zero Day Initiative (ZDI), grazie alle quali è in grado di fornire le soluzioni più idonee all'endpoint.

- **Application Control:** al fine di evitare che i singoli endpoint possano essere utilizzati quali trampolino di lancio per l'esecuzione di software malevolo, è inibita l'esecuzione di applicazioni indesiderate, sconosciute e potenzialmente dannose. Il controllo dell'esecuzione delle applicazioni viene realizzato attraverso la combinazione di vari criteri dinamici, di funzionalità di "whitelisting/blacklisting" e di un vasto catalogo di applicazioni.
  Tutti questi elementi vengono configurati e combinati direttamente dalla console centralizzata consentendo una gestione granulare per ogni singola Amministrazione contraente, oltre che per unità organizzativa o per singolo utente.
- **Machine Learning e Behavior Analysis**: Alle tradizionali tecniche anti-malware è affiancato un motore di nuova generazione che include analisi comportamentale e meccanismi di machine-learning predittivi. L'approccio basato sul Machine learning, applicato prima e durante l'esecuzione dei file, unito a tecniche di *cancellazione del rumore*, ha l'obbiettivo di ridurre drasticamente i falsi positivi. L'analisi comportamentale risulta efficace contro tecniche di injection, ransomware e attacchi alla memoria o al browser.
- **Network Fingerprinting**: La funzionalità permette di monitorare il traffico di rete sull'endpoint alla ricerca di pattern noti al fine di identificare possibili comunicazioni originate da oggetti malevoli.
- **Known Threats**: La soluzione beneficia dell'accesso alla vasta fonte di intelligence fornita dalla Smart Protection Network di Trend Micro, alimentata da più di 3500 ricercatori nel mondo con centinaia di terabyte analizzati giornalmente. Ciò consente di mantenere una protezione metodicamente aggiornata con migliaia di informazioni su zero-days e minacce. Tutte le informazioni raccolte ed elaborate dagli analisti vengono rese disponibili ad Apex One sottoforma di oggetti come URL, IP, Domini, File, Network Pattern, Firme e altri. La fase di analisi e risposta a fronte di eventuali minacce è supportata dalle informazioni fornite dalla Smart Protection Network, che facilitano la comprensione della natura di un oggetto analizzato. Inoltre, sulla base di un comportamento noto all'intelligence, è possibile ottenere un riscontro automatico sulle tecniche di attacco utilizzate (MITRE ATT&CK), e sul dataset di informazioni presenti nel database globale delle minacce.
- **Data Loss Prevention (DLP)**: La protezione DLP, integrata nell'agent endpoint, consente di avere visibilità e controllo dei dati sia "at rest" che "in transit" oltre che prevenirne la perdita.
  Mediante la console di gestione è possibile sia determinare la natura di un dato da proteggere indicandolo in termini di parole chiave, attributi di file o di regular expression, sia creare un template composto da più "Data Identifiers" garantendo granularità nell'identificazione dell'informazione da monitorare.
  Grazie ad un approccio basato su policy è possibile assegnare ad ogni utente o gruppo di utenti un set di regole DLP composte da: ✓*Template*: modello di regola preconfezionato o personalizzato che determina la natura del dato da monitorare e/o proteggere ✓*Canale*: la selezione degli ambiti di applicazione della policy con la possibilità di scegliere il flusso del dato da monitorare su canali specifici (Email, Web, FTP, SMB, Peer To Peer, USB, Clipboard, Stampanti, etc.) ✓*Azione*: scelta dell'azione da intraprendere quando un dato trova riscontro nella policy. Azioni possibili sono il logging, il blocco della trasmissione, il consenso alla trasmissione dietro giustificazione e la registrazione del dato. Inoltre è possibile gestire le notifiche agli utenti tramite pop-up del software agent.
- **Restore Encrypted Files**: il comportamento dei ransomware segue un modello noto finalizzato a cifrare, rendendo inaccessibili, i file sugli endpoint. Il motore di analisi comportamentale effettua il backup predittivo dei file potenzialmente oggetto di attacco, la funzionalità di Restore Encrypted Files permette di ripristinare i file cifrati da un malware subito dopo la sua identificazione, recuperandone i contenuti dal backup.

13.2. PROTEZIONE DALLE MINACCE WEB AVANZATE "ZERO-DAY" TRAMITE ISOLAMENTO REMOTO DEL BROWSER

La piattaforma presente nel Centro Servizi per la protezione degli endpoint è dotata di componenti tecnologiche dedicate con capacità avanzata per proteggere i dati dell'Amministrazione contraente dalle minacce veicolate attraverso la navigazione sul Web. Il sistema ha la capacità di monitorare l'uso degli endpoint alla ricerca di oggetti malevoli al fine di prevenirne l'azione e la diffusione. L'identificazione di **oggetti sospetti, comprensivi delle URL di navigazione del browser,** ne consente l'invio all'ambiente isolato, sandbox, per un'analisi avanzata utilizzando diversi metodi di rilevamento. Nel momento in cui viene rilevata dalla analisi della sandbox una minaccia, gli agent installati sugli endpoint recepiscono automaticamente l'IOC e/o la signature per intraprendere le azioni di rilevamento, blocco, quarantena o eliminazione dell'oggetto. La sandbox consente agli amministratori di accedere ad una reportistica dettagliata con la descrizione delle diverse fasi dell'attacco rilevato, riportando ogni singola azione effettuata dall'oggetto malevolo di tipo zero-day quali, per esempio, comandi powershell eseguiti, file o chiavi di registro modificate, chiamate URL verso l'esterno.
Le ulteriori funzionalità a supporto della detection delle minacce web avanzate "zero-day" sono le seguenti:

1. **Analisi avanzata:** La sandbox utilizza immagini virtuali personalizzabili, coincidenti con i sistemi operativi da analizzare, che contengono configurazioni, driver, applicazioni, versioni e linguaggi. Questo approccio aumenta drasticamente la capacità di rilevazione di minacce avanzate, comprese quelle che tentino l'evasione dagli ambienti sandbox più comuni.
   La stessa ha accesso internet esterno sicuro tale da permetter l'identificazione di minacce multi-stage, download, URL, Command and Control (C&C) e altro. Inoltre, la soluzione permette il caricamento manuale di artefatti da parte degli amministratori.

2. **Rilevazione malware:** Viene eseguita con tecniche di analisi statica, euristica, comportamentale, web e file reputation consentendo la rilevazione su numerosi tipi di file quali, a titolo di esempio non esaustivo: documenti, file compressi, oggetti dinamici, contenuti web, script e URL. La soluzione è in grado di *detonare* oggetti anche su ambienti **Android** (mobile, IoT, Automotive).
3. **Rilevazione ransomware:** La capacità di rilevazione e blocco, consente di identificare e stoppare attività legate ad attacchi Ransomware. Sfruttando un mix di tecniche composte da analisi statica, dinamica ed euristica (behaviour analysis, pattern analysis, verifiche reputazionali e sandbox per oggetti sospetti), il motore di analisi comportamentale analizza le attività eseguite dal sistema e ne valuta le reali intenzioni per ricercare minacce potenzialmente insediate negli asset.

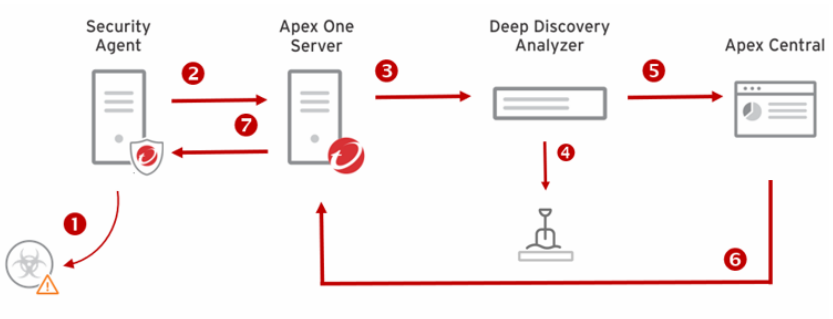

Figura 37 – Workflow del contrasto alle minacce tramite sandbox

La figura illustra le fasi di contrasto alle minacce attraverso l'uso della sandbox.
L'agent rileva una potenziale minaccia (**1**) e la invia all'Apex One Server (**2**). Il potenziale malware o url viene quindi inviato al modulo di esecuzione nella Sandbox Deep Discovery Analyzer (**3**), dove, all'interno della sandbox, viene fatto *detonare* e viene analizzato il suo comportamento (**4**). L'esito dell'analisi viene notificato sulla console (**5**) che istruisce l'Apex One Server sulle modalità di protezione da attuare (**6**). In ultimo l'Apex One Server istruisce gli agent installati sugli endpoint sulle operazioni da eseguire (**7**).
Nella figura a fianco è rappresentato un dettaglio dell'esecuzione nella sandbox di una url eseguita in automatico tramite le fasi del processo sopra descritte.

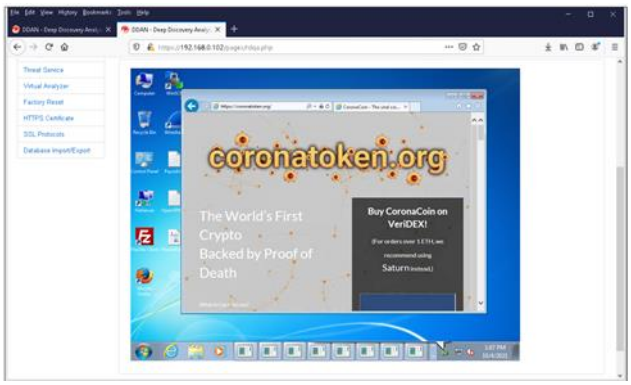

Figura 38 – Esempio di esecuzione nella sandbox

13.3. ORGANIZZAZIONE DEL SERVIZIO, MODALITÀ DI EROGAZIONE E DI INTERAZIONE CON GLI ALTRI SERVIZI.

Il Servizio di protezione degli endpoint, progettato sulla base dei requisiti definiti dal Capitolato Tecnico e in accordo ai miglioramenti proposti in Offerta Tecnica, viene gestito in conformità agli standard di riferimento **ISO/IEC 27001** e **ISO/IEC 20000-1**. In particolare, la confidenzialità e l'integrità delle informazioni impiegate o prodotte in sede di erogazione del Servizio sono garantite dall'adozione di un **Sistema di Gestione della Sicurezza delle Informazioni** (**SGSI**) conforme allo standard ISO/IEC 27001 e dall'applicazione puntuale dei necessari controlli tecnici e amministrativi; la capacità, la continuità e le performance del Servizio sono invece garantite dall'adozione di un **Sistema di Gestione dei Servizi IT** (**SGS-IT**) conforme allo standard ISO/IEC 20000-1 e dalla implementazione consistente di tutti i necessari processi di gestione del Servizio (IT Service Management). L'organizzazione del servizio EPP si sviluppa nelle fasi di seguito riportate.

