ID AQ 2367

PIANO DEI FABBISOGNI SERVIZI

Spett.le
TELECOM ITALIA S.p.A.

La scrivente A.O. Ordine Mauriziano di Torino C.F. / P.IVA 09059340019 Codice IPA **asoom_to** con sede legale in Torino Prov. TO CAP 10128 Nazione IT Indirizzo Via Magellano 1 chiede che venga realizzato quanto di seguito indicato:

EDP/EPR (QUADRO A)
Servizio di Hardening (Quadro F)
Servizio di formazione (compilare il QUADRO G)
Servizio di manutenzione (compilare il QUADRO I)
Servizio di supporto specialistico (compilare il QUADRO H)

Invio delle fatture

Codice Univoco Ufficio:
CIG (quando disponibile)**: 9839401292**
NSO (quando disponibile)**: all'atto della firma del contratto**
CUP: G16G22000070005

Domicilio fattura:

Località Torino Prov. TO CAP 10128_ Nazione Italia
Indirizzo Via Magellano 1

Silvia Torrengo _____
E-mail **(obbligatoria)** storrengo@mauriziano.it_____

DATA TIMBRO E FIRMA DEL CLIENTE

Descrizione del Contesto di Riferimento in cui si riferisce la fornitura dell'Amministrazione

- La fornitura è riferita alla sostituzione e upgrade dell'attuale sistema antivirus aziendale With-Secure, in modo che siano comprese le funzionalità necessarie all'Azienda oggi non disponibili (L'attività andrà svolta sia sulle macchine con sistema operativo client, sia con quelli server)
- L'Amministrazione è inoltre interessata ad implementare funzionalità di EDR comprese in convenzione.
- Oltre alla fornitura di licenze l'amministrazione è interessata ai seguenti servizi:
  1) Supporto al deploy e alla migrazione iniziale;
  2) Formazione dei dipendenti che amministreranno la piattaforma;
  3) Servizi di manutenzione sul prodotto.

Macro Requisiti ed Obiettivi che l'Amministrazione si propone con la fornitura

Con la fornitura, l'amministrazione desidera:

- Sostituire l'attuale sistema antivirus With-Secure attualmente installato su PDL e server senza dare disservizi per l'utenza, per quanto possibile, potenziando le funzionalità di sicurezza oggi implementate;
- Integrare il prodotto nel workflow aziendale in modo da gestire le attuali configurazioni "custom" richieste dai fornitori\partner dell'azienda (esclusioni, regole, etc…);
- Preconfigurare il prodotto con un support specialistico in modo da evitare possibili disservizi, sia su OS "moderni", sia su OS "legacy" (secondo la tabella di compatibilità dichiarata dal produttore);
- Implementare durante il deploy del prodotto, con l'aiuto di un support specialistico, regole specifiche per le varie tipologie di dispositivi\VM da coprire (pdl, pdl legacy, server, server legacy, server linux, notebook);
- Configurare i relay per la distribuzione degli aggiornamenti;
- Implementare le politiche di scansione per non appesantire i client meno prestanti con apposite regole;
- Implementare un sistema di risk management per gli endpoint gestiti;
- Implementare funzionalità antimalware avanzate, in particolar modo sui server (sia con sistemi operativi microsoft, sia con sistemi operativi linux);
- Riuscire a monitorare gli IoC che ci vengono inviati su tutti i tipi di S.O.;
- Proteggere le VM su cloud, tenendo in considerazione che i server e i client potrebbero non accedere direttamente ad internet, se non tramite proxy o un server relay on prem;
- Attivare un servizio di manutenzione sul prodotto per la durata delle licenze.

Il contratto è interamente finanziato dal PNRR all'interno del progetto CUP G16G22000070005.

Tempistiche richieste per la realizzazione della fornitura, con descrizione di eventuali vincoli e/o criticità

l nuovo sistema EDP/EDR andrà messo in produzione entro il 31/12/2023 e il collaudo entro il 31/1/2024.

Indicazione del luogo di interesse della fornitura
A.O. Ordine Mauriziano
S.C. Sistemi Informativi
Via Magellano 1
10128 Torino (TO)

Durata del Contratto Esecutivo
24 mesi come da convenzione

Se il prodotto software è acquistato in sostituzione di un prodotto software già presente presso l'Amministrazione indicare il tipo di prodotto attualmente utilizzato e se è un prodotto SaaS o On premise. La migrazione di un prodotto che sia SaaS oppure On premise necessità di un supporto di servizi professionali.

