Implementazione di un sistema di Early Warning per la rilevazione ed analisi delle nuove minacce informatiche

Capitolato Speciale d'Oneri
Capitolato Tecnico All. 1

Indice

1. Premessa

La Funzione di Tutela Aziendale – Analisi Rischi e Security Intelligence - Business Security Intelligence, ha tra i suoi compiti principali quello di prevenire ed anticipare gli incidenti di natura informatica, assicurando l'analisi e l'elaborazione dei dati disponibili ed il monitoraggio del grado di esposizione dell'Azienda ai rischi interni ed esterni, ed individuando e gestendo, di concerto con le funzioni aziendali coinvolte, i fenomeni critici.

In particolare, Poste Italiane si è dotata, nel corso del tempo, di uno strumento di Early Warning, consistente nella piattaforma "portale BSI", che garantisce l'invio delle notifiche relative alla scoperta di nuove vulnerabilità o codici malevoli - con la possibilità di acquisire informazioni relative alle sole tecnologie o prodotti di interesse -, secondo i criteri definiti, a tutti i referenti delle società del gruppo.

2. Ambito di applicazione

Allo scopo di continuare l'acquisizione tempestiva delle informazioni necessarie alla valutazione e segnalazione delle nuove criticità aventi impatto sul business aziendale, si ritiene necessario quindi procedere al rinnovo di licenza del servizio dedicato all'Early Warning attualmente in uso presso il portale BSI, utilizzato nelle fasi di rilevazione, analisi e reportistica dei dati riferiti alle nuove vulnerabilità, malicious code, minacce di natura informatica ed altri segnali di attività sospette.
Si ritiene inoltre opportuno rivisitare, ampliare ed integrare la piattaforma "portale BSI" in una nuova piattaforma di Early Warning ad uso interno di Poste italiane.
Tale servizio dovrà inoltre consentire il supporto del personale di Poste Italiane incaricato della gestione delle criticità nella definizione delle opportune contromisure, delle priorità d'intervento, attraverso una dettagliata strategia di mitigazione delle minacce.

3. Oggetto della fornitura

La gara è ripartita tra licenze e servizi.

3.1.1. Fornitura licenze

- ✓ Una licenza del servizio di **Early Warning** "Deepsight Early Warning Advanced Pack 8.0" per la segnalazione delle nuove minacce, vulnerabilità e codici virali rilevati in rete Internet attraverso la rete di monitoraggio o altri enti qualificati, di durata annuale, comprensiva del servizio di manutenzione per lo stesso periodo.

- ✓ La disponibilità della **banca dati** storica di Symantec di informazioni qualificate ed affidabili riguardanti vulnerabilità, exploit e minacce informatiche, organizzate e strutturate.

3.1.2. Fornitura servizi professionali

- ✓ Creazione della "Nuova piattaforma di Early Warning" partendo dalla manutenzione , integrazione ed evoluzione dell'attuale piattaforma software Interna di Poste Italiane (Portale BSI).Tale piattaforma sarà deputata alla gestione delle fonti dati provenienti dal servizio Deepsight, e da altri servizi interni ed esterni a Poste Italiane in merito alle segnalazioni delle minacce e vulnerabilità (a titolo esemplificativo e non esaustivo pacchetto Secunia Vulnerability Intelligence Manager (VIM) 3.x)

3.1.3. Caratteristiche del servizio Early Warning Deepsight Advaced pack

Il servizio Deepsight Early Warning Advanced Pack 8.0 prevede:

- 2 account amministrativi per il portale online, per accedere alle informazioni del servizio e alla configurazione delle notifiche ai destinatar dei vari alert.
- La possibilità di definire liste (gruppi) di tecnologie (sistemi operativi e/o applicativi), in modo da poter catalogare le varie segnalazioni fornite dal servizio.
- La possibilità di distribuire a 2 differenti destinatari le varie segnalazioni in base alla tipologia di alert e alle liste di tecnologie interessate.
- Le notifiche possono essere inviate via email, RSS oppure SMS.

Le informazioni fornite dal DeepSight Advanced Pack coprono le seguenti tipologie di dati:

- Report Base:

- Livello globale di sicurezza ThreatCon
- Vulnerabilità
- Malicious Code (inclusa documentazione base di reverse engineering, se disponibile)
- Security Risk

- Report Avanzati:

- Domain (su particolari domini Internet configurati dal Cliente)

- Port Activity (su particolari porte TCP/UDP configurate dal Cliente)
- Industry Activity (per settore di mercato)
- Network Infection
- Monitoring da honeynet
- Studi di analisi e ricerca sulla sicurezza in generale o su temi specifici valutati di interesse dal team di Intelligence di Symantec

3.1.3.1. Configurazione e personalizzazione del servizio

Dovrà essere possibile gestire profili tecnologici multipli, ovvero liste di prodotti/piattaforme/vendor per le quali si vogliono ricevere segnalazioni di nuove vulnerabilità, in modo da consentire a Poste Italiane di poter ricevere notifiche personalizzate sulla base delle tecnologie di interesse.

