Progressivo Domande	Documento	Riferimento	Quesito	Risposta
1	Capitolato Tecnico	EW_REQ_7	Cosa è il sistema CERT? Cosa si intende per migrazione verso ambiente CERT (CAGE)?	Il CERT (*Computer Emergency Response Team)* è un progetto volto alla gestione centralizzata degli eventi informatici. La migrazione prevede lo spostamento della piattaforma attuale, comprensiva delle basi dati, nell'ambiente Hardware adibito al CERT, definito "CAGE".
2	Capitolato Tecnico	EW_REQ_9	Per "Gestione" si intende "visualizzazione"?	Per "Gestione" si intende la possibilità di poter creare e modificare delle technology list in base agli asset gestiti da coloro che sono profilati all'accesso. (Più tecnology list per più utilizzatori)
3	Capitolato Tecnico	EW_REQ_12	Chi provvede ad inserire il "grado di affidabilità"? Su quale base viene imputato?	Il "grado di affidabilità", valutato sulla base del modello 4x4, verrà inserito dall'operatore.
4	Capitolato Tecnico	EW_REQ_13	Quante dovrebbero essere le fonti dati da normalizzare? Di che tipologia sono? (su che format vengono traspostate: DB, CSV, etc..)	Le fonti dati da normalizzare sono attualmente 2, con la possibilità di aggiungere ulteriori fonti dati aperte. I formati sono DB,RSS,CSV
5	Capitolato Tecnico	EW_REQ_14	Quante dovrebbero essere le fonti dati da normalizzare? Di che tipologia sono? (su che format vengono traspostate: DB, CSV, etc..)	Dovranno essere aggiunte e normalizzate informazioni recuperate da social network come Twitter e Facebook, quindi il formato sarà quello previsto dalle API (JSON,CSV,XML) e l'integrazione di dati provenienti da Black Market (HTML)
6	Capitolato Tecnico	EW_REQ_16	L'applicativo dovrà avere un meccanismo di backup custom? Non potrà quindi essere inserito all'interno delle procedure standard per il backup di dati lato DB e application servers?	Il backup può essere inserito all'interno di procedure standard.
7	Capitolato Tecnico	EW_REQ_17	Le informazioni raccolte all'interno del repository sono prettamente record di DB oppure un parco documentale composto ad esempio da pdf?	Le informazioni interne al Repository possono essere record DB o file strutturati come excel/xml
8	Capitolato Tecnico	EW_REQ_21	Il Sistema deve prevedere l'integrazione con qualche Sistema di Gestione centralizzata log delle attività utente? Devono essere sottoposti a monitoring centralizzato dei Sistemi? Quanti? Di che tipologia?	La soluzione deve consentire la creazione di regole per il filtraggio e la visualizzazione di eventi in base a technology list o altri criteri. Non è previsto monitoring o integrazione con log delle attività degli utenti da parte di altre strutture.
9	Capitolato Tecnico	EW_REQ_22	Si intende un Sistema proattivito di monitoring e correlazione eventi? Su quali regole dovrebbero essere correlative gli eventi?	Deve essere possibile esportare, nei formati indicati, i dati filtrati dall'utente.
10	Capitolato Tecnico	EW_REQ_24	Quale tipologia di "cambi" deve essere tracciata? Cambi a cosa?	Dovranno essere tracciati i cambiamenti/evoluzioni di una determinata minaccia, per avere la possibilità di ricavarne lo storico e gli aggiornamenti.
11	Capitolato Tecnico	EW_REQ_28	Chi provvede all'identificazione di un attacco avvenuto in una honeypot? Ci sono degli operatori interni in grado di identificare attacchi, capirne le caratteristiche e quindi stilare un rapporto tecnico da inserire nel repository? I tracciati firewall non identificano obbligatoriamente traffico malevolo, su quali basi il Sistema dovrebbe identificare quello sospetto? Oppure si intende in tale punto l'integrazione con il Sistema DeepSight di Symantec (che descrive esattamente le caratteristiche esposte in EW_REQ__28)?	L'identificazione di un attacco avvenuto in una honeypot può essere tracciato sia da informazioni ricevute direttamente da Symantec ed altri servizi esterni, sia da eventi gestiti internamente da altre strutture da cui potremmo prelevare un dato filtrato.
12	Capitolato Tecnico	EW_REQ_29	Con quale criterio la soluzione dovrebbe essere in grado di applicare un livello di affidabilità? Cosa si intende per numero di segnalazioni? 0day da fonti non ufficali?	Le fonti dati, il cui grado di affidabilità verrà inserito da un operatore in base ad un modello 4x4, potranno essere fonti non ufficiali o ufficiali, che contengono riferimenti riguardo alla vulnerabilità.
13	Capitolato Tecnico	EW_REQ_35	Si intendono App Native? Per quali piattaforme? (Android, iOS, Windows, Balck Berry?) a quale utenza sarebbero rivolte, quella di back-office, quella esterna oppure entrambe?) che funzioni dovrebbero avere?	Per App si intendono Mobile Applications da sviluppare al fine di essere utilizzate tramite sistemi operativi Android, IOS, Windows e BlackBerry che consentano l'accesso ai servizi della piattaforma al personale di Poste Italiane preposto, tramite device.
14	Capitolato Tecnico	EW_REQ_44	Per destinatari in questo contest si intendono utenze esterne Poste Italiane? Ci sono implicazioni di licensing legate al ricorso a strumenti di reporting tipo Microsoft Reporting Services?	I destinatari del report possono essere sia interni che esterni a Poste Italiane. La struttura non ha a disposizione licenze di Microsoft Reporting Services.
15	Capitolato Tecnico	N.A.	L'attuale soluzione presente con che tecnologie è stata implementata e sviluppata? (Java, .Net, Sharepoint, WebSphere,IIS, MS SQL, Oracle, etc..)	L'attuale soluzione è stata sviluppata con tecnologia .NET
16	Capitolato Tecnico	N.A.	La soluzione prevista deve essere un'estensione a livello di codici sorgente all'attuale oppure solo funzionale?	La soluzione può essere rivista anche a livello di codice sorgente, per l'applicazione delle funzionalità richieste.
17	Capitolato Tecnico	N.A.	Facendo riferimento al requisito EW_REQ_52 del capitolato tecnico all.1 dove viene indicata come necessaria la certificazione ITIL3 per il profilo professionale Master, si richiede se è necessario averla al momento della partecipazione in gara o se è sufficiente dimostrarla entro i 25 giorni naturali per la costituzione del team, così come indicato nel requisito EW_REQ_55. Questo tenuto conto che sempre nel requisito EW_REQ_55 viene indicato come tempo massimo di consolidamento del team 45 gg naturali, tempo nel quale l'impresa partecipante può sostituire le proprie risorse qualora risultassero non rispondenti o non adeguate.	La certificazione ITIL3 per il profilo professionale Master è necessario averla al momento della partecipazione in gara.