Presa in carico del servizio:

- **Assessment degli endpoint**: si procede con il censimento di tutti i dispositivi fissi (postazioni di lavoro) e mobile (Laptop, Smartphone, etc…) in uso presso l'Amministrazione nel perimetro del servizio. Per ciascuno dei dispositivi individuati viene verificata la compatibilità con la soluzione tecnologica in uso. Inoltre, in questa fase, viene identificato in dettaglio lo stato dei sistemi logici, fisici e virtuali, acquisendo tutte le informazioni relative anche agli apparati di sicurezza presenti.
- **Pianificazione delle installazioni:** A valle dell'assessment e delle verifiche di compatibilità si procede con la pianificazione dell'installazione degli agent di Endpoint protection su ciascun dispositivo rilevato secondo le priorità identificate in accordo con l'Amministrazione.

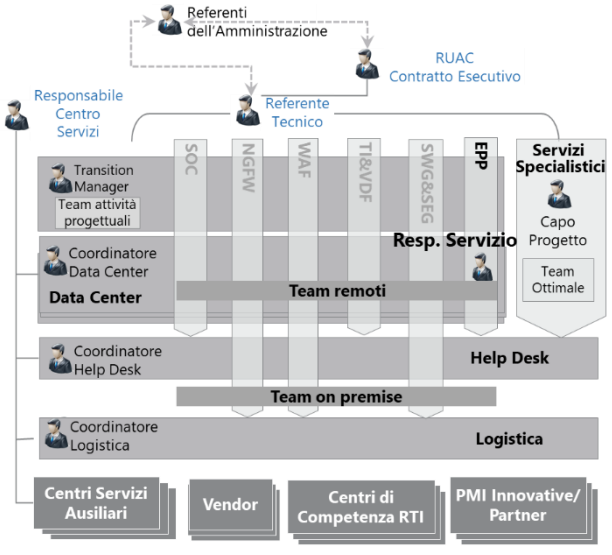

Figura 39 – Organizzazione del servizio EPP

Erogazione del servizio:

- **Implementazione delle policy di sicurezza:** la soluzione tecnologica implementerà le policy di sicurezza dell'Amministrazione in conformità a quanto disposto per i dispositivi connessi alla rete, come ad es. utilizzo di un sistema operativo approvato, installazione di una VPN o l'esecuzione di un software antivirus aggiornato.
- **Installazione degli agent:** La procedura di installazione viene concordata congiuntamente con l'Amministrazione. La procedura di installazione può prevedere anche la rimozione di un antivirus eventualmente già presente sulle postazioni, al fine di evitare finestre temporali in cui i dispositivi non siano coperti dalla protezione o conflitti tra i due strumenti di protezione. Ove si renda necessario, ad esempio per il numero elevato di endpoint, è possibile creare, in accordo con l'Amministrazione, un ambiente di staging per eseguire la fase pilota del servizio e dove replicare configurazione particolari che richiedano un tuning della configurazione.
- **Attivazione del Servizio:** Attivazione del servizio per tutti gli endpoint censiti in accordo con il piano di rollout condiviso con l'Amministrazione.
- **Conduzione operativa**: la conduzione della soluzione tecnologica riguarda tutte le fasi del ciclo di vita del servizio e si sostanzia nelle seguenti attività: ✓Gestione centralizzata; ✓Conduzione applicativa; ✓Manutenzione ordinaria della piattaforma; ✓Attivazione dei nuovi sistemi con le corrette policy

di pertinenza; ✓eventuale deprovisioning dell'agent; ✓Tuning delle configurazioni; ✓Monitoraggio e gestione di eventuali malfunzionamenti degli agent.

- **Produzione della Reportistica**: Vengono prodotti periodicamente dei report per l'Amministrazione finalizzati all'individuazione della diffusione di malware o di eventi sospetti che richiedono un approfondimento. I report vengono realizzati sulla base di una serie di template standard definiti in fase di progetto esecutivo.
- **Supporto alla gestione incidenti**: ✓controllo di alert e report finalizzati all'individuazione di tentativi di attacco, di eventi sospetti che richiedono un approfondimento, di possibili falsi positivi (tale attività può innescare reazioni quali l'apertura di un incidente di sicurezza oppure verifiche con il responsabile/cliente); ✓supporto alla analisi dei log "post mortem" per la determinazione della causa di un incidente e la individuazione dei rimedi applicativi/infrastrutturali/di sicurezza.

La piattaforma eroga i propri servizi verso la rete dell'Amministrazione ma rende possibile l'ulteriore erogazione anche attraverso internet per garantire la copertura dei device anche quando non sono fisicamente collegati dall'interno delle infrastrutture dell'Amministrazione. La comunicazione via internet è corredata da funzionalità di firma e cifratura dei dati scambiati che ne garantiscono la sicurezza.

Per ciascuna Amministrazione contraente viene configurato un Apex One Server dedicato presso l'Amministrazione. In sede di progettazione della soluzione, per ogni singola Amministrazione, è possibile prevedere ulteriori livelli di segregazione tali da garantire la presenza di apparati di frontiera che separino le reti delle amministrazioni rispetto al Centro Servizi. Tutti i sistemi e le applicazioni coinvolte subiscono un regolare processo di aggiornamento periodico sulla base delle distribuzioni delle patch rese disponibili dai vendor.

La figura illustra l'architettura di alto livello proposta.

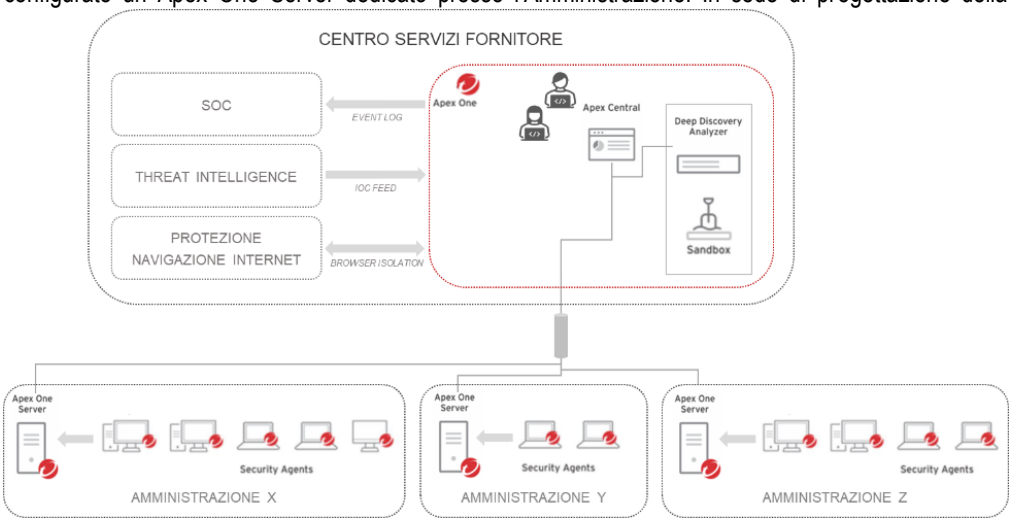

Figura 40 – Architettura del servizio di Protezione degli Endpoint

Si riportano di seguito le **interazioni** principali del Servizio Protezione End Point verso gli altri servizi:

- **Interazione con il servizio Security Operation Center L1.S1**: (cfr. § 6.2 sezione interazioni).
- **Interazione con il servizio Next Generation Firewall L1.S2**: (cfr. § 6.2 sezione interazioni).
- **Interazione con il servizio Web Application Firewall L1.S3**: (cfr. § 6.2 sezione interazioni).
- **Interazione con il servizio "Threat Intelligence & Vulnerability Data Feed" L1.S5**: (cfr. § 10.3 sezione interazioni).
- **Interazione con il servizio Protezione Navigazione Internet e Posta Elettronica L1.S6**: (cfr. § 6.2 sezione interazioni).

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

Una strategia efficace di prevenzione di attacchi di natura cyber prevede l'implementazione di **iniziative formative a carattere innovativo** allo scopo di promuovere comportamenti in linea con i principi e gli obiettivi di sicurezza informatica. L'incremento della **consapevolezza** e della **sensibilità** degli utenti si posiziona quale **obiettivo strategico** per contrastare potenziali minacce informatiche e preservare il patrimonio informativo delle Amministrazioni. In tale contesto il RTI propone un Servizio di "Formazione e Security Awareness" efficace ed efficiente, **caratterizzato da numerosi elementi a valore aggiunto, migliorativi rispetto ai requisiti minimi di gara,** che il RTI è in grado di offrire grazie all'utilizzo di approcci metodologici innovativi riconosciuti a livello nazionale ed internazionale; alle numerose esperienze maturate dal RTI; alle competenze messe a disposizione anche mediante il coinvolgimento dei Centri di Ricerca/Competenza e partnership tecnologiche; all'utilizzo di strumenti e tecniche di apprendimento innovative.

14.1. METODOLOGIE E COMPETENZE MESSE A DISPOSIZIONE

Il fattore umano è ancora oggi un elemento chiave della sicurezza rispetto ai rischi e alle minacce cyber. Per questo, il RTI ritiene che il miglior "firewall umano" sia l'investimento nella formazione e nella sensibilizzazione degli utenti e ha dunque consolidato un approccio didattico basato su **attività formative sinergiche ed eterogenee** volte a incrementare l'attenzione e le competenze necessarie per prevenire e riconoscere potenziali minacce cyber.

Nello svolgimento di tali attività, il RTI fa principalmente riferimento alle **metodologie** ed agli **approcci innovativi** già adottati e largamente validati per attività analoghe in Italia e nel contesto internazionale del suo network.