Dovrà essere possibile creare differenti profili di spedizione delle notifiche da collegare con i profili tecnologici al fine di configurare la notifica sui requisiti definiti dal Team di Progetto di Poste Italiane.

Il servizio dovrà essere disponibile in modalità 24x7 e dovrà consentire di ricevere gli alert delle vulnerabilità scoperte e dei malicious code individuati secondo il canale informativo prescelto (e-mail, sms o telefono).

Nel momento in cui viene pubblicata una nuova vulnerabilità o un malicious code che soddisfa i criteri di cui sopra, si vuole ricevere una notifica che riporti una componente anagrafica, una descrizione della vulnerabilità/malicious code, un dettaglio tecnico con relativi sintomi, eventuali patch/hot-fix disponibili o workaround utili alla mitigazione dell'impatto.

3.1.3.2. Centralizzazione dei data feed e pubblicazione

Aggregazione di fonti informative sicure ed affidabili in un data base conforme agli standard.
La correlazione delle stesse alla tecnology list o all'asset, dove presente, fornita da Posteitaliane, dove possibile, ed una lista di sistemi Business Core da tenere sotto particolare attenzione.
Pubblicazione in tempo reale delle notizie su un portale web-based, dove sarà prevista una prima vista di sintesi della minaccia, con particolare accento su :

- l'identificativo univoco della minaccia (CVE ID);

- valutazione a livello globale (cvss2);
- valutazione a livello aziendale, dove possibile;

  (derivante da una correlazione con una tecnology list fornita da poste italiane)
- tecnologia o sistema impattato;
- severity;

La "Notizia di Sintesi" dovrà avare un link diretto alla notizia di dettaglio, con la spiegazione sulla dinamica della minaccia, che riporterà oltre le informazioni sopracitate, anche i possibili interventi di mitigazione (work-around, patch), con la possibilità di allegare, secondo la profilatura, documenti in formato pdf per ampliare il dettaglio.
Tale portale dovrà poter essere profilato per poter garantire la consultazione in base al livello di responsabilità aziendale.

3.1.3.3. Tracciatura delle minacce

Monitoraggio mirato su alcuni applicativi o sistemi Business Critical che permette di dare priorità alle attività di mitigazione degli incidenti in ambienti di particolare interesse per l'azienda

3.1.3.4. Informativa Istantanea e feedback

Ogni minaccia dovrà essere assegnata automaticamente ad uno o a più gruppi in base alla tecnology list o all'asset, dove presente, il ticket generato deve poter prevedere dei campi dove possono essere aggiunti i piani di mitigazione che vengono previsti per poter far fronte alla minaccia
In caso di minacce di carattere d' urgenza, la soglia deve e può subire variazioni che il portale deve prevedere di poter gestire, il sistema dovrà notificare prontamente , via email, ai responsabili preposti, dando notizia su :

- l'identificativo univoco della minaccia (CVE ID) ;
- valutazione a livello globale (cvss2);
- valutazione a livello aziendale, dove possibile;

  (derivante da una correlazione con una tecnology list fornita da poste italiane)
- tecnologia o sistema impattato;
- severity;
- i link alla descrizione estesa sul portale dove si potranno tracciare, ognuno per le proprie competenze, le attività per porre in sicurezza l'infrastruttura in esame.

Dovrà essere predisposto anche un sistema di notifica via sms, con una sintesi di 160 caratteri del caso in esame.

3.1.3.5. Report

Nel portale dovrà essere previsto una sezione per la reportistica delle minacce, in base alla tecnologia, il tipo e all'impatto sui servizi aziendali.
Inoltre una vista in tempo reale quelle a più grave impatto, con la tracciatura delle contromisure e sullo stato avanzamento lavori

3.1.4. Caratteristiche della Banca Dati storica

Il servizio fornito deve rendere disponibile, tramite portale Internet, una banca dati contenente i dati storici riguardanti le varie tipologie di attacco, vulnerabilità e codici malevoli (malicious code). In aggiunta è richiesto il rispetto dei seguenti requisiti:

- ✓ Eventuale integrazione con altre soluzioni (ad esempio asset configuration management) attraverso standard aperti;
- ✓ Accesso mediante front-end web;
- ✓ Aggiornamento dei dati in tempo reale;
- ✓ Durata della licenza pari almeno a 12 mesi.
- ✓ Tipologie di filtri/viste gestite da un "super-user e personalizzabili";
- ✓ Modalità di notifica via e-mail, sms;
- ✓ Possibilità di accedere ai contenuti secondo ruoli diversi;
- ✓ Possibilità di attribuire il livello di rischio alle minacce in modo personalizzabile dall'utente;
- ✓ Disponibilità di report predefiniti e personalizzabili.

4. Requisiti Minimi obbligatori della fornitura

Le caratteristiche elencate nel presente capitolo si intendono minime e obbligatorie, pena l'esclusione dalla gara.
Le caratteristiche migliorative rispetto a quanto prescritto non saranno oggetto di valutazione ai fini dell'aggiudicazione.

