PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT

LOTTO 2

COMUNE DI BORGOMANERO

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	29/03/2023
2.0	Seconda emissione	12/04/2023

Indice

1. INTRODUZIONE

1.1 PREMESSA

Il presente documento descrive il Piano Operativo TIM, relativamente alla richiesta di fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-apt per il Cliente Comune di BORGOMANERO, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (identificato dal codice: 8107652 – Richiesta Piano Operativo/Ordine).
Con questo progetto il Comune di Borgomanero intende acquisire:

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- Endpoint Protection Platform & Endpoint Detection & Response
- Servizi di Manutenzione
- Servizi Professionali

1.2 SCOPO

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro ed in risposta al Piano dei Fabbisogni inviato dal cliente.

1.3 RIFERIMENTI

Identificativo
Piano dei Fabbisogni – Comune di Borgomanero – Richiesta Piano Operativo/Ordine 8107652
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

1.4 ACRONIMI E GLOSSARIO

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa

2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- ✓ **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**

  Nome Cognome: Massimiliano Materazzi
  e-mail: massimiliano.materazzi@telecomitalia.it

che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- ✓ **Responsabile del Fornitore** (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale).
  Nome Cognome: Elena Di Prima
  telefono/cellulare:335 6331216
  e-mail: elena.diprima@telecomitalia.it

che riferirà, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo

- ✓ **Referente Tecnico per l'erogazione dei servizi**

  Nome Cognome: Antonio Dell'Erba
  telefono/cellulare:3316002172
  e-mail: antonio.dellerba@telecomitalia.it

che dovranno garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5).

2.1 CATEGORIZZAZIONE DEGLI INTERVENTI

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

Ambito (layer)	Obiettivi Piano Triennale
□ Servizi	□ Servizi al cittadino
	□ Servizi a imprese e professionisti
	x Servizi interni alla propria PA
	□ Servizi verso altre PA
□ Dati	□ Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	□ Aumentare la qualità dei dati e dei metadati
	□ Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
□ Piattaforme	□ Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	□ Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	□ Incrementare e razionalizzare il numero di piattaforme per le amministrazioni
□ Infrastrutture	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	□ Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

	infrastrutture interne verso il paradigma cloud)
	□ Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
□ Interoperabilità	□ Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	□ Adottare API conformi al Modello di Interoperabilità
□ Sicurezza Informatica	x Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	□ Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

3. PROGETTO DI ATTUAZIONE

Il progetto di attuazione prevede la fornitura di quanto indicato nella tabella seguente, in cui viene indicato l'importo contrattuale complessivo; in ciascuna voce oggetto di quotazione economica si indicano il dettaglio dei prodotti e dei servizi oggetto del contratto esecutivo, anche in base alle indicazioni riportate nei rispettivi paragrafi relativi ai prodotti e ai servizi previsti.

Tipologia Prodotto	Codice Articolo	Descrizione Articolo	Produttore	Quantità	Prezzo Totale
Fornitura	GZ ULTRA - GOV 2 Y - C - F1	BUNDLE GRAVITY ZONE	BITDEFENDER	140	1.985,20 €
Servizi	JSAN-STA	Junior Security Analyst - fascia standard	DINETS	17	3.867,50 €
Servizi	SP-STA	Security Principal - fascia standard	BV_TECH	3	930,00 €
Servizi	SST-STA	Senior Security Tester - fascia standard	BV_TECH	7	1.911,00 €
Manutenzione 24 mesi	MANHP-EPP-F1-BIT	Manutenzione HP EPP in fornitura 24 mesi (24x7x4)	DINETS	140	168,00 €
Importo Complessivo					**€ 8.861,70**

La durata del Contratto Esecutivo è 24 mesi.

Relativamente ai prodotti in fornitura, questi sono è costituiti da:

- N. 140 Bundle Gravity Zone Bitdefender le cui caratteristiche specifiche e funzionali sono descritte nel capitolo dedicato.

4. PRODOTTI RICHIESTI

PRODOTTI	BRAND	FASCIA	MODELLO	CODICE ARTICOLO PRODUTTORE	N.
EPP-BIT F1	Bit Defender	1	BUNDLE GRAVITY ZONE	GZ ULTRA - GOV 2 Y - C - F1	140

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

5. PRODOTTI DELLA FORNITURA

Nel seguente paragrafo è riportata la descrizione tecnica dei prodotti forniti.

