

Acquisizione della soluzione tecnologica per la "Gestione delle vulnerabilità (Vulnerability Management) dei sistemi informativi e relativi servizi connessi".

Codice CIG: 8003275F72
6.2-2019-249

Commissione tecnica
per la valutazione delle offerte ammesse

Verbale di valutazione

Luca Galassi FF LF

Il giorno 20 gennaio 2020 alle ore 09:15, presso la sede di Trentino Digitale Spa, in Trento, Via Pedrotti n. 18, si è riunita la Commissione tecnica in prima seduta per esaminare le offerte ammesse in relazione alla "Richiesta di offerta, in unico lotto, per l'acquisizione di una soluzione tecnologica per la gestione delle vulnerabilità (Vulnerability Management) dei sistemi informativi e relativi servizi connessi, mediante procedura di gara - Codice CIG: 8003275F72" - indetta da Trentino Digitale Spa.

La Commissione, definita con atto interno di nomina della commissione di gara a firma del Presidente di Trentino Digitale Spa (dott. Roberto Soj) e di repertorio nr. 1 di data 13/01/2020 è composta da:

PRESIDENTE:

Lorenzo Grosselli - (Direzione Tecnica – U.O. SOC Cybersecurity)

COMPONENTI ESPERTI:

Laura Galvagni- (Direzione Tecnica – U.O. SOC Cybersecurity)

Francesco Telch (Direzione Tecnica - U.O. SOC Cybersecurity)

Svolge la funzione di segretario verbalizzante il Presidente, il quale dichiara di aver ricevuto la documentazione di gara dall'ufficio Approvvigionamenti della Direzione Acquisti di Trentino Digitale Spa nella persona della dott.ssa Chiara Parolin.

La commissione rileva la presenza di un'unica offerta da parte dell'azienda ALFA SYSTEM SPA.

Il Presidente ricorda ai membri della commissione l'obbligo di mantenere la segretezza in merito alle operazioni di valutazione ed ai contenuti dei documenti esaminati nonché l'importanza di effettuare valutazioni oggettive ed assolute.

La commissione tecnica verifica che i documenti relativi all'offerta pervenuta sono i seguenti (in formato digitale):

- Trentino Allegato_Relazione tecnica v0.2
- DataSheet-Tenable.sc_Continuous_View
- Tenable_SCCV_Activation_Air-Gapped_Environment
- Tenable.sc Statement of Qualifications

Prima di dare lettura del contenuto dell'offerta oggetto di giudizio, la Commissione procede alla disamina degli atti di gara e, in particolare, dei documenti "Richiesta di offerta" e "Capitolato Tecnico".

La Commissione avvia la disamina del documento "Trentino Allegato_Relazione tecnica v0.2" relativo all'offerta dell'azienda ALFA SYSTEM SPA al fine di assegnare i punteggi secondo lo schema definito nei documenti di gara. Gli altri documenti non saranno oggetto di valutazione, in quanto non richiesti negli atti di gara.

Alle ore 12:00 la Commissione sospende le operazioni di valutazione e decide di riprendere le attività alle ore 13:40.

La commissione riprende le attività all'ora concordata e prosegue nella valutazione e relativa assegnazione dei punteggi riferiti a "criteri" e "sub-criteri" secondo le dichiarazioni dell'azienda ALFA



SYSTEM SPA presenti nella "Relazione Tecnica".

In seguito a puntuale valutazione la commissione procede ad attribuire i coefficienti per singolo criterio e sub-criterio.

In allegato al presente verbale la tabella di dettaglio.

In seguito al procedimento di riparametrazione, si constata che l'offerente ha superato positivamente le soglie tecniche definite conseguendo un punteggio complessivo di 69,50 su 70 punti.

Alle ore 16:00 la Commissione chiude le operazioni di valutazione e consegna i verbali della seduta al Delegato della Società per la prosecuzione delle attività.

Il Presidente dà atto che il presente verbale, scritto con mezzo informatico, è fedele all'andamento della seduta.