4.1. Requisiti generali

Codice Requisito	Descrizione Requisito
EW_REQ_1.	Come caratteristica generale, valida per tutti i componenti software della fornitura offerta dall'Impresa, si richiede che: - la tecnologia di tutti i componenti sia di ultima generazione; - per nessun componente sia stata annunciata, al momento della presentazione dell'offerta, la messa fuori produzione dello stesso o la sospensione del relativo supporto da parte del produttore; nel caso in cui detto annuncio venga effettuato nell'arco dei quattro anni successivi all' aggiudicazione, l'impresa si impegna a garantire a Poste Italiane il supporto di tutte le componenti oggetto della fornitura fino alla scadenza dei quattro anni.
EW_REQ_2.	Poste Italiane non potrà accettare applicativi software che siano in Beta Test o comunque non ancora ufficialmente rilasciati.
EW_REQ_3.	**Freeware – Shareware – Open Source** Non sono ammessi prodotti Freeware, Shareware ed Open Source con la sola eccezione di componenti di sistema, quali application server e database utilizzabili al solo scopo di gestione temporanea del dato. In questo caso, la componente va garantita come parte organica della soluzione offerta e deve essere certificata dall'impresa, che ne garantisce la completa compatibilità ed integrazione con la piattaforma nonché l'evoluzione tecnologica e la manutenzione nell' ambito della soluzione offerta.
EW_REQ_4.	L'Impresa si impegna a definire un'architettura logica, basata sulle risorse informatiche messe a disposizione da Poste Italiane, che garantisca la completa scalabilità per far fronte, con un'aggiunta di componenti hardware che non modifichino l'architettura indicata e che si integrino con quanto offerto, sfruttando parti di quanto in essa previsto, ad un aumento nella quantità di dati, nel numero di utenti concorrenti e nelle performance, senza la necessità di modificare il software applicativo ed il modello dati.
EW_REQ_5.	Il software sviluppato o integrato nella soluzione offerta deve essere conforme agli standard adottati presso il Sistema Informativo di Poste Italiane; in particolare: • le interazioni legate alle analisi statistiche avanzate, legate ad un numero limitato di utenti, dovranno essere effettuate tramite un interfaccia Client. La piattaforma dovrà poi rendere disponibile la possibilità di esportare i risultati di queste analisi in formato WEB; • Le interazioni uomo-macchina per gli utenti finali devono avvenire attraverso una interfaccia utente WEB; • le comunicazioni tra i vari componenti client e server applicativi devono utilizzare il protocollo HTTP o HTTPS.

Codice Requisito	Descrizione Requisito
EW_REQ_6.	La piattaforma di Early Warning deve prevedere il tracciamento delle attività svolte dagli utenti con diritti di amministrazione.

4.2. Requisiti di integrazione con l'ambiente operativo di Poste Italiane

Ai fini della realizzazione del progetto, risulta determinante l'impegno, da parte dell'Impresa, ad acquisire le competenze e le conoscenze necessarie per la salvaguardia degli investimenti pregressi intrapresi da Poste Italiane, che si concretizzano in una perfetta integrazione della fornitura con il contesto operativo, organizzativo e tecnologico nel quale opera il Sistema Informativo di Poste Italiane.

La piattaforma oggetto di fornitura dovrà quindi garantire i seguenti requisiti di progetto:

Codice Requisito	Descrizione Requisito
EW_REQ_7.	Integrazione della Nuova piattaforma di Early Warning con i sistemi già in esercizio presso la Centrale Allarmi di Poste Italiane, con particolare riguardo alle funzioni del Portale Web BSI, quale strumento di consultazione delle informazioni rese di volta in volta disponibili, ad uso delle funzioni interne interessate (a titolo esemplificativo e non esaustivo pacchetto Secunia Vulnerability Intelligence Manager (VIM) 3.x).
EW_REQ_8.	Conformità delle istruzioni operative prodotte nell'ambito del progetto con l'insieme di normative, standard e procedure, già in vigore presso il Sistema Informativo di Poste Italiane.

4.3. Requisiti funzionali Nuova piattaforma Early warning

Di seguito sono descritti I requisiti della Nuova piattaforma di Early Warning che andrà ad integrare e migliorare le attuali funzionalità del portale BSI.

4.3.1. Componente Repository Nuova piattaforma Early Warning

Di seguito sono descritti i requisiti minimi relativi al Repository Centralizzato del sistema di Early Warning, configurabile, scalabile ed estendibile nel tempo.