Le **attività di formazione** sono suddivise in **diverse sessioni**, catalogate per area tematica. Dal punto di vista operativo, ogni fase progettuale prevede l'esecuzione delle seguenti attività:

1) **Pianificazione.** La prima fase del progetto mira a definire in dettaglio le attività, il gruppo di lavoro e i temi specifici da trattare. Il RTI predispone meeting e incontri con i referenti dell'Amministrazione per individuare i temi specifici e pianificare il materiale.
2) **Implementazione.** Formalizzazione del materiale predisposto, a seguito di una adeguata implementazione, per le sessioni di formazione sulla base delle indicazioni e delle scelte dei contenuti formativi fatti dalla stessa Amministrazione.
3) **Condivisione.** Le bozze dei contenuti formativi saranno valutate e approvate dagli organi predisposti dalla stessa Amministrazione dopo opportuna condivisione.

4) **Erogazione.** Il RTI erogherà il servizio attraverso le modalità previste, quali: sessioni di formazioni frontali e/o da remoto, divulgazione del materiale informativo in tema "Security Awareness", somministrazione dei test di verifica e sessioni di review.

Il RTI eroga il servizio di formazione in linea con l'**expertise**, la **seniority** e l'**interesse** dei partecipanti di ciascuna sessione. Ciascuna sessione è adeguata e calibrata secondo la platea di fruitori, garantendo così un significativo coinvolgimento dei partecipanti e una facile ed immediata trasmissione delle conoscenze. Al fine di garantire una efficace erogazione del servizio "Formazione e Security Awareness", il RTI mette a disposizione **specifiche figure professionali** con competenze adeguate maturate in molteplici esperienze pregresse di erogazione di servizi di formazione. Il RTI gode di una **comprovata esperienza** nel settore grazie alla molteplicità di corsi erogati a multinazionali e PMI, nazionali ed internazionali in molti settori: dal farmaceutico, chimico, energetico.

Particolarmente rilevanti sono gli accordi di collaborazione che il RTI ha già in essere con l'**International Institute for Counter Terrorism di Tel Aviv – Israele,** impegnato nella formazione specialistica sui temi della lotta al terrorismo, intelligence e protezione della sicurezza nazionale, e con la **Fondazione YMCA Italia**, con la mission di sostenere attività indirizzate allo sviluppo professionale, per l'erogazione di corsi specialistici di alta formazione su temi specifici in ambito Cyber Security e intelligence, avvalendosi anche di docenti internazionali di comprovata esperienza in contesti operativi sensibili.

Nell'ambito specifico, le figure identificate possiedono una conoscenza approfondita delle diverse tipologie di attacchi informatici, delle policy e linee guida di sicurezza a supporto dei processi organizzativi su diversi ambiti di applicazione (es. gestione del rischio, classificazione delle informazioni, gestione degli incidenti, utilizzo sicuro dei servizi informativi), delle tecniche di attacco e delle metodologie e degli strumenti operativi richiesti nell'ambito dell'Information e Cyber Security. Inoltre, sono previste all'interno del team figure in possesso delle **certificazioni CISM** (Certified Information Security Manager) e qualifica di **Lead Auditor ISO 27001**. Infine, il RTI ha definito un percorso di **formazione continua per il proprio personale** che prevede il conseguimento delle principali certificazioni internazionali in ambito Cyber Security e Information Security (CISA, CISM, CISSP, CSX, CEH, ISO27001, ISO22301, ITIL, COBIT, CIPM, CIPT, etc.). Il RTI garantirà le competenze/certificazioni sopra riportate anche attraverso **le collaborazioni con i Competence Center** (Cyber 4.0, etc.) che garantiranno formazione continua alle risorse del RTI coinvolte nei Contratti Esecutivi (cfr. cap. 17).

14.2. PROPOSTE INNOVATIVE, ADEGUATEZZA DEI CONTENUTI ED EFFICACIA DEGLI STRUMENTI PER L'EROGAZIONE DEL SERVIZIO

L'obiettivo del percorso formativo è quello di **trasmettere le competenze, le tecniche e i metodi necessari** per prevenire e reagire al meglio qualora si verifichi un incidente di sicurezza. Le competenze trasversali, quali la conoscenza dei rischi di sicurezza e il corretto uso dei dispositivi aziendali e personali, ricoprono oggi un ruolo cruciale nel mondo delle Amministrazioni.

Dal punto di vista contenutistico, il servizio di formazione prevede di trattare argomenti di complessità crescente. Questo approccio è in grado di garantire una maggiore assimilazione degli argomenti trattati da parte dei partecipanti e di garantire un'efficace costruzione della consapevolezza delle risorse (fattore umano e strumenti) e del loro utilizzo per ridurre la superficie di attacco e di conseguenza i possibili incidenti informatici. In particolare, il RTI garantisce la **copertura di argomenti di base**, come la protezione dei dispositivi personali e aziendali (es. computer, smartphone e tablet); la formazione del personale in merito **all'importanza e alla protezione delle credenziali d'accesso** (es. robustezza password) e la **salvaguardia dei propri dati e delle informazioni personali**; il **riconoscimento di tentativi di intrusione e truffa** (es. spam, phishing, social engineering); il **governo delle politiche di sicurezza**; l'**analisi del rischio**, anche in relazione alle metodologie AgID e le soluzioni di controllo e pratiche di prevenzione/risposta ad eventuali incidenti.

Figura 41 – Fasi Processo Formazione

Nello specifico, d'accordo con gli organismi, le figure preposte all'interno dell'Amministrazione e le esigenze evolutive dei corsi di formazione**,** il RTI potrà affrontare alcune tra le tematiche sopradescritte con particolare riferimento: ✓alle funzioni dei dispositivi aziendali e alle eventuali minacce e criticità ad essi associate; ✓all'approfondimento dell'importanza delle credenziali di accesso, le loro caratteristiche e i metodi per creare credenziali di accesso efficaci; ✓alle linee guida in merito all'utilizzo dei dispositivi aziendali on-site e in remote-working, d'accordo con gli organi preposti in merito e in linea con le policy dell'Amministrazione di riferimento; ✓all'importanza delle informazioni e dei dati, con particolare attenzione alle caratteristiche peculiari di questi, al fine di garantire una panoramica sulla loro salvaguardia; ✓alle minacce cyber, elencando tipologia e possibili azioni; ✓alla social engineering e al riconoscimento delle truffe; ✓alle principali normative nazionali ed europee in ambito di sicurezza informatica; ✓alle metodologie dell'analisi del rischio; ✓alle indicazioni di eventuali soluzioni di controllo utili alla prevenzione e alla risposta di eventi negativi; ✓all'introduzione alla gestione del rischio e dei comportamenti individuali da usare in caso di incidenti di sicurezza.

Inoltre, il RTI prevede l'erogazione di contenuti formativi in tema di analisi del rischio anche **sulla base del tool di risk assessment dell'Agenzia per l'Italia Digitale (AgID) messo a disposizione della PA**. Lo strumento, accessibile in modalità web, è pensato per guidare l'utente nelle varie fasi di esecuzione del Risk Assessment e consente ad ogni PA di effettuare le operazioni di self assessment, predisporre gli opportuni piani di trattamento ed eseguire il monitoraggio delle iniziative volte a ridurre il livello di rischio informatico. Il RTI prevede l'erogazione dei contenuti formativi relativi attraverso la **predisposizione di lezioni frontali ad hoc** con personale specializzato; la creazione di una sezione dedicata sulla piattaforma e-Learning e la creazione e la diffusione di pillole di sicurezza in merito, al fine di garantire una conoscenza quanto maggiore dello strumento AgID.

L'approccio proposto dal RTI per l'erogazione del servizio "Formazione e security awareness" si articola nelle seguenti iniziative, garantendo così **l'alternanza di pratiche formative tradizionali ed innovative.**

01 **Le attività di formazione verranno così predisposte**, garantendo l'utilizzo di tecniche formative innovative utili per la costruzione ed erogazione dei contenuti:

Preparazione di materiale formativo ed erogazione di sessioni frontali, contestualizzando il materiale in base alle **pratiche operative** adottate dagli utenti (es. Mobile, BYOD, Cloud Computing), al **ruolo** da essi ricoperto e alle necessità dell'Amministrazione (es. normative di settore, minacce già verificate). Il materiale, inoltre, potrà basarsi su **fatti realmente accaduti presso l'Amministrazione**, avvalendosi delle testimonianze delle persone interne coinvolte. Tale approccio innovativo mira a coinvolgere nell'interezza il discente ed alimentare il suo interesse costruendo il know how a partire da eventi

realmente accaduti. Nel corso delle sessioni frontali il RTI garantisce l'erogazione dei contenuti con l'obiettivo di costruire una consapevolezza della sicurezza informatica collettiva quanto più approfondita. Per questo motivo, il RTI identificherà, di concerto con l'Amministrazione e le strutture interne, i contenuti da inserire in **appositi spazi** (es. Piattaforma di e-learning, Portale Intranet dell'Amministrazione) dedicati alla fruizione del materiale condiviso nel corso delle diverse sessioni. All'interno di questi spazi, il RTI potrà prevedere anche l'inserimento di una sezione di "Frequently Asked Questions" (FAQ) che riporterà le domande e le relative risposte che, con ricorrenza frequente, sono emerse nel corso delle sessioni formative. Infine, sarà possibile inserire nella sezione dedicata il materiale multimediale preparato per lo svolgimento delle lezioni frontali ed **eventuali immagini di sensibilizzazione** contenute all'interno delle "pillole di sicurezza" di seguito descritte.