5.3 ENDPOINT PROTECTION PLATFORM & ENDPOINT DETECTION & RESPONSE

Una soluzione EPP/EDR consente di proteggere gli endpoint di tipo client da minacce quali virus, trojan, worm, etc, bloccando le attività di applicazioni che risultano potenzialmente dannose, fornendo inoltre funzionalità utili all'investigazione e al ripristino in seguito a violazioni di sicurezza. Nell'Accordo quadro sono previste quattro fasce dimensionali per il Vendor Bitdefender per il quale di seguito alleghiamo le specifiche tecniche della soluzione proposta.

Bitdefender EPPEDR.docx

7.SERVIZIO DI SUPPORTO SPECIALISTICO

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	**17**
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	**3**
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	
Senior Security Analyst - fascia straordinaria	SSAN-STR	SR_SEC_AN_STR	
Senior Security Architect - fascia standard	SSAR-STA	SR_SEC_ARCH_STD	
Senior Security Architect - fascia straordinaria	SSAR-STR	SR_SEC_ARCH_STR	
Senior Security Tester - fascia standard	SST-STA	SR_SEC_TEST_STD	**7**

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

Per le competenze che ciascuna risorsa specialistica deve possedere si rimanda a quanto previsto nell'allegato 2 – Capitolato Tecnico – Parte Speciale (paragrafo 3.2.4), e come di seguito riportate:

Junior Security Analyst: in possesso di almeno una delle seguenti certificazioni: EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst,

Security Principal: in possesso della certificazione ISACA CISM (Certified Information Security Manager)

Senior Security Architect: in possesso della certificazione (ISC)^2 CISSP (Certified Information System Security Professional)

Senior Security Analyst: in possesso di almeno una delle seguenti certificazioni:
EC-Council CSA (Certified SOC Analyst) e/o CompTIA CySA+ (Cyber Security Analyst) e/o GIAC Certified Intrusion Analyst

Il Cliente Comune di Borgomanero intende svolgere un servizio di VAPT attraverso l'impiego del servizio di supporto specialistico.

VAPT

Il servizio di Vulnerability Assessment Penetration Test, verso gli indirizzi IP esterni del Cliente, identificati in fase di kick-off del progetto viene dimensionato per 12 IP esterni.

L'analisi comprenderà, in modo non esclusivo, le seguenti attività:

- Enumerazione di tutti i sistemi Internet-facing presenti nel range di indirizzi IP condivisi dal Cliente;
- Per ogni sistema identificato, enumerazione dei servizi di rete esposti tramite l'impiego di tecniche avanzate di port scanning – l'analisi prevede l'identificazione di tutte le porte TCP e UDP (se presenti) esposte dai target oggetto di analisi;
- Fingerprinting di tipo e versione del sistema operativo dei sistemi e dei servizi esposti, e verifica della presenza di eventuali versioni obsolete e/o vulnerabili;
- Scansione automatica tramite vulnerability scanner professionali (e.g., Tenable Nessus) con l'obiettivo di identificare vulnerabilità note e configurazioni non sicure;
- Analisi dell'output dei vulnerability scanner e validazione delle vulnerabilità tramite analisi manuale e/o tramite l'impiego di strumenti di terze parti o sviluppati ad-hoc dai Security Engineer di BV TEH – obiettivo di tale analisi è l'eliminazione di eventuali falsi positivi e falsi negativi generati dagli strumenti automatici;
- Sfruttamento delle vulnerabilità, siano esse singole o concatenate tra loro, identificate durante le fasi preliminari (e.g., tramite moduli Metasploit e/o exploit custom o privati di BV TECH), in accordo con le regole di ingaggio e le esigenze del Cliente finale;
- Esecuzione di attività post-exploitation, tra le quali sono previste in modo non esclusivo azioni mirate all'elevazione dei privilegi, effettuare movimenti laterali verso altre macchine o componenti della rete (normalmente non raggiungibili), verificare la possibilità di esfiltrare dati, creare persistenza sulla rete target;

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- Raccolta di evidenze post-exploitation (e.g., dati estratti, screenshot, etc.) e sviluppo di eventuali Proof of Concept (PoC) exploit necessari per la riproduzione delle problematiche.

Eventuali applicazioni web esposte dai sistemi in perimetro non saranno oggetto di analisi. Tuttavia, qualora in fase di analisi venissero riscontrate ed enumerate tecnologie e versioni relative ai servizi web esposti, questi verranno normalmente processati.

Nota: BV TECH non effettuerà alcun attacco che potrebbe causare una condizione di Denial of Service (DoS), salvo diverse richieste del Cliente identificate in fase di kick-off del progetto.

Modalità Operativa: le attività saranno svolte da remoto, previa firma di apposito documento di liberatoria di autorizzazione.