Codice Requisito	Descrizione Requisito

Codice Requisito	Descrizione Requisito
EW_REQ_9.	La soluzione deve essere strutturata in modo che ogni informazione ed i dati correlabili provenienti dai sistemi in uso siano archiviati in una base storica, convenzionalmente denominata **Early Warning Repository,** in cui devono essere custoditi per un periodo di tempo sufficiente, al fine di consentire elaborazioni ed analisi statistiche.
EW_REQ_10.	Per la conservazione del dato centralizzato non potranno essere utilizzati tecnologie o prodotti Freeware, Shareware ed Open Source.
EW_REQ_11.	Il modello dati del **Early Warning Repository**, dovrà essere **configurabile e scalabile**, andando a reperire, laddove possibile, le informazioni tramite flussi di elaborazione schedulati.
EW_REQ_12.	La soluzione deve prevedere funzionalità di **controllo della qualità dei dati** (duplicazione, validità, mancanza informazioni) al fine di evidenziare eventuali anomalie nei dati da sottoporre ad analisi statistiche.
EW_REQ_13.	La soluzione deve prevedere la gestione dell'AGGIORNAMENTO dei dati storicizzati, al fine di garantire la necessaria rapidità ed affidabilità nella gestione dello storage a disposizione, nonché la possibilità di estendere temporaneamente il periodo di giacenza dei dati, al fine di consentire elaborazioni ed analisi statistiche rilevanti.
EW_REQ_14.	La soluzione e gli sviluppi devono prevedere l'integrazione , nelle nuove basedati, dei dati presenti nelle Repository "Vulnerabilities" e "Malicious code" della Portale BSI.
EW_REQ_15.	La soluzione e gli sviluppi dovranno customizzare la reportistica standard al fine di rendere disponibile: ○ reportistica di sintesi sulle vulnerabilità e minacce informatiche di potenziale impatto sui sistemi e la tecnologie in uso a Poste Italiane; ○ reportistica di dettaglio sulle vulnerabilità e minacce informatiche ○ reportistica su singola vulnerabilità o minaccia.
EW_REQ_16.	I servizi intesi allo sviluppo applicativo dovranno implementare e personalizzare l'applicativo per una adeguata gestione documentale della reportistica prodotta. In particolare: ○ gestione del ciclo di vita dei documenti; ○ funzioni di ricerca avanza; ○ backup.
EW_REQ_17.	Il modulo deve permettere l'esecuzione di operazioni di **manipolazione dati**: unione, ordinamento, concatenazione, sottoinsiemi, suddivisioni archivi, aggregazione dati categorici, al fine di considerare anche informazioni esterne al Repository

Codice Requisito	Descrizione Requisito
EW_REQ_18.	La soluzione deve consentire la **visualizzazione** di grafici e report statistici in una stessa finestra, al fine di poter individuare con facilità la presenza di dati anomali e correlazioni tra le grandezze, mediante appositi tool guidati.
EW_REQ_19.	La soluzione deve rendere disponibili funzionalità di grafica standard (torte, istogrammi, tabelle riassuntive, ecc.).
EW_REQ_20.	Deve essere possibile esportare i dati in formato, testo, CSV, XML, PDF, HTML, JPEG/GIF/PNG.
EW_REQ_21.	Deve consentire la condivisione delle analisi in appositi file di progetto, che possono essere salvati su un server centralizzato o spediti via e-mail, per dare la possibilità a un team di analisti di lavorare in modo condiviso sui modelli di analisi.
EW_REQ_22.	La soluzione deve prevedere la definizione di **regole User-Driven**, ovvero condizioni e criteri di selezione complessi, al fine di evidenziare eventi rilevanti per la sicurezza.
EW_REQ_23.	I risultati delle esecuzioni delle regole dovranno poter essere **rappresentabili in vari formati** (Excel, HTML, CSV, XML, file di testo, PDF), in modo da poter pubblicare e distribuire le evidenze delle occorrenze relative all'evento identificato.
EW_REQ_24.	I risultati dell'esecuzione delle regole **dovranno poter essere esportati e salvati** all'interno del Repository, per la storicizzazione delle evidenze e per consentire ulteriori manipolazioni dei dati.
EW_REQ_25.	La soluzione deve prevedere la possibilità di **tenere traccia dei cambi avvenuti storicamente,** consentendo di riallocare i dati storici in funzione delle evoluzioni avvenute ed effettuare analisi storiche coerenti.
EW_REQ_26.	Il modulo **deve poter abilitare report ed analisi sui rischi di Sicurezza** e Tutela definiti. Report quali livelli di esposizione di date aree o sistemi.
EW_REQ_27.	In funzione delle evidenze legate agli indicatori, dovrà essere disponibile una componente che consenta di definire **criticità** (associate ad esempio all'impatto di una vulnerabilità su di un sistema) e **piani d'azione** volti alla risoluzione di esse. I form di gestione di criticità e piani di azione devono essere personalizzabili mediante campi aggiuntivi per l'inserimento delle informazioni necessarie. Dovrà inoltre essere possibile definire un **workflow** che autorizzi il supervisore allo svolgimento delle attività di propria competenza.

4.3.2. Componente Web & Documents Reporting Interface Nuova piattaforma Early Warning

Tale modulo deve permettere di organizzare ed accedere a tutte le informazioni prodotte dalla piattaforma, comprendendo sia le informazioni utili al controllo della piattaforma stessa sia quelle derivanti dalle operazioni di correlazione ed analisi.

Codice Requisito	Descrizione Requisito
EW_REQ_28.	Il modulo deve permettere l'accesso via Web ai risultati prodotti dalla piattaforma.
EW_REQ_29.	Il modulo deve permettere di organizzare e strutturare i risultati prodotti, in modo da semplificare l'accesso ed il reperimento delle informazioni.
EW_REQ_30.	Il modulo deve permettere di effettuare, direttamente dall'interfaccia Web, le procedure di analisi predisposte.
EW_REQ_31.	Il modulo deve consentire la creazione e manutenzione tramite interfaccia web di cruscotti di sintesi o **dashboard** quale riepilogo dello stato di rischi, valutazioni qualitative, etc. il tutto profilato secondo ruolo e funzione all'interno di Poste Italiane.
EW_REQ_32.	Il modulo deve **consentire la creazione tramite interfaccia web di report di dettaglio** ed analisi, andando via via più nel dettaglio attraverso drill-down successivi.