02 **Preparazione e condivisione di un set di "pillole di sicurezza"**. I contenuti delle "pillole di sicurezza" si focalizzano su numerosi aspetti relativi alla sicurezza delle informazioni e includono **suggerimenti e buone pratiche** che prenderanno in considerazione sia le principali minacce cyber (es. Phishing) sia minacce connesse alle nuove tecnologie (es. Mobile, BYOD, IoT). Nelle pillole, inoltre, sono inseriti e approfonditi alcuni esempi riguardanti attacchi realmente subiti dall'Amministrazione allo scopo di sensibilizzare ulteriormente gli utenti. Infine, come sopra riportato, all'interno di ogni pillola è previsto l'inserimento di apposite immagini di sensibilizzazione che possono essere distribuite sui diversi **endpoint dei dipendenti** e fruite anche attraverso la piattaforma di e-learning, di cui al successivo punto 04, messa a disposizione dal RTI. **Si rappresenta in figura un esempio di "pillole di sicurezza".**

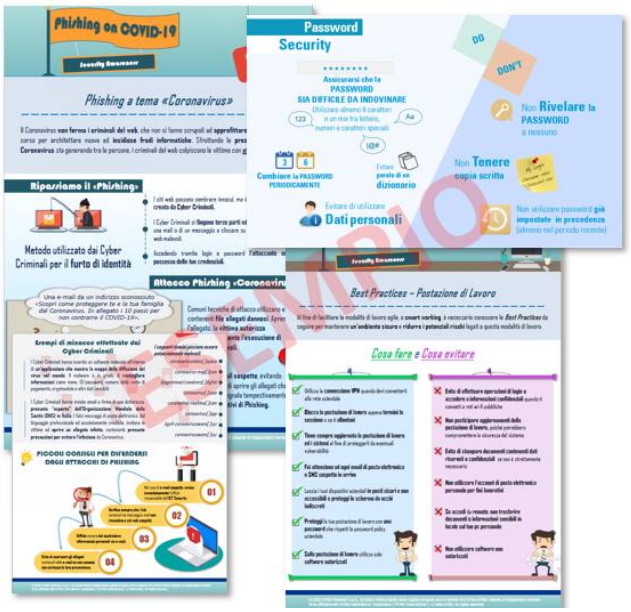

Figura 42 – Esempi di pillole di sicurezza

03 **Diffusione newsletter periodiche.** Le newsletter sono inviate tramite mail a tutti i dipendenti con cadenza concordata con l'Amministrazione in funzione delle esigenze da questa identificate. I contenuti delle newsletter vertono, ad esempio, su tematiche relative alla sicurezza informatica, alla Cyber Security, all'intelligenza artificiale (IA). All'interno delle newsletter sono previsti anche aggiornamenti su fatti ed eventi recentemente accaduti, è possibile includere anche commenti di esperti e di personale interno all'Amministrazione che possa testimoniare su fatti realmente accaduti all'interno della stessa. È inoltre possibile segnalare eventi di interesse comuni relativamente alle tematiche trattate. Le newsletter possono, inoltre, comprendere anche **le "pillole di sicurezza"** predisposte dal RTI ed essere corredate dalle immagini di sensibilizzazione precedentemente citate.

04 **Preparazione e condivisione di materiale informativo tramite contenuti e-Learning anche in modalità escape-room ed erogazione di "Security Gaming".** Lo scopo della condivisione di materiale virtuale è quello di **rendere** accessibile in ogni momento le conoscenze e le informazioni condivise dal RTI e di supportare attivamente l'evoluzione del singolo individuo da potenziale fattore di rischio ad attore protagonista per la difesa di asset e informazioni aziendali. Il RTI offre la **piattaforma di e-learning Cyber GURU** (cfr. §17.2), **personalizzata con logiche innovative di comunicazione, interazione e ingaggio** con un percorso formativo articolato nel tempo che consente di mantenere alta l'attenzione. Grazie alla creazione di un piano editoriale personalizzabile sulla base delle esigenze specifiche e i moduli auto-consistenti, ispirati alla logica del microlearning, l'approccio formativo del RTI favorisce una fruizione allineata all'esigenze dell'utente.

Come elemento a valore aggiunto il RTI si rende disponibile, se richiesto dall'Amministrazione, ad erogare un servizio di supporto e assistenza sulla piattaforma di e-learning allo scopo di favorire un utilizzo corretto da parte dell'utente finale. Il servizio può comprendere, qualora ritenuto necessario dall'Amministrazione, una guida all'utilizzo della piattaforma da pubblicare all'interno dell'intranet aziendale. Il RTI ha sviluppato un **corso completo inerente ai numerosi rischi di natura cyber** ed erogato per mezzo della già citata piattaforma e-learning. Tale corso è supportato da un framework narrativo di riferimento grazie alle tecniche dello storytelling e alle logiche innovative di gamification. Con riferimento a quest'ultimo aspetto, il RTI prevede anche l'erogazione di **"Security gaming"**, della durata di due minuti ciascuno, al fine di migliorare la consapevolezza sull'utilizzo dei dispositivi e degli strumenti informatici.

Tra i temi trattati dai "Security gaming" (es. "Gioco dell'Oca" o "Puzzle Game"): la robustezza delle password, malicious mail, reti sicure e social media. Infine, il RTI prevede anche la predisposizione di **escape-room** dedicate per accrescere il coinvolgimento e la consapevolezza relativa alla sicurezza (es. ai giocatori sono concessi 20 minuti per fuggire da una stanza chiusa a chiave dopo aver trovato una serie di indizi nascosti relativi ai rischi di Cyber Security).

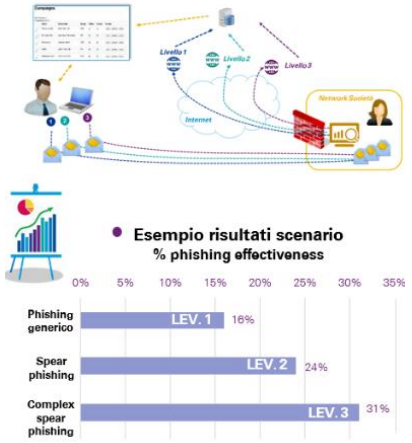

Figura 43 – Esempio risultati scenario

05 **Simulazioni di campagne di Phishing** per sensibilizzare i dipendenti dell'Amministrazione ricreando uno scenario di attacco apparentemente verosimile. L'approccio proposto dal RTI per tali attività si basa sulla corretta individuazione dei possibili elementi di vulnerabilità (es. attuale sensibilità a tematiche di COVID-19) ed al loro exploiting mediante campagne progressivamente evolute. La campagna di phishing viene lanciata da server gestiti dal team del RTI verso i dipendenti dell'Amministrazione, secondo gli scenari concordati. A seguito dell'invio **vengono monitorati i comportamenti degli utenti tramite la console di controllo**.I risultati di questa prima simulazione di attacco phishing vengono raccolti ed analizzati per stimare una panoramica del livello **"**as-is" di awareness. Il RTI è disponibile, se richiesto, ad erogare **simulazioni di campagne di Phishing più sofisticate** (es. Spear Phishing), caratterizzate dall'invio di mail in numero ridotto ma mirate ad un gruppo di destinatari specifici (es. ai dipendenti che sono risultati presentare carenze durante le esercitazioni precedenti).

Il livello di complessità comprende, a titolo esemplificativo, l'inclusione di apposite landing page in cui l'utente viene invitato ad inserire informazioni di carattere personale (es. credenziali di accesso).

14.3. TECNICHE INNOVATIVE DI VERIFICA DEL LIVELLO DI APPRENDIMENTO E SENSIBILIZZAZIONE

Il raggiungimento degli obiettivi formativi e la qualità di tale servizio saranno garantiti mediate l'utilizzo di un approccio metodologico ben strutturato che prevede come punto centrale il monitoraggio continuo dell'apprendimento attraverso una molteplicità di strumenti a carattere innovativo. L'attività di verifica del livello di apprendimento e sensibilizzazione è effettuata mediante l'utilizzo di innovativi strumenti di "*addestramento esperienziale*" ed in particolare mediante **la simulazione di campagne di Phising**, attività già descritta al punto 5 del paragrafo precedente. Tale strumento innovativo consente infatti di verificare sul campo l'effettiva messa in pratica di comportamenti adeguati e delle buone pratiche apprese durante il percorso formativo. Le verifiche del livello di apprendimento vengono effettuate anche attraverso **esercitazioni e sessioni collettive di "Review".** Il RTI predispone dei **test scritti a risposta multipla** che, una volta completati, vengono discussi con tutta l'aula, dando luogo ad una "review" collettiva. Le "Review" finali sono parte integrante dei programmi formativi finalizzati a garantire il confronto tra i partecipanti sulle nozioni apprese, su eventuali dubbi e sulle curiosità emerse. Il RTI prevede la somministrazione di test a risposta multipla e l'inserimento di **quiz anche all'interno della sessione e-Learning.** I test hanno come oggetto tutti gli argomenti trattati nel corso di formazione e sono soggetti ad una correzione collettiva al fine di sensibilizzare e coinvolgere quanto più possibile gli utenti e rispondere ad eventuali curiosità. Oltre ai test a risposta multipla, sono previsti anche **test in modalità multimediale** che possono essere predisposti mediante filmati interattivi incentrati sulle dinamiche proprie del gioco (es. punti, livelli, premi) al fine di sollecitare l'impegno e la competitività sulle tematiche di cyber security, affrontate durante il corso. I test possono essere svolti individualmente e sono suddivisi rispettando le sessioni di erogazione del corso. Il RTI può prevedere, qualora richiesto, una **breve sessione di esercitazione orale per ogni partecipante**. Il formatore responsabile della sessione, a fine programma e a seguito dell'erogazione dei test scritti, sottopone al partecipante un quesito relativo ad un possibile incidente di sicurezza. Al partecipante vengono messi a disposizione cinque minuti per indicare la natura dell'incidente di sicurezza e una sua possibile risoluzione. Al termine dei cinque minuti, il formatore svela la risposta più appropriata e la condivide con l'intera classe per raccogliere eventuali dubbi o commenti.
Inoltre, il RTI aggiunge come ulteriore elemento migliorativo, in base agli ambiti progettuali precedentemente descritti, la predisposizione e la condivisione, con l'Amministrazione, della seguente documentazione:
Executive report: reportistica contenente i risultati di alto livello di tutte le attività svolte ed eventuali suggerimenti al fine di mitigare i rischi derivanti dalle problematiche riscontrate;
Report tecnico: reportistica contenente i risultati tecnici di dettaglio, oltre che la spiegazione puntuale di tutti gli step intrapresi per ottenere i risultati presentati

15. PRESENZA DI ULTERIORI FUNZIONALITA' AGGIUNTIVE

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

16. PORTALE DELLA FORNITURA

Il RTI predisporrà un Portale della Fornitura, raggiungibile tramite Internet, a disposizione delle singole PA per il governo dei servizi, nel rispetto dei requisiti descritti nel Capitolato Tecnico Generale (cfr. §9.1).
Più in generale, il portale previsto dal RTI offrirà servizi: a Consip, per il governo dell'AQ nel suo complesso; alle singole Amministrazioni contraenti per il governo dei Contratti esecutivi affidati al RTI; a tutti gli utenti per la fruizione degli strumenti offerti e la condivisione delle informazioni di interesse.
Il Portale della Fornitura è anche il punto di accesso per i team del RTI per il popolamento dei contenuti e per la normale condivisione della conoscenza.