Letto, confermato e sottoscritto.

I membri della Commissione:

Lorenzo Grosselli , Presidente nonché segretario verbalizzante;

Laura Galvagni;

Francesco Telch.



n°	criteri/elementi	n.	sub-criteri/elementi di valutazione	Giudizio sintetico	punti D max	punti Q max	punti T max	Coeff. Attribuito	Sub-criterio riparametrato	Punteggio complessivo Criterio
1	Requisiti generali di sistema	1.1.	La soluzione garantisce un processo di aggiornamento offline per poter effettuare l'adeguamento dei sistemi interni attraverso reti "air gapped"	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	8
		1.2	La soluzione proposta include funzionalità di scanning sia attivo che passivo, anche attraverso il monitoraggio del traffico, per avere un quadro completo delle vulnerabilità	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	3			1,00	3	
		1.3	La soluzione proposta è in grado di operare sia in modalità agent-based che agentless	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	2			1,00	2	
		1.4	La soluzione proposta garantisce la registrazione degli eventi in real time	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
		1.5	La soluzione proposta può inoltrare i log raccolti ad una fonte esterna ovvero poterli mettere a disposizione in un formato intellegibile	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			0,90	1	
2	Requisiti architetturali	2.1	La soluzione proposta garantisce un repository centralizzato per la raccolta e la gestione delle informazioni su 2048 host situati su più reti locali comunicanti tra di loro ma non necessariamente connesse ad Internet	Requisito tecnico presente nella soluzione proposta			1	1,00	1	10
		2.2	La soluzione proposta garantisce la conservazione delle informazioni raccolte per un determinato, e configurabile dalla committente. Trascorso tale periodo tali informazioni devono essere cancellate in maniera automatica senza intervento esterno.	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	3			1,00	3	
		2.3	La soluzione proposta permette la gestione di motori multipli per la scansione, distribuiti su rete geografica, da una console centralizzata	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
		2.4	La soluzione supporta la possibilità di effettuare la scansione delle reti periferiche utilizzando motori di scansione locali	Requisito tecnico presente nella soluzione proposta			2	1,00	2	
		2.5	La soluzione proposta garantisce che possano essere aggiunti dei motori di scansione senza costi aggiuntivi per l'aggiudicataria	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	2			1,00	2	
		2.6	La soluzione proposta include delle funzionalità per la gestione del flusso di informazioni generato dalla attività di scanning per evitare volumi di traffico tali da impedire il normale funzionamento dell'infrastruttura della committente	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
3	Rilevazione degli asset e scanning delle vulnerabilità	3.1	La soluzione garantisce un repository centralizzato per la raccolta e la gestione delle informazioni su 2048 host situati su più reti locali comunicanti tra di loro ma non necessariamente connesse ad Internet	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	2			1,00	2	18,5
		3.2	La soluzione proposta garantisce la possibilità di rilevare gli asset di interesse sia in maniera attiva (active scanning) sia in modalità passiva analizzando il traffico di rete	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
		3.3	La soluzione proposta garantisce nativamente tanto il discovery dei servizi standard quanto di quelli non standard o configurati per non trasmettere alcun tipo di banner durante la connessione	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
		3.4	La soluzione proposta supporta una shell sicura (ssh) con la capacità di effettuare una privilege escalation durante le attività di scan e audit delle configurazioni sui sistemi Unix	Requisito tecnico presente nella soluzione proposta			1	1,00	1	

Handwritten signatures and initials:
 - Top right: A large stylized signature.
 - Middle right: A signature that appears to read "Santo Polignani".
 - Bottom right: A signature that appears to read "Francesco".