4.4. Servizi Professionali

Codice Requisito	Descrizione Requisito
EW_REQ_33.	La fornitura deve prevedere un effort totale di almeno **160 gg./uu.**, suddiviso per le diverse figure professionali proposte.

4.4.1. Figure professionali e skill-mix

Nella Tabella che segue è riportato il fabbisogno stimato per la fornitura in gara, in base alle Figure Professionali richieste, e il relativo skill-mix minimo richiesto:

Scheda Tecnica Servizi Offerti			
Figura Professionale	**Fabbisogno Stimato (N° Risorse)**	**Fabbisogno Stimato (N° gg/uu)**	**Profilo**
Project Manager	1	40	Master
Security Specialist	2	120	Senior
Totale	**3**	**160**	

Di seguito si riportano, per ogni profilo e figura professionale: l'esperienza di riferimento, le conoscenze e le competenze professionali richieste.

Codice Requisito	Descrizione Requisito
EW_REQ_34.	I Profili **Master** devono possedere un'esperienza generale ICT di almeno 10 anni
EW_REQ_35.	I Profili **Senior** devono possedere un'esperienza generale ICT di almeno 7 anni
EW_REQ_36.	**Conoscenze generali** Le risorse utilizzate dall'Impresa devono dimostrare di avere maturato esperienze progettuali che coprano le seguenti aree di interesse: • progettazione, sviluppo ed esercizio dei sistemi IT • progettazione e realizzazione di progetti di Information Security
EW_REQ_37.	**Competenze metodologiche** Tutte le risorse messe a disposizione devono possedere le seguenti competenze metodologiche: • padronanza delle principali metodologie di sviluppo e collaudo • padronanza delle principali metodologie, tecnologie e prodotti di integrazione sistemi • padronanza delle metodologie di valutazione e reporting delle attività di sviluppo • padronanza delle metodologie di controllo e riduzione del rischio: – Riskassessment/management – Configuration&quality management
EW_REQ_38.	Le risorse di Figura professionale Project Manager devono possedere le seguenti caratteristiche: • **Profilo professionale:** Master • **Seniority professionale:** seniority di almeno 7 anni nella definizione

Codice Requisito	Descrizione Requisito
	pianificazione e conduzione di progetti in ambito ICT. Il ruolo richiede un bagaglio di esperienze professionali accumulate in almeno 10anni lavorativi ed esperienze progettuali maturate in realtà aziendali di analoga complessità. • **Certificazioni necessarie:** – ITIL 3
EW_REQ_39.	Le risorse di Figura professionale **Security Specialist** devono possedere le seguenti caratteristiche: • Profilo professionale: Senior • Formazione scolastica a livello universitario • Seniority professionale: Conoscenza ed esperienza applicativa nell'impiego delle metodologie di progettazione e implementazione di sistemi di almeno 5 anni **Attività specifiche del ruolo:** • Referente dei contenuti di Business e dell'analisi degli User Requirement • Responsabile della definizione della metodologia di calcolo adottata, degli indicatori di interesse e degli algoritmi di calcolo – Conoscenza delle prassi di gestione del rischio IT – Personalizza gli algoritmi di calcolo – Documenta le procedure di calcolo – Esegue i system test – Supporta il collaudo finale del sistema di analisi • **Conoscenze e competenze specifiche:** – capacità di ideare e sviluppare la soluzione sulla base dei requisiti espressi dal Cliente – conoscenza avanzata delle basi di programmazione sia procedurale sia object-oriented – conoscenze specialistiche approfondite tali da poter supportare l'azienda nelle fasi di analisi preliminare, impostazione e sviluppo di progetti complessi e/o nelle valutazioni dell'utilizzo di tecnologie emergenti. – consolidata esperienza pluriennale sull'intero ambiente di configurazione / sviluppo ed esecuzione del prodotto specifico. – conoscenze specialistiche approfondite in amministrazione di sistemi/database con tecnologie specifiche ovvero in specifici campi di applicazione; – capacità autonoma di configurazione e di problemsolving.
EW_REQ_40.	La fornitura deve essere realizzata da personale in possesso dei requisiti sopra riportati e rispondente allo skill-mix minimo indicato nella Tabella 1. Il criterio guida utilizzato per la classificazione è quello della seniority ovvero