Figura 44 – Schema del Portale della Fornitura

16.1. SOLUZIONI TECNOLOGICHE E FUNZIONALITÀ DEL PORTALE DELLA FORNITURA

La soluzione proposta deriva dalle esperienze maturata dalle aziende del RTI nella realizzazione di analoghe piattaforme a supporto della gestione di forniture su analoghi contesti di servizio.

La soluzione tecnologica scelta dal RTI per la realizzazione del Portale della Fornitura è basata su uno stack di prodotti prevalentemente open source. In particolare, adotta la piattaforma **Liferay Digital Experience Platform** (Liferay DXP), leader di mercato, che supporta diversi standard d'interoperatività (JSR168, JSR170, JSR160, FTP, WebDAV, CIFS/SMB, Microsoft SharePoint, Web Services, REST API, RSS) consentendo di: ✓accedere ai contenuti attraverso API Standard Content Repository for Java Technology; ✓integrare attraverso WebDAV l'accesso ai contenuti con sistemi Desktop ✓fornire attraverso Web Service un accesso a tutti i servizi della componente di base del sistema portale; ✓scambiare in modo semplice ed efficace contenuti web con altri portali attraverso la tecnologia RSS.

L'adozione della piattaforma Liferay DXP permette al RTI di realizzare il portale in ottica responsive e multi-device in osservanza dei principi di accessibilità definiti dalla Legge Stanca (n.4/2004) e successivi aggiornamenti (come, ad esempio il D.lgs. n. 106/2018) e alle 'Linee guida di design per i servizi web della PA' tracciate da AgID. Il Portale consente l'accesso, in modalità multicanale, a tutti gli strumenti operativi e di governo, in modalità profilata e selettiva: ✓ai referenti dell'Amministrazione per la rispettiva area di competenza, ✓al Management delle aziende del RTI, ✓a tutte le risorse dei Team di presidio e operanti presso le sedi di erogazione, ✓ad eventuali soggetti terzi. Di seguito la descrizione delle principali Aree in cui è strutturato il portale, schematizzate nell'immagine a lato.

Per garantire la completa copertura delle necessità previste dagli atti di gara, il Portale della Fornitura prevede le seguenti funzionalità, ottenute integrando strumenti dedicati: ✓Controllo accessi e gestione identità; ✓Governo fornitura; ✓Gestione della Conoscenza; ✓Analisi dati e reporting; ✓Comunicazione e collaborazione in chiave "social"**.**

Controllo accessi e gestione identità

L'accesso ad alcune sezioni del Portale è possibile previa autenticazione.

Attraverso funzionalità dedicate, è possibile profilare gli utenti, definendone i diritti di accesso. Sono previste, quindi, le principali seguenti categorie di utenti:

1. **Utente Non autenticato**: utente generico del World Wide Web (WWW);
2. **Utenti autenticati** Utente Amministrazione: utente accreditato appartenente ad uno dei soggetti che ha aderito ai servizi della fornitura - Utente Organismi di coordinamento: utente con profilo specifico per l'esecuzione delle attività di Governance della fornitura, con abilitazioni differenziate fra Organismo Tecnico e Organismo strategico - Utente RTI: utenti accreditati rappresentanti il RTI nel presente lotto di fornitura e in dettaglio: Responsabile del contratto (RUAC AQ e RUAC CE), Responsabili Tecnici per l'erogazione dei servizi, e altre figure di riferimento del RTI - Utente Osservatori e CONSIP: utenti accreditati che svolgono le funzioni di monitoraggio della qualità e della sicurezza sulla fornitura.

Governo fornitura

Le funzionalità di Governo della fornitura, in termini di Program e Project Management (PPM), garantiscono un punto di accesso unico per il governo dei progetti e la gestione dei piani e della documentazione a diverso livello di dettaglio (AQ, Contratto Esecutivo e singole iniziative progettuali), profilato secondo gli specifici ruoli dei diversi fruitori: una sezione a livello di AQ offrirà una visione complessiva del contratto mentre sottosezioni specifiche permetteranno di avere le informazioni a livello di singolo CE.

Il RTI prevede di utilizzare, quale piattaforma di PPM, la soluzione basata sulla suite **Microsoft Project**, **Planner**, **Power Automate** integrata in maniera nativa con gli strumenti di Intelligenza Artificiale, denominati Microsoft PowerBI.

La soluzione permette di visualizzare lo stato della "domanda" (fabbisogni delle Amministrazioni) e della "risposta" (CE e relativi progetti), pianificandone l'andamento e monitorarne i progressi in modo centralizzato. Il Portale della Fornitura darà quindi supporto all'intero processo di project management nelle sue "capabilities" chiave:

- Demand management con cui si garantisce una condivisione fra gli attori durante tutto il processo di gestione della domanda;
- Gestione delle risorse, dei costi e del tempo con predisposizione e condivisione del planning e dell'effort complessivo. Il monitoraggio di soglie specifiche permetterà anche di anticipare e segnalare con alert puntuali le situazioni di criticità;
- Workflow personalizzabile relativo a rischi, problemi, decisioni, azioni e cambiamenti per automatizzare e semplificare il lavoro. È possibile, per ciascuno dei ruoli definiti nell'organizzazione, seguire e automatizzare l'intero processo di governo del progetto dall'attivazione alla chiusura delle diverse iniziative;
- Cruscotti e reportistica: si prevedono viste destinate a utenti diversificati nel ruolo:
  - dashboard di AQ, di CE e di progetto che offriranno viste a diverso livello di dettaglio permettendo una valutazione dell'efficacia delle attività svolte in relazione a specifici KPI quali tempi, stato delle attività e obiettivi raggiunti, qualità dei risultati, costi e risorse (umane e no) con valori personalizzabili;
  - grafici interattivi che tracciano il progresso anche di singoli obiettivi o di un gruppo di essi.
- Documentazione operativa: una specifica sottosezione documentale permetterà, nel rispetto agli standard di qualità, di tracciare in maniera strutturata e condividere note di lavoro significative, punti di attenzione, criticità di progetto anche sincronizzandosi con altre fonti dati.

Gestione della Conoscenza

L'area del **Knowledge** è dedicata agli strumenti per la gestione della conoscenza in grado di alimentare, sulla base delle esperienze pregresse e nel corso della fornitura, il cospicuo patrimonio informativo a disposizione del RTI (esperienze, framework per la stesura di componenti di offerta, metodologie e tecniche, white paper, ricerche di mercato, studi sull'evoluzione dei trend tecnologici/normativi). Tale Area permette di poter accedere agli strumenti integrati tra loro e descritti di seguito.

- Knowledge Management System (KMS): il sistema proposto garantisce la condivisione della conoscenza, a supporto delle diverse strutture organizzative coinvolte nella fornitura. Il sistema di KM, basato sull'utilizzo della piattaforma Liferay DXP, garantisce la governance dell'informazione salvaguardandone i contenuti. Tutti i tipi di informazioni / documenti trattati siano tracciati e ricercabili attraverso metadati che ne identifichino la

sorgente, le responsabilità, le modifiche apportate etc. Il sistema di KMS è articolato nelle seguenti aree principali: ✓Article: consente di aggiungere, modificare ed eliminare articoli di tipo knowledge; ✓News: permette di aggiungere, modificare ed eliminare articoli di tipo news; i ✓Libreria Metodologie / Best Practice: adibita alla raccolta di documentazione informativa sulle Metodologie e Best Practice utilizzate dal RTI nell'AQ ✓Q&A: permette di moderare sessioni Q&A tra gli utenti Hot Topics Analytics; permette di analizzare i quesiti e le richieste degli utenti, come pure i tipi di informazione che gli utenti ricercano ✓disponibilità di Strumenti di Collaboration.

- Base documentale (Knowledge Base Management System) Costituisce il repository centralizzato dove archiviare, classificare ed organizzare, i documenti di carattere generale della fornitura riguardanti sia il contesto dell'Appalto Specifico, le finalità e i risultati della fornitura sia i dettagli relativi ai servizi erogabili inclusa la relativa documentazione tecnica di supporto. La categorizzazione documentale è suddivisa in tre aree:
  - **Area Comunicazione**, di libero accesso ai Referenti dell'Amministrazione, ospita i documenti di interesse generale riguardanti il contesto del Contratto Quadro e le specificità dell'Appalto Specifico, le finalità e i risultati della fornitura e i dettagli relativi ai servizi erogabili
  - **Area Informativa**, contiene i documenti relativi alla gestione tecnica dell'Appalto Specifico come ad esempio, documentazione tecnica di supporto, aggiornamento degli asset relativo al parco applicativo e delle informazioni, FAQ, soluzioni degli Incident, Piani di Lavoro, verbali, etc.
  - **Area Deliverable**, dedicata alla raccolta di tutti i deliverable richiesti dall'Amministrazione.

Lo strumento KBMS dotato di un Workflow engine che consente di definire l'iter approvativo per i documenti di fornitura e di un Motore di ricerca semantico: intelligente e personalizzato, che permette di ritrovare documenti di interesse.

16.2. STRUMENTI DI ANALISI DEI DATI E REPORTING

Per le funzionalità di analisi dei dati e reporting il RTI prevede l'uso di **MS Power BI** che tramite report statici e dinamici, offre ai diversi stakeholders la possibilità di effettuare analisi multidimensionali su tutti i parametri caratteristici dell'AQ: 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 CE sottoscritti, etc.. Particolare attenzione è rivolta alla realizzazione dei cruscotti di monitoraggio relativi ai Piani dei Fabbisogni, Piani Operativi e CE. 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. In questo modo sarà possibile tenere sotto controllo anche offline un particolare aspetto dei CE attivi, senza la necessità di dover accedere alla piattaforma.

Figura 45 – Dashboard di reportistica

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

16.3. SOLUZIONI, PROCESSI E STRUMENTI DI COMUNICAZIONE E DI COLLABORAZIONE IN CHIAVE "SOCIAL" CON LE AMMINISTRAZIONI CONTRAENTI

Come soluzioni e strumenti di comunicazione e di collaborazione in chiave "social" il RTI adotta due componenti della piattaforma Microsoft 365: **MS Teams** e **MS Yammer**.

Microsoft Teams è una App di messaggistica che consente di condividere uno spazio di lavoro per la collaborazione e la comunicazione in tempo reale, le riunioni, la condivisione di file fra tutti i membri di un gruppo di lavoro. Permette di comunicare con la massima efficacia, creare team di lavoro con chat di gruppo, organizzare riunioni on line, chiamate, conferenze e condividere documenti.