La fornitura dovrà sostituire il nostro antivirus aziendale With-Secure con le funzionalità aggiuntive previste dal nuovo prodotto e che permettono di raggiungere un livello di sicurezza maggiore e di misurare il rischio di sicurezza degli endpoint.
Stesso agent su client e server con policy differenziate per O.S. o gruppo di endpoint opportunamente identificati.

Le installazioni di prodotti software richiedono la configurazione del software di management sia per la componente Client (EPP) che Server (SPP)
L'amministrazione metterà a disposizione ambienti virtuali on prem per l'installazione dei server di relay, mentre la console di management dovrà essere ospitata su cloud messo a disposizione dal produttore, che dovrà risultare qualificato QI1/QC1, secondo la classificazione prevista dall'Agenzia per la cybersicurezza nazionale (ACN).

QUADRO A - EDP/EPR

Descrizione del Servizio
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.

Per l'EPP/EDR sono previste quattro fasce dimensionali:
- EPP_EDR_1 (fascia 1): fino a 500 client
- EPP_EDR_2 (fascia 2): fino a 1000 client
- EPP_EDR_3 (fascia 3): fino a 5000 client
- EPP_EDR_4 (fascia 4): oltre 5000 client

Protection Platform & Endpoint Detection and Response				
Fascia di acquisizione	Codice Servizio	Brand	Codice Fornitore	Quantità (moduli)
EPP & EDR - Fascia 1	EPP-F1-CYN	CYNET	Cynet-360-EPP-EDR-C-F1	
	EPP-F1-TM	TRENDMICRO	OS01141-EPP-C-F1	
	EPP-F1-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F1	
	EPP-F1-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C - F1	
EPP & EDR - Fascia 2	EPP-F2-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F2	
	EPP-F2-TM	TRENDMICRO	OS01141-EPP-C-F2	
	EPP-F2-CYN	CYNET	Cynet-360-EPP-EDR-C-F2	
	EPP-F2-MCA	MCAFEE	MV6DEE-AA-BA+DLPECE-AT-BA-F2	
EPP & EDR - Fascia 3	EPP-F3-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F3	**1500**
	EPP-F3-TM	TRENDMICRO	OS01141-EPP-C-F3	
	EPP-F3-CYN	CYNET	Cynet-360-EPP-EDR-C-F3	
	EPP-F3-MCA	MCAFEE	MV6DEE-AA-DA+DLPECE-AT-DA-F3	
EPP & EDR - Fascia 4	EPP-F4-BIT	BITDEFENDER	GZ ULTRA - GOV 2 Y - C – F4	
	EPP-F4-TM	TRENDMICRO	OS01141-EPP-C-F4	
	EPP-F4-CYN	CYNET	Cynet-360-EPP-EDR-C-F4	
	EPP-F4-MCA	MCAFEE	MV6DEE-AA-EA+DLPECE-AT-EA-F4	

Il servizio di installazione e configurazione, come indicato nell'Accordo Quadro, è compreso nella fornitura ed il relativo costo incluso nei corrispettivi dei prodotti offerti.
E' compreso nella fornitura il servizio di Contact Center che dovrà essere reso disponibile alla data di attivazione dell'AQ. Il servizio dovrà essere accessibile mediante un "Numero Verde" (gratuito) per le comunicazioni telefoniche e deve comprendere le attività previste nella Guida all'Accordo Quadro.

QUADRO F - Servizio di Hardening

Descrizione del Servizio

Il servizio di hardening fornisce all'Amministrazione il supporto operativo necessario per rendere sicuri i client utilizzati. Le attività effettuate dovranno essere aderenti a quanto previsto dalle "*Linee guida per adeguare la sicurezza del software di base*" rilasciate da AgID.
Le specifiche attività che dovranno essere eseguite sono dipendenti dagli specifici software utilizzati sui client, ma in linea generale possono essere riassunte in:

- censimento ed eliminazione di programmi non necessari dalle postazioni utente. Potenzialmente ogni programma è una porta di accesso per soggetti non legittimati e dunque la loro diminuzione consente di limitare i rischi di intrusioni. Tutti i programmi che non sono stati autorizzati e controllati e che non sono strettamente utili all'esecuzione delle attività lavorative dovrebbero essere rimossi;

- supporto ai sistemisti nelle fasi di monitoraggio e controllo che il sistema operativo e i programmi leciti siano aggiornati alle ultime versioni e agli ultimi "*service pack*" disponibili;
- controllo che sui client siano abilitati i servizi autorizzati, ossia che non vi siano "*demoni*" in ascolto sulle porte di rete se non quelli strettamente necessari;
- verifica che gli utenti abbiano i corretti privilegi in relazione al loro ruolo e che appartengono ai corretti gruppi utenti;
- verifica della consistenza delle password richieste e della periodicità di cambio password richiesta agli utenti;
- supporto ai sistemisti PA nella definizione di gruppi di policy che potranno essere applicati agli utenti sulla base dei loro ruoli;
- verifica che gli eventi di sicurezza siano correttamente storicizzati (logging) ai fini del controllo e dell'audit;
- supporto al personale dell'Amministrazione nella distribuzione delle azioni correttive individuate (ad es. installazione di eventuali *patch* mancanti, realizzazione e installazione di fix temporanee, etc..) siano esse relative al sistema operativo che ai programmi utilizzati.

Il servizio dovrà essere effettuato sulle postazioni di tipo client e dovrà includere almeno i seguenti software:

- Sistemi operativi Windows Client;
- Sistemi operativi macOS;
- Sistemi operativi UNIX/Linux di tipo Client;
- Principali Web Browser (Edge, Explorer, Firefox, Chrome);
- principali applicativi software di produttività (Microsoft Office/LibreOffice, Pdf Readers, Thunderbird.

Servizio di Hardening			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Fase di assessment	ASS	HARD_ASSMNT	**1**
Fase di distribuzione degli interventi - 1001_5000	DISINT 1001-5000	HARD_DISTR_1001_5000	**3**
Fase di distribuzione degli interventi - 2_1000	DISINT 2-1000	HARD_DISTR_2_1000	
Fase di distribuzione degli interventi - 5001_	DISINT>5000	HARD_DISTR_5001_	
Fase di progettazione degli interventi	PRINT	HARD_PROG	**1**

QUADRO G - Servizio di Formazione

Descrizione del Servizio

Il servizio di formazione e affiancamento consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione Contraente che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'AQ, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software;
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale;
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti presso l'Amministrazione e le relative finalità;
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

È richiesto che tali attività formative siano erogate in moduli da massimo 16 ore e che per ogni modulo siano previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni indicativamente di 8 ore ciascuna:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste;
- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità *traning on the job*.

Formazione			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (moduli)
Modulo Formativo	FOR	FORMAZIONE	**1**

QUADRO H - Servizio di Supporto Specialistico

Descrizione del Servizio

Il servizio 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 riguarderda le attività riportate nel seguito:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

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

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa
d) il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito.

Tale servizio potrà essere acquistato dalle Amministrazioni Contraenti unicamente in maniera contestuale ai prodotti e avere durata massima pari a 24 mesi.
Il servizio potrà essere prestato secondo le seguenti modalità:
i. in fase iniziale - lett. a) del precedente elenco;

ii. in modalità "*spot*" - lett. b) e lett c) (limitatamente alla modalità "a chiamata") del precedente elenco

iii. con periodicità definita - lett. c) (limitatamente alla modalità "presidio") e d) del precedente elenco.

Servizio Supporto Specialistico			
Fascia di acquisizione	Codice Servizio	Codice Fornitore	Quantità (gg/uomo)
Junior Security Analyst - fascia standard	JSAN-STA	JR_SEC_AN_STD	**177**
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	**31**
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	**117**
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	**44**
Senior Security Tester - fascia straordinaria	SST-STR	SR_SEC_TEST_STR	

QUADRO I - Servizio di Manutenzione

Descrizione del Servizio

Il servizio di manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità.
La manutenzione, in base alla qualità del servizio richiesto per i servizi erogati, prevede due profili *Low Profile* (*Business Day*) o *High Profile* (*H24*) e potrà essere offerta per annualità, quindi per 12 mesi o massimo 24 mesi.
Le attività di manutenzione sono associate ai soli elementi di fornitura acquistati nell'ambito del presente AQ e potranno essere acquistate solo contestualmente alla fornitura.
La manutenzione deve comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site.
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:
  1. intervento presso la sede/luogo interessato;
  2. ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati;
  3. verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