Codice Requisito	Descrizione Requisito
	l'esperienza professionale maturata: il profilo di livello più alto (Master) corrisponde a quello con la massima esperienza informatica, sia in termini tecnologici, sia in termini di abilità a collegare le evoluzioni dell'informatica stessa al business.
EW_REQ_41.	**Staffing risorse** Le risorse dovranno essere rese disponibili al più entro 20 giorni naturali consecutivi dalla data di stipula del contratto.
EW_REQ_42.	**Costituzione Team** Il Team per l'erogazione dei servizi dovrà essere costituito nella sua globalità al più entro 25 giorni naturali consecutivi dalla stipula del contratto. All'atto della costituzione del Team, Poste Italiane procederà a verificare, anche attraverso colloqui, la corrispondenza delle risorse fornite rispetto ai requisiti richiesti e a quanto indicato dall'Impresa nella documentazione di gara presentata. Nel caso in cui una o più risorse del Team risultino non corrispondenti e/o siano ritenute da Poste Italiane non adeguate alle attività da svolgere, l'Impresa è tenuta alla loro immediata sostituzione con altre idonee di livello, profilo, certificazioni ed esperienza analoghi o superiori a quelle richieste ed offerte, senza che ciò comporti costi aggiuntivi per Poste Italiane. Il consolidamento del Team dovrà concludersi al più entro 45 giorni naturali consecutivi dalla stipula del contratto, fermo restando quanto disposto in materia di subappalto (si vedano le Disposizioni contrattuali di riferimento). Trascorso tale termine senza che il Team sia stato consolidato in maniera conforme, Poste Italiane, dopo formale diffida, procederà alla risoluzione del contratto, dando corso all'incameramento della cauzione, salvo risarcimento dei maggiori danni. A conclusione delle verifiche positive sarà redatto, dal Responsabile di Progetto incaricato da Poste Italiane, il *Verbale di rispondenza*, necessario per la prosecuzione della fornitura. L'Impresa si impegna a mantenere la stabilità del Team iniziale durante l'intero periodo di validità contrattuale e ad assicurare la sostituzione al più di **una** risorsa, per propria decisione o su richiesta di Poste Italiane. E' fatta salva la possibilità per Poste Italiane di verificare, anche in corso d'opera, la corrispondenza delle risorse fornite rispetto ai requisiti richiesti e a quanto indicato dall'Impresa nella documentazione di gara presentata. Nel caso in cui una o più risorse risultino non corrispondenti e/o siano ritenute da Poste Italiane non adeguate alle attività da svolgere, l'Impresa è tenuta a sostituirle, entro 15 giorni naturali consecutivi dalla richiesta, con altre idonee di livello, profilo, certificazioni ed esperienza analoghi o superiori a quelle richieste ed offerte, senza che ciò comporti costi aggiuntivi per Poste Italiane.

4.4.2. Servizi di Analisi e Personalizzazione Applicativo

In seno alle attività previste dal presente documento, particolare rilevanza detengono le attività di analisi e progettazione della "Nuova piattaforma di Early Warning":

Codice Requisito	Descrizione Requisito
EW_REQ_43.	L' attività progettuale deve coprire le seguenti aree: • Project Management tecnico ed organizzativo; • Analisi del contesto e dei requisiti; • Servizi di Installazione e Configurazione della piattaforma; • Integrazione manutenzione ed evoluzione della piattaforma Portale BSI; • Esplorazione ed Analisi dei dati di sicurezza; • Costruzione degli Indicatori; • Esplorazione ed Analisi dei dati; • Integrazione dei servizi di Alerting a disposizione; • Attività di tuning, customizzazione e training della piattaforma; • Formazione del Team di analisti di Tutela Aziendale; • Avviamento all'Esercizio; • Collaudo della piattaforma.
EW_REQ_44.	Inoltre devono essere forniti anche: • manutenzione delle componenti software in fornitura nonché delle componenti derivanti dalle attività di sviluppo: attivata dalla data di collaudo e garantita per la durata di 12 mesi.

4.4.3. Servizi di supporto al roll-out: tuning e collaudo

I servizi forniti devono rispondere ai seguenti requisiti.

Codice Requisito	Descrizione Requisito
EW_REQ_45.	Per l'ambiente ditest interno, l'Impresa: • deve effettuare l'eventuale installazione del software applicativo • ha in carico la gestione delle configurazioni del software applicativo • deve predisporre i piani tecnici di dettaglio, verificandone la coerenza e l'aggiornamento per la durata dell'intero progetto • deve predisporre un documento con la descrizione delle attività e il relativo effort previsto a carico della struttura di Poste Italiane
EW_REQ_46.	L'Impresa deve fornire, in occasione della presentazione dei piani di collaudo, l'indicazione di dettaglio della propria metodologia di collaudo e rilascio
EW_REQ_47.	La metodologia di progetto proposta deve prevedere l'effettuazione delle attività di testing articolata su tre livelli: test di sistema, test di integrazione e test unitario. Nel caso del test unitario è sufficiente specificare i test effettuati e la metodologia di applicazione adottata. Nel caso dei test di sistema e dei test di integrazione occorre documentare nel "Piano