MS Teams sarà dedicato alla collaborazione nell'ambito dei progetti, sia internamente al RTI, sia per migliorare l'efficacia delle interazioni fra i membri dei gruppi di lavoro del raggruppamento e i referenti delle Amministrazioni contraenti, facilitare e velocizzare le iterazioni.

Le caratteristiche del sistema consentono ai Referenti Tecnici di configurare, modificare e gestire l'organizzazione di "working room" virtuali, in modo semplice ed efficace.

Infatti il sistema consente: ✓la creazione di "stanze virtuali" per le riunioni, dotate della documentazione utile per le fasi preparatorie degli incontri e per la discussione vera e propria. In questo spazio è possibile, inoltre, creare una sorta di blog in cui i partecipanti possono relazionarsi e chiarire eventuali dubbi pre-riunione allo scopo di fare della riunione in presenza un momento di eccellenza e di sintesi; ✓funzioni di video conferenza, per eventuali partecipanti a distanza;

✓funzioni di messaggistica on line con cui la community dei responsabili della fornitura potrà fare domande e fornire risposte in qualunque momento.

MS Teams potrà essere utilizzato nel corso della fornitura per mantenere costantemente aggiornati gli stakeholders dei progressi della migrazione, condividere eventuali criticità ed i punti di attenzione. Potranno essere costituiti Team specifici fra RTI, Amministrazione con canali dedicati al progetto di migrazione oppure dedicati alle attività di revisione degli Indicatori di digitalizzazione congiuntamente con gli Organismi di coordinamento e controllo.

MS Yammer è un Enterprise Social Network (ESN), invece orientato alla comunicazione "esterna". Consente di costituire comunità su scala più ampia tra le diverse organizzazioni coinvolte dall'iniziativa, condividendo e sfruttando le conoscenze e le esperienze maturate nei diversi progetti di migrazione. L'ambito di utilizzo di Yammer si distingue da quello di Teams per la gestione di conversazioni che non passano esclusivamente da meccanismi di chat istantanea, ma che conservano validità per gli appartenenti alla "comunità" anche per periodi più lunghi, come nel caso della condivisione delle esperienze.

17. INNOVAZIONE

Per garantire un elevato livello di innovazione nell'erogazione dei Servizi di gara il RTI propone l'adozione di soluzioni e modalità operative, facendo leva su un approccio organico che valorizza tutti gli elementi distintivi e di unicità del RTI, in termini di:

- **Metodologie, soluzioni organizzative e strumenti operativi** proposti per gestire, per l'intera durata dell'AQ, tutte le attività necessarie a promuovere e diffondere l'innovazione in ciascun ambito dei servizi richiesti e sul singolo CE;
- **Presenza di numerose e complementari strutture operative innovative** (cfr. cap.1 - Ecosistema dell'Innovazione) che saranno coinvolte dall'Innovation Hub e utilizzate sul singolo CE, con ruoli, competenze e attività specifiche assegnate (come illustrato nel seguito del paragrafo), al fine di apportare *know-how* e soluzioni innovative e consistenti per rispondere alle esigenze di trasformazione delle PA aderenti all'AQ.

17.1. METODOLOGIE, SOLUZIONI ORGANIZZATIVE E STRUMENTI ADOTTATI

Per diffondere l'innovazione all'interno dell'Amministrazione, il RTI propone l'adozione di un approccio metodologico di Innovation management "proattivo" e "reattivo" che consentirà di: ✓disporre, sin dalla stipula dell'AQ, di **strutture operative preposte alla gestione dell'innovazione**; ✓utilizzare **modalità operative snelle e flessibili** che permettano di individuare la struttura operativa dell'Ecosistema dell'Innovazione più idonea alle esigenze della singola PA. In tale ottica, l'Innovation Hub assume un ruolo centrale come unità operativa che presidierà, a livello di AQ, tutte le tematiche connesse all'innovazione, gestendo direttamente un framework metodologico e organizzativo pensato appositamente per la presente Fornitura (schematizzato a lato) che: ✓**valorizza le organizzazioni interne dei componenti del RTI** (es. *competence center*, osservatori, *innovation lab*, centri di ricerca e start-up innovative) e dei relativi *network* ed ecosistemi di innovazione presidiati (es. incubatori e acceleratori, *network* di *start-up* e PMI innovative con cui gli operatori economici collaborano stabilmente); ✓**individua e disciplina puntualmente soluzioni organizzative e strumenti operativi** da adottare in ogni fase del *funnel* (imbuto) di innovazione, massimizzando il contributo innovativo da parte di ciascuna struttura operativa ingaggiata in tutti i servizi proposti. In particolare, il *framework* organizzativo e metodologico proposto è articolato nelle seguenti fasi:

FASE 1 (F1): Approach to Innovation Gestita secondo due approcci complementari e sinergici:

- **Approccio proattivo**: le strutture innovative presenti all'interno dell'Ecosistema dell'innovazione implementano un processo virtuoso di monitoraggio dei *trend* di mercato relativi a soluzioni innovative e tecnologie emergenti in ambito della Sicurezza che possono essere oggetto di potenziale interesse per l'evoluzione e innovazione dell'Amministrazione. Tale attività consente al RTI di "anticipare i bisogni di innovazione";
- **Approccio reattivo**: i professionisti del RTI che interagiscono con l'Amministrazione rilevano "sul campo" uno o più bisogni specifici di innovazione direttamente espressi e/o correlati alle richieste di supporto indicate dall'Amministrazione.

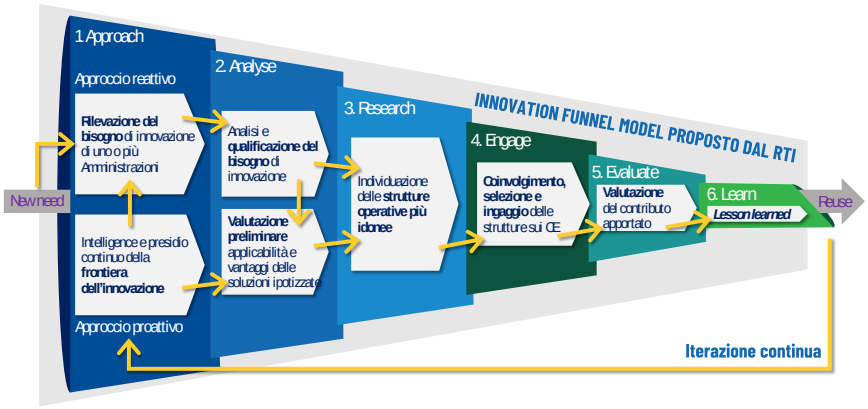

Figura 46 – Innovation Funnel Model

FASE 2 (F2): Analysis Rilevato il bisogno di innovazione, l'Inn-Hub attiverà, coinvolgendo le strutture dell'Ecosistema dell'Innovazione competenti per ambito, una fase di analisi approfondita e qualificazione del bisogno espresso/rilevato sul singolo CE, con la finalità di mappare e declinare puntualmente: ✓**Obiettivi e risultati attesi** dall'Amministrazione; ✓**Soluzioni e tecnologie abilitanti** già esistenti sul mercato per rispondere al bisogno di innovazione ed eventuali *benchmark* e *best practice* da "riusare", sviluppate in ambito pubblico su scala globale; ✓***Stakeholder* da coinvolgere** in fase di progettazione e implementazione della soluzione innovativa; ✓***Key User* e *task owner* dei Servizi e processi** dell'Amministrazione impattati dall'introduzione della soluzione; ✓**Servizi di gara da attivare**.

FASE 3 (F3): *Research* Sulla base delle evidenze raccolte in fase 2, l'Inn-Hub valuta la necessità e le modalità di coinvolgimento, all'interno dei gruppi di lavoro impiegati sui singoli CE, di: ✓**Livello 1**: Strutture operative innovative che fanno parte delle organizzazioni interne degli operatori economici del RTI (es. *competence center*, *tech-labs*, centri di ricerca e sviluppo, osservatori tematici). Esse forniscono ai *team* operativi RTI tutto il *know-how* necessario per la progettazione di soluzioni ad elevato contenuto innovativo; ✓**Livello 2**: Incubatori e acceleratori di innovazione che collaborano stabilmente con il RTI. Tali strutture supportano l'Inn-Hub e le strutture innovative del RTI nell'individuazione delle migliori soluzioni da proporre all'Amministrazione; ✓**Livello 3**: Start-up e PMI innovative che saranno in grado di apportare *know-how* a valore aggiunto e soluzioni ad elevato contenuto innovativo.

La selezione delle strutture da coinvolgere sul singolo CE, è definita di volta in volta dall'Inn-Hub, basandosi sulla valutazione integrata di 5 *driver* di selezione (D): ✓**D1–Innovatività delle soluzioni proposte** ✓**D2–Applicabilità delle soluzioni alle PA italiane**;✓**D3–Tempistiche di ingaggio delle strutture**; ✓**D4–scalabilità e riuso delle soluzioni**; ✓**D5-presenza sul territorio.**

FASE 4 (F4): *Engage* Nell'ambito di tale fase, l'Inn-Hub gestisce il processo di contatto, coinvolgimento e ingaggio delle strutture innovative individuate in Fase 3. In particolare, il modello organizzativo proposto prevede differenti modalità di ingaggio, quali: ✓**Strutture innovative interne**: strutture già integrate nel RTI che coprono a 360 gradi le competenze tematiche, funzionali, metodologiche e tecnologiche relative al contesto di gara, rispetto alle quali è richiesta l'introduzione di soluzioni innovative; ✓**Start-up**: strutture in grado di proporre soluzioni operative e tecnologiche ad elevato contenuto innovativo (soluzioni

disruptive), capaci di avviare all'interno delle PA percorsi di accelerazione dell'innovazione e di trasformazione digitale di Servizi erogati e processi gestiti; ✓**PMI innovative:** strutture presenti sul territorio, capaci di generare innovazione facendo leva sulla conoscenza di esigenze e bisogni specifici del territorio all'interno del quale operano le Amministrazioni; ✓**Ingaggio delle strutture operative individuate:** Le strutture interne sono rapidamente attivate dall'Inn-Hub, andando a completare e integrare i team di intervento con competenze peculiari in linea con l'esigenza espressa dall'Amministrazione. *Start-Up* e PMI innovative sono ingaggiate secondo un modello operativo articolato in più *step*: **1)** preselezione di un *cluster* del *set* di strutture individuato in Fase 3; **2)** contatto, valutazione e selezione di una *short list* di operatori per la definizione di prototipi e/o lo sviluppo di soluzioni-pilota. Gli operatori saranno confrontati in base alle peculiarità specifiche, utilizzando anche modalità di valutazione innovative (es. *Call4Ideas*, *Hackaton*); **3)** integrazione della struttura selezionata all'interno dei *team* di intervento che erogano i Servizi oggetto di fornitura.