Ogni intervento di manutenzione dovrà prevedere la redazione del relativo "*verbale di intervento*" e l'eventuale aggiornamento della documentazione di progetto.
Gli interventi dovranno concludersi con l'attività di verifica del corretto funzionamento del software oggetto della fornitura
Il servizio di manutenzione deve essere realizzato nel rispetto degli SLA previsti, anche con interventi da effettuarsi presso i siti dell'Azienda, pena l'applicazione delle penali indicate nell'Accordo Quadro.

Si ritiene di attivare il servizio in modalità LP per 24 mesi

Servizio di manutenzione		
Fascia di acquisizione	Codice Servizio	Quantità (mesi)
Manutenzione LP	MANLP-EPP-F1	
	MANLP-EPP-F2	
	MANLP-EPP-F3	24
	MANLP-EPP-F4	
	MANLP-NAC-F1	
	MANLP-NAC-F2	
	MANLP-NAC-F3	
	MANLP-NAC-F4	
	MANLP-NAC-F5	
	MANLP-NAC-F6	
	MANLP-NGFW-F1	
	MANLP-NGFW-F2	
	MANLP-NGFW-F3	
	MANLP-NGFW-F4	
	MANLP-NGFW-F5	
	MANLP-NGFW-F6	
	MANLP-Anti-APT-F1	
	MANLP-Anti-APT-F2	
	MANLP-SPP-F1	
	MANLP-SPP-F2	
	MANLP-SPP-F3	
	MANLP-SPP-F4	

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

LOTTO 2

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	15/06/2023
2.0	Recepite precisazioni Cliente	20/06/2023

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 Azienda Ospedaliera Ordine Mauriziano di Torino, in conformità alle richieste espresse dall'Amministrazione nel Piano dei Fabbisogni (richiesta Piano Operativo/Ordine 7284266).
Con questo progetto l'Ente intende acquisire:

- Endpoint Protection Platform & Endpoint Detection & Response

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 - Azienda Ospedaliera Ordine Mauriziano di Torino – Richiesta Piano Operativo/Ordine 7284266
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 2

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)**

  Massimiliano Materazzi
  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.

- ✓ **Responsabile del Fornitore** (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale).

  Cristina Moscato:
  335 5644666
  Cristina.moscato@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**

  Stefano Picerno:
  338 6728220
  Stefano.Picerno@telecomitalia.it

che dovrà 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 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

La soluzione prevede la fornitura e l'installazione della soluzione Bitdefender EPP /EDR e relativa assistenza tecnica per 24 mesi.

Le attività prevedono:

- 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 2 agent Bitdefender con ruolo di Relay
- Installazione di 2 Security Virtual Appliance per ottimizzare la scansione degli ambienti virtuali.
- 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.
- Associazione delle policy agli agenti installati in funzione delle esigenze.

4. PRODOTTI RICHIESTI

PRODOTTI	BRAND	FASCIA	MODELLO	CODICE ARTICOLO PRODUTTORE	N.
EPP & EDR	BITDEFENDER	3	BUNDLE GRAVITY ZONE	GZ ULTRA - GOV 2 Y - C – F3	1500

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.
In allegato è riportata la scheda illustrativa del prodotto Bit Defender richiesto dall'Amministrazione.

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 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.
Le giornate specialistiche saranno erogate per l'affiancamento all'Amministrazione sulla piattaforma di gestione degli incident e sull'analisi degli stessi per meglio definire le politiche di Remediation.
Il perimetro del supporto viene esteso alle licenze BitDefender già presenti nell'Amministrazione.
Qualsiasi altra necessità sarà valutata di volta in volta in accordo con l'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	**177**
Junior Security Analyst - fascia straordinaria	JSAN-STR	JR_SEC_AN_STR	
Security Principal - fascia standard	SP-STA	SEC_PRINC_STD	**31**
Security Principal - fascia straordinaria	SP-STR	SEC_PRINC_STR	
Senior Security Analyst - fascia standard	SSAN-STA	SR_SEC_AN_STD	**117**
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	**44**
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