Codice Requisito	Descrizione Requisito
	dei test" i casi di test, previsti e preventivamente concordati con Poste Italiane, nonché il dettaglio degli esiti di applicazione degli stessi. L'accettazione da parte di Poste Italiane del processo e degli esiti dei test effettuati è propedeutica per avviare la fase di collaudo parziale o globale del sistema. Verrà nominato da Poste Italiane un responsabile unico per tutte le fasi di collaudo. Il collaudo sarà svolto nei tempi previsti da Poste Italiane e con il supporto dell'Impresa, che si dovrà assumere la responsabilità diretta dell' esecuzione delle relative attività. La durata del collaudo sarà specificata tenendo conto anche dell'eventuale periodo di predisposizione dell'ambiente. L'attività verrà svolta in ambienti logistici individuati da Poste Italiane con le modalità indicate dal "Piano di Collaudo" redatto dall'Impresa e approvato da Poste Italiane. Nell'ambito del "Piano di Collaudo" l'Impresa sottoporrà, per l'approvazione, le procedure di collaudo specificando: • gli strumenti che intende impiegare • le strutture organizzative dell' Impresa e di Poste Italiane responsabili delle diverse fasi di collaudo • le modalità di registrazione dei dati • Il "Piano" dovrà inoltre essere così articolato: o designazione, da parte dell' Impresa del proprio rappresentante e delle risorse in possesso delle specifiche competenze ritenute necessarie che lo coadiuveranno nello svolgimento dell'attività o pianificazione di dettaglio delle prove di collaudo o condizioni di collaudo o moduli, report, procedure di alimentazione sottoposti a verifica o criteri di gestione dei malfunzionamenti o tipologie di test previste o condizioni di accettabilità/rifiuto della prova. Saranno altresì oggetto di verifica durante il periodo di collaudo oltre al software realizzato, tutti gli altri prodotti della fase realizzativa: • analisi di migrazione • disegno di dettaglio • piano dei test e documenti a supporto • manuale operativo di esercizio • piano di roll-out • lista oggetti di consegna • risultati dei tests. La conformità di quanto sopra verrà sancito attraverso un documento formale di accettazione. Durante la fase di collaudo le attività richieste all'Impresa sono: • supporto alla predisposizione dell'ambiente di collaudo: l'attività è volta a dare supporto alle strutture di Poste Italiane che devono predisporre l'ambiente di collaudo quali: definizione e caricamento della base dati, installazione del software applicativo, personalizzazione del software di base • supporto durante l'esecuzione del collaudo: tale supporto dovrà prevedere una illustrazione del sistema realizzato, e, per tutta la durata del collaudo: o un responsabile del collaudo, cui segnalare i problemi o il supporto all' utilizzo delle funzionalità realizzate.

4.4.4. Tempi di realizzazione e piano di Roll out

Il fornitore dovrà garantire l'avvio dell'implementazione del sistema di Early Warning, nel rispetto dei requisiti funzionali esposti nel presente documento, secondo il seguente ordine :

- entro 7 gg. lavorativi dalla data di stipula del contratto dovrà essere attivato il servizio Deepsight e configurato all'interno del "portale BSI".
- entro 20 gg. lavorativi dalla data di stipula del contratto dovrà essere caricata la parte di storico mancante ,proveniente dalla Banca dati Symantec, all'interno del portale BSI.
- entro e non oltre il 31/12/2012 dovranno essere ultimati tutti gli sviluppi previsti dai servizi professionali ed oggetto di questo capitolato.

Durante le varie fasi del progetto il fornitore garantire la continuità delle attuali attività di Security Advisory, senza causare alcun disservizio nel raggiungimento dei risultati richiesti.

4.5. Garanzia

Codice Requisito	Descrizione Requisito
EW_REQ_48.	**Garanzia:** Lo sviluppo del software oggetto di fornitura, nonché le componenti derivanti dalle attività di sviluppo, devono essere garantite e manutenute dalla consegna e per un periodo di 12 mesi a partire dalla data di collaudo.

4.6. Servizio di manutenzione correttiva ed evolutiva nel periodo di garanzia della piattaforma evoluta

Codice Requisito	Descrizione Requisito
EW_REQ_49.	Il servizio di manutenzione deve comprendere: • **Manutenzione correttiva**, che assicura il ripristino delle funzionalità a seguito di malfunzionamenti dei componenti software oggetto della fornitura • **Manutenzione evolutiva**, che assicura il diritto ad acquisire, in modo gratuito e senza limitazioni, le nuove release/versioni dei componenti software oggetto della fornitura.
EW_REQ_50.	**Manutenzione correttiva: modalità generali del servizio** Gli interventi correttivi comprenderanno la diagnosi di tutti i malfunzionamenti segnalati, il ripristino del servizio, la risoluzione completa