FASE 5 (F5): *Evaluate,* al termine delle attività svolte dalla struttura operativa ingaggiata, l'Inn-Hub effettua una valutazione del contributo fornito, con l'obiettivo di valorizzare l'esperienza, in termini di criticità riscontrate e superate, *lesson learned*, *best practices* da poter riusare all'interno dell'AQ. Tale valutazione permette di agevolare eventuali ingaggi futuri della struttura e tiene conto di: ✓***rating*** dell'Amministrazione in termini di soddisfazione rispetto al bisogno di innovazione iniziale; ✓***feedback*** del Responsabile Tecnico del Servizio sul coinvolgimento della struttura in termini di efficacia nelle attività operative; ✓livello di **soddisfazione** espresso direttamente dalla struttura stessa ingaggiata, rispetto alle attività svolte sul progetto.

FASE 6 (F6): *Learn,* L'ultima fase dell'Innovation Funnel Model proposto prevede una fase di sistematizzazione del materiale illustrativo delle soluzioni innovative sperimentate e introdotte sulla singola Amministrazione, con l'obiettivo di condividere i processi digitali a disposizione con tutte le Amministrazioni interessate ad avviare percorsi di innovazione tecnologica e trasformazione digitale.

17.2. SOGGETTI COINVOLTI E PRINCIPALI CARATTERISTICHE

Si riporta di seguito una sintetica descrizione dei Centri di Ricerca, delle PMI e Start-up innovative con cui il RTI collabora per portare valore aggiunto ai servizi erogati.

Il Center for Cyber Security and International Relations Studies (CCSIRS), è parte del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università degli Studi di Firenze e analizza l'influenza del cyberspazio sulla sicurezza nazionale italiana. Il Centro mira ad accrescere e approfondire lo studio delle dinamiche della dimensione cyber attraverso un approccio *policy oriented*. Il suo approccio **multidisciplinare** garantisce l'integrazione dei tradizionali ambiti delle Scienze Sociali (politologia, economia, giurisprudenza, studi strategici e militari), con le discipline proprie dell'Ingegneria Informatica. Inoltre, la fiducia nella ricerca del Centro si traduce in un significativo investimento nel settore R&D, con l'obiettivo di restare sempre aggiornati sugli ultimi sviluppi tecnologici, regolativi e politici, sia in Italia che nel resto del mondo. Questa missione si concretizza non solo con pubblicazioni, documenti di ricerca e analisi indipendenti, ma anche con la partecipazione alle maggiori conferenze relative ai temi di interesse, funzionali agli obiettivi dell'Amministrazione che richiede un **costante aggiornamento**, anche in tempo reale, per erogare servizi coerenti con le novità del settore, attrarre consenso e accrescere competitività.

Cyber Guru, startup innovativa che offre servizi formativi volti a diffondere le buone pratiche per prevenire ed evitare gli attacchi hacker attraverso un sofisticato portale e-learning che consente di incidere in modo concreto ed efficace su attitudini e comportamenti, trasformando le persone in "agenti attivi" del sistema di Cyber Defense. La soluzione permette di **aumentare la consapevolezza** (awareness) degli utenti rispetto ai rischi che si corrono nell'interazione con le tecnologie digitali e con il Web e **di influenzare i comportamenti degli utenti,** per renderli adeguati alle necessità di protezione delle organizzazioni e dei dati aziendali critici e personali, oltre che alle sfide imposte dall'evoluzione del crimine informatico.

Gli **Insights Centre** di KPMG sono importanti showcase hub, localizzati in tutto il Mondo, in ambito di Data & Analytics e Technology Innovation. L'Insight Centre italiano, posto al 9° piano del Building KPMG a Milano, fa parte di un network globale in espansione, con sedi a Tokyo, Londra, Parigi, Madrid, New York, Francoforte, Zurigo, Melbourne, Sydney, Hong Kong, Vancouver e molti altri, si tratta di un'area di circa 500 metri quadri in cui sono concentrate le più importanti tecnologie Data Driven che permettono di gestire, interagire e analizzare i dati per valorizzarne il significato trasformandolo in conoscenza e abilitando nuove soluzioni e modelli di business.

Haruspex, PMI innovativa, nata nel 2016; offre una soluzione di Cyber Security in grado di prevedere, in base al livello di confidenza desiderato, come potrebbe essere attaccata un'infrastruttura ICT, prima che si verifichino gli attacchi, fornendo così soluzioni per neutralizzare gli aggressori. Haruspex utilizza un motore di intelligenza artificiale per costruire un "*digital twin*" degli attaccanti e della struttura, effettuando milioni di simulazioni di attacco e abilitando quindi anche scenari what-if e la security-by-design.

ReeVo, PMI innovativa fondata nel 2003; è il cloud provider italiano focalizzato sui servizi di Cyber Security e archiviazione che consente alle aziende e alle Amministrazioni di proteggere e custodire il vero patrimonio aziendale rappresentato dai dati. ReeVo, oltre a custodire i dati attraverso risorse e piattaforme tecnologiche, analizza le minacce, le vulnerabilità e i rischi dei servizi del cloud e delle reti clienti al fine di proteggerli da attacchi esterni ed interni. Infine, ReeVo dispone di Centri di Competenza distribuiti sul territorio nazionale specializzati nella ricerca di soluzioni innovative specializzate sulla Cyber Security.

Boolebox, PMI innovativa fondata nel 2011; dispone di una suite di applicazioni per la protezione dei dati aziendali che preservano l'integrità e la riservatezza dei dati da qualsiasi accesso non autorizzato, interno o esterno all'azienda, grazie alla crittografia di grado militare e garantendo così i più elevati standard di cifratura per proteggere i dati sensibili dagli attacchi informatici.

Bluenet PMI innovativa che sviluppa nuovi programmi di ricerca e sviluppo di carattere scientifico e tecnologico nei campi dell'informatica e dell'elettronica. Con una consolidata esperienza in applicazioni di controllo accessi, identità legata a documenti elettronici, sistemi operativi per microcontrollori, smart card ed applicazioni NFC, con brevetti e tecnologie innovative già mature. In particolare, Bluenet dispone di una piattaforma di timbro digitale con elevato valore di efficienza, gestione di impronte digitali e riconoscimento facciale.

17.3. AMBITO DI INTERVENTO E VALORE AGGIUNTO CONCRETAMENTE APPORTATO IN TERMINI DI INNOVAZIONE E INCREMENTO DELLE QUALITÀ

Di seguito sono descritti **gli ambiti di intervento** dei Centri di Ricerca, delle PMI e delle Start-up innovative e **il valore aggiunto** concretamente apportato nell'esecuzione delle prestazioni in termini di **innovazione e incremento della qualità**.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Attraverso l'accesso al **know-how**, alle **metodologie** e agli **strumenti** largamente sperimentati, il RTI può conferire un taglio innovativo concreto a molti dei servizi offerti: dalla **formazione**, alle attività di **vulnerability assessment,** alla **gestione del rischio**, alla **configurazione delle strutture organizzative dei diversi servizi**. Inoltre, il Centro mette a disposizione dei team di intervento del RTI know-how verticale a garanzia dell'innovazione dei Servizi di gara erogati; offre contributi tecnico-metodologici (best practice, studi e analisi) rispetto alle soluzioni più innovative e sperimentali proposte dal mercato; collabora all'ideazione e progettazione di soluzioni innovative, con stima di tempi, costi e benefici degli interventi, nonché definizione di nuovi processi e procedure e relativo impatto sui sistemi delle Amministrazioni; contribuisce all'utilizzo di modalità innovative di assessment (ad es. mediante logiche di crowd-testing); dispone di benchmark con realtà assimilabili in contesti nazionali e internazionali. A livello tecnico e pratico, il Centro si pone come obiettivo lo **sviluppo, la produzione e la diffusione di servizi e soluzioni innovative ad alto valore tecnologico**, ad esempio: ✓**Cyber Threat Intelligence,** piattaforma con funzionalità di info-sharing per la gestione dei dati classificati. Il software punta a collezionare, gestire e processare le informazioni non classificate, attraverso l'emissione di report semi-automatici, con elevati standard di qualità garantiti da analisti e componenti AI/ML; ✓**Cyber Human Factor,** l'assessment del livello di esposizione al fattore umano legato al rischio cyber. Il servizio valuta le capacità di risposta, in relazione ai cambiamenti della minaccia e ai rischi cyber correlati con il fattore umano; ✓**Cyber Maturity Assessment,** l'assessment del livello di maturità tecnologica sui più importanti temi della cyber security, sia in termini di tecnologie che di processi interni e/o esterni; ✓**Framework Compliance Tool,** strumento in grado di determinare un piano per ottenere la piena conformità ai maggiori standard dell'IT security. Il software analizza e compara automaticamente più di una decina di riferimenti internazionali (es. ISO, NIST, CMMC), valutando in maniera automatizzata i processi dell'organizzazione e stabilendo le azioni da attuare per colmare i gap identificati. In ultimo, il RTI può attingere al **network di partnership** pubbliche e private di cui gode il CCSIRS e ai costanti aggiornamenti diffusi da questo su diverse tematiche di ricerca come: il Cyber Warfare, la Cyber Diplomacy, la Cyber Security, la Cyber Law, La Cyber Intelligence e il Cyber Terrorism.