8. SERVIZIO DI FORMAZIONE

Il servizio consente la fruizione di sessioni formative impartite presso le sedi dell'Amministrazione Contraente che permettano di istruire i discenti sulle specifiche tecnologie acquistate nell'AQ, e deve avere l'obiettivo di:

- istruire i discenti sulle principali minacce che i prodotti acquistati si prefiggono di contrastare;
- descrivere gli apparati installati in termini di caratteristiche, configurazione e funzionalità, con particolare enfasi sulle componenti software
- mettere il personale designato dall'Amministrazione Contraente in grado di provvedere alla gestione delle componenti installate in maniera autonoma ed ottimale
- descrivere le eventuali attività di integrazione effettuate con altri prodotti acquistati o con prodotti già presenti presso l'Amministrazione e le relative finalità
- realizzare demo e/o attività di test che consentano ai discenti di apprendere le principali funzionalità dei prodotti attraverso l'esperienza diretta.

Tali attività formative saranno erogate in moduli da massimo 16 ore e per ogni modulo sono previsti al massimo 10 discenti. Ogni modulo è composto da due sezioni indicativamente di 8 ore ciascuna:

- una sezione teorica, in cui sono descritti i sistemi interessati e le relative funzionalità previste
- una sezione pratica, in cui il personale dell'Amministrazione opererà attivamente sui sistemi, secondo una modalità traning on the job.

9. SERVIZIO DI HARDENING

Con tale servizio si vuole fornire all'Amministrazione il supporto operativo necessario per rendere sicuri i client utilizzati. Le attività effettuate dovranno essere aderenti a quanto previsto dalle "Linee guida per adeguare la sicurezza del software di base" rilasciate da AgID.
Le specifiche attività che dovranno essere eseguite sono dipendenti dagli specifici software utilizzati sui client, ma in linea generale possono essere riassunte in:

- eliminazione di programmi non necessari dalle postazioni utente. Potenzialmente ogni programma è una porta di accesso per soggetti non legittimati e dunque la loro diminuzione consente di limitare i rischi di intrusioni. Tutti i programmi che non sono stati autorizzati e controllati e che non sono strettamente utili all'esecuzione delle attività lavorative dovrebbero essere rimossi
- supporto ai sistemisti PA nelle fasi di monitoraggio e controllo che il sistema operativo e i programmi leciti siano aggiornati alle ultime versioni e agli ultimi "service pack" disponibili
- controllo che sui client siano abilitati i servizi autorizzati, ossia che non vi siano "demoni" in ascolto sulle porte di rete se non quelli strettamente necessari
- verifica che gli utenti abbiano i corretti privilegi in relazione al loro ruolo e che appartengono ai corretti gruppi utenti
- verifica della consistenza delle password richieste e della periodicità di cambio password richiesta agli utenti
- supporto ai sistemisti PA nella definizione di gruppi di policy che potranno essere

applicati agli utenti sulla base dei loro ruoli
- verifica che gli eventi di sicurezza siano correttamente storicizzati (logging) ai fini del controllo e dell'audit
- supporto al personale dell'Amministrazione nella distribuzione delle azioni correttive individuate (ad es. installazione di eventuali patch mancanti, realizzazione e installazione di fix temporanee, etc..) siano esse relative al sistema operativo che ai programmi utilizzati

Il servizio dovrà essere effettuato sulle postazioni di tipo client e dovrà includere almeno i seguenti software:
- Sistemi operativi Windows Client
- Sistemi operativi macOS
- Sistemi operativi UNIX/Linux di tipo Client
- Principali Web Browser (Edge, Explorer, Firefox, Chrome)
- Principali applicativi software di produttività (Microsoft Office/Libre Office, Pdf Readers, Thunderbird).