<table>
<tr><th>Codice Requisito</th><th>Descrizione Requisito</th></tr>
<tr><td></td><td>delle anomalie (comprese le eventuali sostituzioni dei componenti danneggiati e l'aggiornamento della relativa documentazione e manualistica) e le relative comunicazioni al responsabile che ha segnalato l'anomalia stessa.
Per ciascun intervento sarà cura dell'Impresa produrre un Rapporto di Intervento.
Il suddetto Rapporto di Intervento deve contenere almeno le seguenti informazioni:
• data e ora di apertura del malfunzionamento;
• ticket rilasciato dall' Impresa;
• data e ora della risoluzione del malfunzionamento;
• sito e nominativo del dipendente o della struttura di Poste Italiane che ha effettuato la richiesta;
• tipologia di modulo software soggetto al malfunzionamento;
• descrizione del malfunzionamento riscontrato;
• eventuale sostituzione del modulo software con uno di caratteristiche funzionali e prestazionali uguali o superiori.
Il ripristino della funzionalità deve essere sottoscritto dall'utilizzatore del componente danneggiato o da altro dipendente di Poste Italiane che certifichi la piena funzionalità delle parti oggetto dell'intervento.
Il Rapporto d'Intervento deve essere fornito da colui che ha effettuato l'intervento stesso in duplice copia: una copia deve essere consegnata al dipendente di Poste Italiane che firma il rapporto.</td></tr>
<tr><td>EW_REQ_51.</td><td>Manutenzione correttiva: tempi di risposta
Sarà compito del Referente di Poste Italiane comunicare all'Impresa il malfunzionamento ed assegnare all'anomalia la classe di gravità, utilizzando la casistica illustrata nella tabella seguente.
<table>
<tr><th>Categoria</th><th>Descrizione</th></tr>
<tr><td>Bloccante</td><td>Si tratta di un difetto o anomalia che impedisce l' uso dell'applicazione o di una o più funzionalità importanti.</td></tr>
<tr><td>Non Bloccante</td><td>Malfunzionamenti per cui non è impedito l'uso delle funzioni.</td></tr>
</table>
La risposta alle segnalazioni di anomalie deve avvenire entro 2 ore solari in orario lavorativo (lun-ven 8,30-18,30) dalla segnalazione stessa.
L'Impresa dovrà garantire un livello di intervento in funzione della categoria di malfunzionamento, così definita.
Per "impedimento all'uso dell'applicazione o delle sue funzioni" si intende una malfunzione vera e propria dell'applicazione o gli effetti che tale malfunzione ha causato alla base dati.
In relazione alla tipologia di anomalia rilevata, i tempi di ripristino e</td></tr>
</table>

<table>
<tr><th>Codice Requisito</th><th>Descrizione Requisito</th></tr>
<tr><td></td><td>risoluzione sono riportati nella tabella al requisito successivo e sono validi sia per anomalie hardware che software.
Per Ripristino si intende la disponibilità alla messa in produzione dei componenti del sistema interessati dall' anomalia, tramite una soluzione Quick-Fix.
Per Risoluzione si intende la disponibilità alla messa in produzione dei componenti del sistema interessati dall' anomalia con la completa risoluzione dell' anomalia stessa.
L'intervento deve concludersi con il perfetto funzionamento della soluzione realizzata.
Il tempo di decorrenza viene misurato a partire dalla data ed ora di segnalazione, formalizzata per iscritto.</td></tr>
<tr><td>EW_REQ_52.</td><td>Manutenzione correttiva: tempi di ripristino e risoluzione
I tempi massimi di ripristino del servizio e di risoluzione delle anomalie sono dettagliati nella tabella seguente in giornate lavorative (gg/lav.).
<table>
<tr><th></th><th></th><th>Tempi massimi dalla segnalazione anomalia</th></tr>
<tr><td rowspan="2">Anomalie Bloccanti</td><td>Ripristino</td><td>2 gg/lav.</td></tr>
<tr><td>Risoluzione</td><td>3 gg/lav.</td></tr>
<tr><td rowspan="2">Anomalie Non Bloccanti</td><td>Ripristino</td><td>3 gg/lav.</td></tr>
<tr><td>Risoluzione</td><td>4 gg/lav.</td></tr>
</table></td></tr>
</table>

5. Modalità di partecipazione e criteri di aggiudicazione

5.1. Relazione tecnica

L'Impresa dovrà presentare una *Relazione Tecnica* composta da:

- una proposta di dettaglio della propria soluzione (componenti software offerti e relative illustrazioni funzionali, compresi oggetti software di terze parti essenziali per il funzionamento della soluzione, configurazione minimale della infrastruttura hardware ospitante, performance, affidabilità della soluzione, scalabilità della stessa, etc.), specificando anche le eventuali referenze di analoghe realizzazioni eseguite.
- una dichiarazione dell'impresa in cui sia indicata la conformità dell'offerta a quanto richiesto nei requisiti minimi espressi nel Capitolo 4 del presente documento;

- la Scheda Requisiti minimi redatta come indicato nel paragrafo 5.2 del presente documento;

5.2. Scheda Requisiti minimi

L'Impresa deve compilare la Scheda Requisiti minimi sulla base dei requisiti riportati nel capitolo 4 del presente documento (Requisiti minimi obbligatori della fornitura).

Nella colonna "Riferimento documenti" dovranno essere inseriti i documenti, il paragrafo e la pagina della relazione tecnica, da cui si evince che il requisito viene soddisfatto.

Caratteristica richiesta	Riferimento documenti
EW_REQ_1.	
EW_REQ_2.	
EW_REQ_3.	
.....	
EW_REQ_n.	

5.3. Criterio di aggiudicazione

L'aggiudicazione avverrà, secondo la disciplina del D.Lgs. 163/06 e successive modifiche ed integrazioni, mediante procedura negoziata e con l'applicazione del criterio del prezzo più basso.