	3.5	La soluzione proposta è in grado di performare l'auditing del livello di patch per i sistemi operativi Microsoft e i principali Unix in circolazione al momento di pubblicazione della gara	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.6	La soluzione proposta è in grado di performare l'auditing del livello di patch sugli apparati di rete dei principali vendor	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.7	La soluzione proposta è in grado di performare l'auditing del livello di patch delle principali piattaforme applicative in commercio quali, ad esempio, Java e Adobe	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.8	La soluzione proposta fornisce informazioni qualitative sul livello di pericolosità delle vulnerabilità tramite un sistema di classificazione	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
	3.9	La soluzione proposta fornisce informazioni sulle modalità di sfruttamento delle vulnerabilità	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1,5			1,00	1,5	
	3.10	La soluzione proposta traccia il ciclo di vita di ogni vulnerabilità sia all'interno di un singolo host che all'interno di tutta l'infrastruttura monitorata	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.11	La soluzione proposta supporta l'auditing dei server virtuali VMware	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.12	La soluzione proposta garantisce la possibilità di creare dei gruppi di asset dinamici con etichette definite dalla committente	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
	3.13	La soluzione proposta garantisce la pianificazione delle attività di scanning	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.14	La soluzione proposta permette una selezione granulare dei controlli da effettuare in modo da poter escludere eventuali attività anche solo potenzialmente pericolose per i sistemi	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.15	La soluzione proposta è in grado di recepire gli obiettivi delle attività di scanning in modalità diverse quali, ad esempio, nomi DNS, singoli IP, range di IP, classi di IP o liste predefinite	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.16	La soluzione proposta permette la configurazione di più tenant al suo interno garantendo di poter assegnare un range di indirizzi definito per ognuno di loro	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	3.17	La soluzione proposta permette di poter definire ruoli di amministrazione tanto verticali (singolo tenant) quanto trasversali (più tenant)	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
4		Funzionalità di compliance e Auditing							
	4.1	La soluzione proposta garantisce l'attività di compliance auditing tanto in modalità agent-based quanto agent-less senza che vi sia necessariamente un agent installato sull'host oggetto della verifica	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	8
	4.2	La soluzione proposta mette a disposizione degli operatori una visione complessiva e consolidata dei risultati delle attività di vulnerability assessment e audit compliance	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	4.3	La soluzione proposta fornisce un confronto del livello di adeguatezza dei sistemi verificati rispetto alle best practice dei principali vendor	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
	4.4	La soluzione proposta garantisce l'auditing delle misure di sicurezza e delle configurazioni dei sistemi VMWare, Microsoft e delle maggiori distribuzioni Unix	Requisito tecnico presente nella soluzione proposta			1	1,00	1	

Handwritten signatures and initials:
 - Top right: A large, stylized signature.
 - Middle right: A signature that appears to read "Luis Polig".
 - Bottom right: A circular stamp or signature.