In particolare, dovranno essere dettagliate le scadenze per le attività e/o i deliverable previsti. Per gli elementi e la loro relativa numerosità si dovrà procedere come segue:
- dovranno essere identificati il numero di cluster omogenei di elementi, considerando che l'identificazione delle azioni correttive di un elemento appartenente ad un insieme omogeneo possono essere facilmente ripetute su tutti gli elementi del medesimo insieme anche per mezzo di strumenti di software distribution. Si pensi ad esempio al caso in cui le postazioni client dell'Amministrazione siano tutte derivate da una medesima "immagine" SW, presentando quindi le medesime caratteristiche in termini di pacchetti installati e relativa configurazione, tranne che per le specificità legate al singolo utente (ad es. login/passwd)
- dovranno essere identificate nel dettaglio le attività che dovranno essere effettuate nella realizzazione del servizio. Ad esempio, laddove l'Amministrazione abbia già tutte le informazioni relative allo stato della propria infrastruttura interessata dall'attività, la fase di assessment, potrà non essere effettuata
- dovranno essere identificati il numero di elementi appartenenti a ciascun cluster omogeneo
- dovrà essere calcolata, sulla base di tali elementi, la spesa del servizio in base al listino di fornitura.

10. SERVIZIO 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 è previsto in modalità Low Profile (Business Day).

Il servizio di manutenzione è offerto per 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 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
- 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.

11 PIANO DI LAVORO

11.1 GANTT

Cronoprogramma delle attività

Il nuovo sistema EDP/EDR andrà messo in produzione entro il 31/12/2023 e il collaudo entro il 31/01/2024**.**

11.2 PIANO DI PRESA IN CARICO

Le attività di presa in carico dovranno essere pianificate con l'Amministrazione.

Durante lo svolgimento di tali attività 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 presenza ed il mantenimento nel tempo delle percentuali di personale con le certificazioni e/o credenziali dichiarate in offerta tecnica valide e non scadute;
- 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.

NOTA BENE: l'attività di presa in carico dovrà essere completata entro il termine massimo di 50 gg solari dalla data di stipula del Contratto esecutivo. Se le attività di Presa in carico non sono eseguite nel rispetto dei tempi contrattualmente indicati, l'Amministrazione potrà richiedere l'applicazione della relativa penale (cfr. capitolato tecnico speciale).

11.3 SPECIFICHE DI COLLAUDO

Le schede di collaudo dei servizi/forniture previste saranno concordate con l'Amministrazione.

12. TABELLA RIEPILOGATIVA DEI SERVIZI E RELATIVI IMPORTI CONTRATTUALI

Codice Articolo Convenzione	Descrizione Articolo Convenzione	Produttore	Quantità	Durata	Unità di misura	Prezzo senza IVA	UT Totale	Canone Anno
CS2L2-EPP-F3-BIT	Fornitura in opera EPP-F3-BIT-GZ Business Enterprise - GOV 2 Y - C – F3	BITDEFENDER	1500		Pezzo	11,07	16605,00	
		TELECOMITALIA						
CS2L2-MANLP-EPP-F3-BIT	Manutenzione mensile LP EPP & EPR Fascia 3	TELECOMITALIA	1500	12	Pezzo/mese	0,03		585,00
CS2L2-MANLP-EPP-F3-BIT	Manutenzione mensile LP EPP & EPR Fascia 3	TELECOMITALIA	1500	12	Pezzo/mese	0,03		585,00
CS2L2-ASS	Servizio di Hardening su Client - Fase di assessment	TELECOMITALIA	1		Pezzo	900,00	900,00	
CS2L2-PRINT	Servizio di Hardening su Client - Fase di progettazione	TELECOMITALIA	1		Pezzo	900,00	900,00	
CS2L2-DISINT 1001-5000	Servizio di Hardening su Client - Fase di distribuzione degli interventi - 1001_5000	TELECOMITALIA	3		Pezzo	1000,00	3000,00	
CS2L2-JSAN-STA	Servizio di supporto specialistico - Junior Security Analyst - fascia standard	TELECOMITALIA	177		gg/uomo	227,50	40267,50	
CS2L2-SP-STA	Servizio di supporto specialistico - Security Principal - fascia standard	TELECOMITALIA	31		gg/uomo	310,00	9610,00	
CS2L2-SSAN-STA	Servizio di supporto specialistico - Senior Security Analyst - fascia standard	TELECOMITALIA	117		gg/uomo	271,00	31707,00	

CS2L2-SST-STA	Servizio di supporto specialistico - Senior Security Tester - fascia standard	TELECOMITALIA	44		gg/uomo	273,00	12012,00	
CS2L2-FOR	Modulo Formativo	TELECOMITALIA	1		modulo formativo	990,00	990,00	