Requisiti: il Cliente dovrà fornire a BV TECH un elenco esaustivo di indirizzi IP o subnet con indirizzamento pubblico che costituiranno il perimetro dell'attività, i quali andranno compilati nella liberatoria. Nel caso in cui il Cliente utilizzi sistemi di protezione perimetrale sull'infrastruttura target del penetration test (e.g., firewall, IPS/IDS), si richiede al Cliente l'inserimento in allow list degli IP pubblici di BV TECH per il solo periodo di esecuzione delle analisi, al fine di fornire un risultato completo nei tempi previsti per il progetto.

Durante le giornate uomo sopra indicate saranno svolte le attività di supporto specialistico in base alle esigenze del Comune di Borgomanero e comunque in funzione della fornitura prodotti richiesta tramite questo piano. Qualsiasi altra necessità sarà valutata di volta in volta in accordo con il cliente.

10. SERVZIO DI MANUTENZIONE

La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site.
Il servizio manutenzione prevede 2 profili di qualità, *Low Profile* (*Business Day*) o *High Profile* (*H24*),
Il servizio di manutenzione è offerto per annualità, quindi per 12 mesi o massimo 24 mesi.
Può essere fornita anche con un accesso remoto sicuro (utilizzando account VPN personali configurati e abilitati opportunamente, con tracciatura degli accessi per eventuali successivi audit, accessi che comunque dovranno essere limitati al tempo strettamente necessario all'esecuzione dell'attività, ad esempio mediante utenze token create all'occorrenza) a supporto delle stesse (ad. es. effettuazione di diagnosi attraverso i propri sistemi di gestione e di management per analisi di problematiche e malfunzionamenti segnalati dall'Amministrazione).

Le attività di manutenzione sono previste per i soli elementi di fornitura acquistati nell'ambito del presente AQ.
Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
- intervento presso la sede/luogo interessato

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati o verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Di seguito si riporta quanto richiesto dal cliente nel Piano dei fabbisogni:

Fascia	Codice servizio	Durata (mesi)
HP	CS2L2-MANHP-EPP-F1-BIT	24

11 PIANO DI LAVORO

La soluzione prevede la fornitura e l'installazione della soluzione Bitdefender EPP /EDR .

Le attività prevedono:

- Coordinamento iniziale e definizione delle strategie
- Attivazione console in cloud della soluzione in un'istanza dedicata del cloud Bitdefender.
- Creazione dei pacchetti di installazione dell'agent BEST (Bitdefender Endpoint Security Tool) e definizione delle policy.
- Installazione di un agente Bitdefender con ruolo di Relay
- Integrazione con Active Directory tramite almeno un paio di End Point Windows associati al dominio
- Distribuzione dell'agent di protezione / detection & response BEST (Bitdefender Endpoint Security Tool) su dispositivi server & client sulla base del numero di licenze acquisite; si tenga in considerazione che il numero di dispositivi (fisici e/o virtuali) con sistema operativo server deve essere uguale o inferiore al 35% del numero delle licenze totali acquisite.
- Definizione delle policy di sicurezza
- Associazione delle policy agli agenti installati in funzione delle esigenze
- Configurazione di un security server se richiesto

Inoltre, è prevista la fornitura di un servizio di un Vulnerability Assessment Penetration Test secondo quando riportato nel Capitolo 7.
Il servizio analizzerà, secondo i dettami riportati nel Capitolo 7, 12 IP esterni del Cliente.
Gli IP sopra citati saranno concordati in fase di kick-off del progetto con il Cliente.
Le analisi verranno condotte secondo le attività riportate puntualmente in elenco puntuale riportate nel Capitolo 7.
L'elaborazione del report conclusivo verrà condivisa al Cliente entro 14 giorni solari dalla data di termine delle attività operative indicate precedentemente.

11.1 GANTT

GANTT%20-%20Bitdefender.xlsx

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

11.2 PIANO DI PRESA IN CARICO

L'attività di presa in carico del sistema consiste nell'acquisire tutte le informazioni che sono necessarie all'erogazione dei servizi e di quanto indicato nel sopra riportato piano di lavoro, con l'obiettivo di acquisire know how relativo al contesto organizzativo, tecnologico e funzionale dell'Amministrazione oltre a standard, modalità operative, linee guida, ove presenti. Come specificato da piano dei fabbisogni l'amministrazione contraente fornirà la configurazione esistente degli apparati, l'accesso ai locali tecnici quando previsto, l'accesso da remoto agli apparati e tutto quanto necessario all'attivazione del servizio.