CYBER GURU

L'ambito di intervento della start up è focalizzato **nell'erogazione dei servizi di formazione sulla "Security Awareness".** Attraverso un approccio sinergico fra formazione e verifica, Cyber Guru permette al RTI di implementare il servizio di "Security Awareness" su piattaforma digitale, assicurando **metodologie innovative,** e di aggiornare ed arricchire gli argomenti trattati in base alle minacce cyber più rilevanti del momento e/o al maggiore impatto per l'Amministrazione, permettendo la creazione di test di verifica puntuali e concreti. Infine, Cyber Guru offre **sistemi di reportistica** in grado di soddisfare le esigenze di tutte le figure professionali coinvolte a vario titolo nei programmi formativi e addestrativi. Dunque, attraverso il coinvolgimento della Start-up, il RTI garantisce, con particolare riferimento al servizio di "Security Awareness", che:

- gli argomenti trattati siano aggiornati ed arricchiti regolarmente in base alle minacce cyber più rilevanti del momento e/o dal maggiore impatto per le diverse organizzazioni e figure aziendali;
- vengano affrontate nel dettaglio tematiche relative alla Social Engineering (inclusi Phishing, Smishing, Vishing, Fake News, Truffe Telefoniche), alla protezione delle informazioni (inclusi Gestione delle Password, Privacy & GDPR, Utilizzo dei Social Media, Email security, Classificazione delle Informazioni, Dati Personali Identificativi, Navigazione sul Web, Clean Desk, Lavoro Remoto) e alla conoscenza e al corretto utilizzo delle tecnologie informatiche (Dispositivi Mobili & App, Memorie USB, Browser Web, Dispositivi IoT, E-Commerce, Cyber Hygiene, Backup & Restore);
- sia assicurata una efficiente e aggiornata condivisione di buone pratiche.

INSIGHTS CENTRE DI KPMG

L'Insights Centre rappresenta un fattore chiave della strategia di innovazione che trasforma il modo di lavorare, rendendo le persone attive protagoniste, fornendo loro strumenti e un mindset per pensare in modo diverso e supportandole nelle sfide più critiche. La missione del Centro è quella di creare valore tramite insights, facilitation e thought leadership. L'Insights Centre è dunque un importante showcase hub in ambito di Data & Analytics e Technology Innovation e può, quindi, fornire supporto, in fase di erogazione dei servizi di AQ, in svariati ambiti, ad es. nella gestione del rischio e nell'analisi dei dati e supporta i team di intervento nello sviluppo di soluzioni innovative per la digitalizzazione dell'Amministrazione; contribuisce all'utilizzo di strumenti sofisticati di analisi; supporta l'utilizzo di strumenti innovativi. L'Insights Centre ha infatti consolidato nel tempo varie tecniche di facilitazione, pensiero visivo e attività di co-progettazione partecipativa di cui il RTI fa uso per implementare i servizi richiesti, dall'identificazione delle possibili vulnerabilità, alla gestione dei centri servizi e SOC, etc. Inoltre, **gli spazi degli Insights Centre**, qualora richiesto, **possono essere messi a disposizione dell'Amministrazione** per riunioni, meeting e servizi di formazione.

REEVO

Nell'ambito del RTI, ReeVo garantisce esperienza e competenza in ambito Cyber Security e conferisce un taglio innovativo ai servizi erogati, con particolare riferimento alla protezione, vigilanza e gestione dei dati. ReeVo ha realizzato una piattaforma proprietaria per l'orchestrazione e l'automazione degli elementi di Cyber Security. In tale ambito, grazie alle competenze specialistiche di ReeVo, il RTI potrà beneficiare del know how necessario per la realizzazione di playbook innovativi a supporto dell'integrazione e dell'automazione dei servizi di sicurezza nell'ambito della salvaguardia delle informazioni e nel monitoraggio costante della superficie di attacco.

HARUSPEX

L'innovazione portata dalla soluzione Haruspex all'intero processo di **Cyber Risk Assessment, Management e Remediation** consta di una piattaforma predittiva (H-PAR - Predict, Assess, Remediate), capace di identificare tutti i percorsi di attacco e di definire il numero minimo di contromisure per neutralizzare tutti i rischi, e di una soluzione H-CAP (Correlate, Attribute and Predict), che adotta una logica di monitoraggio continuo in grado di proteggere in modo proattivo un'infrastruttura da attacchi in corso. Nello specifico, la piattaforma H-CAP applica tecniche di **intelligenza artificiale** e **big data** per

fondere le informazioni che provengono dai sensori di intrusione, ad esempio SIEM e IDS, con quelle sui percorsi di attacco che sono calcolate proattivamente dalla piattaforma H-PAR. Dunque, la tecnologia messa a disposizione da Haruspex permette di fornire un taglio innovativo ai servizi SOC. Infatti, la fusione precedentemente descritta produce informazioni che consentono al SOC di prevedere i prossimi attacchi, anticipare l'obiettivo degli attacchi in corso e suggerire contromisure dinamiche per ridurre al minimo il rischio. Utilizzando H-CAP, il SOC può implementare dinamicamente contromisure solo quando e se sono necessarie per ridurre al minimo sia il rischio sia l'investimento in sicurezza. Grazie alla conoscenza dei percorsi di attacco, H-CAP può anche scoprire gli attaccanti che stanno sfruttando vulnerabilità 0-day e suggerire in tempo reale le contromisure in grado di proteggere le risorse critiche. Inoltre, H-CAP, integrando AI e digital twin, riduce drasticamente il numero di falsi positivi.

BOOLEBOX

Boolebox rappresenta un attore cruciale per la strategia della protezione dei dati sensibili con particolare riferimento alla protezione dei dati degli endpoint. Come descritto nel capitolo 13, il RTI ha maturato una consolidata esperienza nell'erogazione di servizi di protezione degli endpoint sia nel comparto della PA che nel mondo privato. Boolebox, pertanto, garantisce al RTI un taglio innovativo e strategico di rilievo nella protezione dei dati sensibili. Specificatamente, il RTI, avvalendosi di Boolebox, e delle soluzioni di "Data centric protection", che uniscono logiche di DRM (Digital Right Management), di DLP (Data Loss Prevention), di Encryption, Classification (Cifratura e classificazione dei dati) e funzionalità di CCP (Content Collaboration Platform), integra il processo di gestione sicura dei dati confidenziali degli endpoint delle Control Room del Centro Servizi.

BLUENET

Bluenet, grazie alla sua tecnologia innovativa, supporta il RTI nella predisposizione del servizio di timbro digitale proposto. Il timbro digitale di BlueNet, grazie ad un innovativo algoritmo di compressione e ad un sofisticato software di cifratura, rappresenta il riferimento di mercato per le soluzioni 2D Code con la maggiore densità di dati. BLUeCODE™ è la tecnologia brevettata della startup innovativa Bluenet s.r.l. che permette di creare un "codice bidimensionale" non falsificabile, stampabile con estrema semplicità, facile da apporre in documenti digitali. Di fatto, il BLUeCODE™ può essere utilizzato per memorizzare al suo interno informazioni destinate ad essere consultate e verificate rapidamente con uno smartphone, un tablet o PC. Può contenere una fotografia, testo, dati biometrici (impronta digitale, riconoscimento facciale) o altri tipi di dati, garantendo la protezione delle informazioni. Il BLUeCODE™ si propone come timbro elettronico di certificazione dei dati e allo stesso tempo strumento di protezione e verifica.

17.4. MODALITÀ ORGANIZZATIVE DEL COINVOLGIMENTO, IN TERMINI DI TEMPISTICHE DI INGAGGIO E MODALITÀ DI RELAZIONE CON LE AMMINISTRAZIONI

Il RTI prevede un coinvolgimento continuativo delle realtà innovative sopracitate per l'intera durata contrattuale attraverso un processo di interazione continua con l'Amministrazione che prevede tra l'altro:

- **L'organizzazione di allineamenti mensili tra l'Amministrazione, i soggetti coinvolti e il RTI volti a** garantire un **corretto flusso comunicativo** e un **costante aggiornamento dei temi, delle attività e delle eventuali criticità rilevate**. Agli allineamenti, effettuati in **modalità online**, partecipano **il referente dell'Amministrazione, un referente del RTI e i rappresentanti dei Centri coinvolti a livello di Contratto Esecutivo**. Il fine dell'allineamento non è semplicemente quello di valutare le attività in essere, ma di **riflettere su eventuali estensioni dell'attività** in diversi ambiti al fine di garantire una **contaminazione coerente** tra gli ambiti di interesse per la stessa Amministrazione. Per ogni allineamento viene predisposta **un'agenda del giorno** preventivamente concordata con l'Amministrazione.
- **Allineamenti bisettimanali on-line** della durata di venti minuti **con i soggetti coinvolti e il RTI.** Per **garantire l'apporto di un concreto valore aggiunto attraverso il coinvolgimento delle realtà proposte.** In tale contesto, vengono valutati **eventuali elementi rilevanti da sottoporre all'attenzione delle Amministrazioni contraenti**.

Lo scopo degli allineamenti è quello di **garantire la continua e costante innovazione** su specifiche fasi di erogazione dei servizi e di creare un flusso comunicativo quanto più aggiornato possibile. Le **tempistiche e i luoghi di esecuzione** degli allineamenti potranno variare secondo le necessità dell'Amministrazione e del RTI. I soggetti coinvolti garantiscono massima disponibilità al RTI e all'Amministrazione, assicurando l'ingaggio immediato ogni qualvolta ritenuto necessario dalle Parti.

Le start-up innovative Cyber Guru e Bluenet hanno già in essere dei rapporti continuativi di collaborazione con le aziende del RTI, operando in modo integrato con i Competence Center e le factory del RTI,

Le Boolebox e Haruspex sono state selezionate seguendo il processo del Funnel Model descritto al §17.1.

18. MIGLIORAMENTO SOGLIE INDICATORI DI QUALITA' - TIIS – TEMPO DI PRIMA INVESTIGAZIONE PER INCIDENTI DI SICUREZZA

Il RTI dichiara l'impegno a garantire i seguenti valori di soglia: ✓Gravità Alta, **TIIS <=2 ore solari**; ✓Gravità Media, **TIIS <=4 ore solari**.

19. MIGLIORAMENTO SOGLIE INDICATORI DI QUALITA' - TCIS – TEMPO DI PRIMO CONTENIMENTO PER INCIDENTI DI SICUREZZA

Il RTI dichiara l'impegno a garantire i seguenti valori di soglia: ✓Gravità Alta, **TCIS <=6 ore solari**; ✓Gravità Media, **TCIS <=10 ore solari**.

20. ASSUNZIONE DELLE RISORSE PROFESSIONALI

Il RTI dichiara l'impegno ad assumere persone disabili, giovani di qualsiasi genere, con età inferiore a trentasei anni, e donne per l'esecuzione dei contratti esecutivi o per la realizzazione di attività ad essi connessi o strumentali, in una quota, 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, **maggiore del 35%.**