	4.5	La soluzione proposta deve garantire l'auditing delle misure di sicurezza e delle configurazioni di database, applicazioni e apparati di rete	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	4.6	La soluzione proposta è dotata di una library regole preconfezionate per le attività di compliance e auditing	Requisito tecnico presente nella soluzione proposta			1,5	1,00	1,5	
	4.7	La soluzione proposta consente la personalizzazione delle regole di audit preconfezionate secondo le necessità della committente	Requisito tecnico presente nella soluzione proposta	1,5			1,00	1,5	
5 Operatività della piattaforma	5.1	La soluzione proposta presenta i risultati delle attività di scansione in viste generali che permettono di filtrare i contenuti, indagare su ogni singolo evento ed elaborare i dati raccolti	Requisito tecnico presente nella soluzione proposta	1,5			1,00	1,5	4,5
	5.2	La soluzione proposta garantisce che le attività di scanning, reporting e alerting possano essere completamente automatizzate	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	5.3	La soluzione proposta possiede avere viste separate per le vulnerabilità attive e quelle già mitigate garantendo la transizione automatica tra una vista e l'altra	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1			1,00	1	
	5.4	La soluzione prioritizza le attività di remediation secondo la loro criticità e raccoglierle in una vista dedicata	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
6 Console e reportistica	6.1	La console della soluzione proposta è configurabile secondo le necessità della committente. Deve essere possibile organizzare le vista tanto in modalità grafica quanto con elenchi personalizzati basati sulle categorie degli asset, sul check delle vulnerabilità o sul compliance audit, su base temporale, su chiavi di ricerca, IP address, etc.	Requisito della soluzione presente. Alcune modalità di organizzazione delle viste non sono direttamente disponibili.	1			0,67	1	9
	6.2	La soluzione proposta permette la creazione di grafici che permettano di visualizzare diversi trend risultanti dalle attività di scanning in un'unica immagine	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	6.3	La soluzione proposta permette di configurare l'intervallo di aggiornamento della console	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	6.4	La soluzione proposta permette di esportare e importare eventuali template di configurazione della console	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	6.5	La soluzione proposta permette la generazione di report personalizzati anche non basati sui template disponibili	Requisito tecnico presente nella soluzione proposta			2	1,00	2	
	6.6	La soluzione proposta permette la possibilità di inserire immagini custom nei report personalizzati	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
	6.7	La soluzione ha le funzionalità necessarie per generare la reportistica almeno nei formati più diffusi quali: PDF, CSV, XML, HTML, RTF and TXT. Tali report devono poter essere inviati in maniera automatica	Requisito della soluzione presente. Alcuni formati di reportistica non sono direttamente disponibili.	1			0,76	1	
	6.8	La soluzione garantisce di poter inserire nei rapporti tanto gli IP quanto i nomi (DNS o NetBISO) degli asset	Requisito tecnico presente nella soluzione proposta			1	1,00	1	
7 Gestione degli accessi	7.1	La soluzione proposta garantisce l'autenticazione degli utenti tramite sistemi LDAP esterni	Requisito tecnico presente nella soluzione proposta			2	1,00	2	9,5

LG

Antonio Polignone

[Handwritten signature]

	7.2	La soluzione proposta fornisce un sistema di gestione degli accessi basato su un modello "role-based" che garantisca una granularità sufficiente a permettere di discriminare gli accessi degli utenti a determinati data set e funzionalità	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	2			1,00	2	
	7.3	Gli amministratori della soluzione proposta possono configurare specifiche politiche di accesso ed assegnarle a ruoli esistenti ovvero poter creare nuovi ruoli.	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	2			1,00	2	
	7.4	Gli amministratori della soluzione proposta possono limitare l'accesso, a livello di ruolo o di singolo utente, ad asset specifici, regole di scansione o archivi delle vulnerabilità rilevate	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	2			1,00	2	
	7.5	La soluzione proposta effettua un audit dettagliato dell'attività degli utenti	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	1,5			1,00	1,5	
8		Caratteristiche migliorative della soluzione di VM							
	8.1	La soluzione proposta è in grado di tracciare diverse associazioni da parte del DHCP associando i risultati delle scansioni agli hostname	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	0,5			1,00	0,5	2
	8.2	La soluzione blocca automaticamente uno scan, se questo è ancora in corso durante gli orari in cui non è permesso, e lo riprende nel momento in cui la fascia oraria lo consenta	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	0,5			1,00	0,5	
	8.3	La soluzione proposta permette di escludere dalle attività di scanning categorie di device quali, ad esempio, le stampanti	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	0,5			1,00	0,5	
	8.4	La soluzione integra una soluzione di ticketing in grado di aprire/inoltare ticket su altre piattaforme	Requisito della soluzione presente/sviluppato con descrizione pienamente esaustiva	0,5			1,00	0,5	
	8.5	La soluzione è in grado di assegnare automaticamente un ticket ad una persona in base a regole definite	Dalla descrizione del fornitore e da verifiche tecniche sulla documentazione pubblica del prodotto l'assegnazione automatica verso specifici utenti non è presente, mentre è presente l'assegnazione automatica a specifici gruppi.	0,5			0,00	0	
		TOTALE PUNTI		38,5	0	31,5			69,5

UG

Marco Spagnoli