L'attività potrà consistere, ad esempio, in riunioni di lavoro, rilevazione delle configurazioni in essere sui vari sistemi, esame della documentazione esistente (es. schemi logici e di low level design dell'infrastruttura di rete, informative sulle connettività presenti, piani di indirizzamento etc) con assistenza di personale esperto e affiancamento condotta con eventuali ulteriori fornitori dell'amministrazione contraente.
Se previsto e/o richiesto dall'amministrazione contraente saranno altresì forniti i dettagli necessari (es. tools IT Management) alla corretta implementazione dei processi di Incident, Change e Deploy Management richiesta per l'espletamento dei servizi descritti nei successivi paragrafi.
Si noti che qualora la documentazione disponibile risultasse non aggiornata e/o incompleta, tutto ciò dovrà risultare in modo dettagliato in un verbale attestante il completamento del piano di presa in carico.

Durante le attività di Presa in carico si dovrà garantire:

- la presenza di tutte le figure coinvolte per l'erogazione dei servizi nonché dovranno essere reperibili e disponibili i Referenti Tecnici;
- la predisposizione di un verbale attestante il completamento della presa in carico da redigere secondo le indicazioni fornite dall'Amministrazione e che dovrà essere sottoscritto dal RTI e dall'Amministrazione.

11.3 SPECIFICHE DI COLLAUDO

Le schede di collaudo dei servizi/forniture previste saranno concordate con l'Amministrazione. Durante il collaudo di una soluzione Bitdefender GravityZone, è importante verificare diversi aspetti chiave per garantire che il sistema sia configurato correttamente e offra la protezione richiesta. Di seguito sono riportati i punti di collaudo per una soluzione Bitdefender GravityZone:

Installazione e configurazione: Verificare che l'installazione e la configurazione della soluzione Bitdefender GravityZone siano state eseguite correttamente e che tutti i componenti siano operativi.

Funzionalità di protezione antivirus e anti-malware: Testare l'efficacia delle funzionalità antivirus e anti-malware della soluzione per garantire la rilevazione e la rimozione tempestive di minacce note e sconosciute.

Protezione anti-ransomware: Verificare se la soluzione Bitdefender GravityZone è in grado di proteggere i sistemi da attacchi di ransomware, inclusa la capacità di rilevare e bloccare l'attività sospetta e di ripristinare rapidamente i file crittografati.

Gestione centralizzata: Testare la funzionalità di gestione centralizzata verificando il corretto

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

funzionamento della console.

Protezione delle postazioni di lavoro e dei server: Verificare se la soluzione Bitdefender GravityZone fornisce una protezione completa per le postazioni di lavoro e i server aziendali, inclusa la capacità di rilevare e rispondere alle minacce in tempo reale.

Aggiornamenti e patch: Verificare se la soluzione Bitdefender GravityZone e gli agent di sicurezza distribuiti sono aggiornati all'ultima release presente.

Integrazione con altre soluzioni di sicurezza: Se necessario, verificare se la soluzione Bitdefender GravityZone può integrarsi con altre soluzioni di sicurezza esistenti all'interno dell'infrastruttura IT aziendale.

Funzionalità di reporting e analisi: Testare le funzionalità di reporting e analisi della soluzione per consentire agli amministratori di monitorare e valutare l'efficacia della soluzione.

12. TABELLA RIEPILOGATIVA DEI SERVIZI E RELATIVI IMPORTI CONTRATTUALI

Codice articolo convenzione	Quantità	Durata (mesi)	Prezzo totale
CS2L2 – EPP-F1-BIT	140		1.985,20 €
CS2L2 - JSAN - STA	17		3.867,50 €
CS2L2 - SP-STA	3		930,00 €
CS2L2 - SST-STA	7		1.911,00 €
CS2L2 - MANHP-EPP-F1-BIT	140	24	168,00 €
		TOTALE	**8.861,70 €**

13. PRESTAZIONEI DI SUBAPPALTO

Nell'ambito dell'Accordo Quadro Cybersecurity 2 per le prestazioni erogate in subappalto è previsto quanto segue:

- Quota massima del subappalto: 50%
- Servizi per i quali è prevista la prestazione in subappalto:
    - Supporto Specialistico.

Nella tabella sottostante è necessario riportare la quota, le prestazioni e il nome delle aziende che erogheranno i servizi in subappalto, nel rispetto di quanto indicato nel Piano dei fabbisogni:

Servizi	Quota subappalto	Azienda del RTI che eroga il servizio	Nome dell'azienda che eroga la prestazione in subappalto
Supporto Specialistico	32,1 %	TIM	BV_Tech
Supporto Specialistico	43,6 %	TIM	Dinets

Gruppo TIM - Uso Interno - Tutti i diritti riservati.