Azienda Ospedaliera di Rilievo Nazionale
"Santobono Pausilipon"
Via Teresa Ravaschieri n.8 - 80122- Napoli
Partita Iva n. 06854100630

Capitolato Speciale di Appalto

PROCEDURA APERTA PER LA FORNITURA DI PRODOTTI (HARDWARE E LICENZE SOFTWARE) E RELATIVI SERVIZI DI INSTALLAZIONE PER IL POTENZIAMENTO DELL'INFRASTRUTTURA DI CYBERSECURITY DELL'AORN SANTOBONO PAUSILIPON.

Progetto Finanziato dal POR Campania FESR – 2014-2020

CUP: H66G23000140005
CIG: A014EACEE1

Sommario

1 Scopo del documento

Il presente Capitolato Tecnico disciplina gli aspetti tecnici connessi alla fornitura e potenziamento di una nuova infrastruttura di Cyber Security per l'Azienda Ospedaliera di rilievo nazionale Santobono-Pausilipon.

1.1 Definizioni ed Acronimi

Di seguito vengono evidenziati i termini utilizzati nel presente documento:

Acronimo	Descrizione
AORN	AORN Santobono Pausilipon
SIEM	Security Information Event Management
XDR	Extended Detection and Response
ISE	Identity Service Engine
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
SDN	Software Defined network
WAF	Web Application Firewalling
PA	Pubblica Amministrazione
IoT	Internet of Things
SLA	Service Level Agreements
VPN	Virtual Private Network
MFA	Multi Factor Authentication
AVC	Application and Visibility Control
FW	Firewall
SA	Stazione Appaltante
GUI	Graphical User Interface

Tabella 1 – Definizioni ed acronimi

2 Il Contesto

Premesso che negli anni l'AORN Santobono Pausilipon (nel seguito AORN) ha intrapreso diverse azioni al fine di rendere sicuri i propri sistemi informatici, attraverso servizi per la sicurezza perimetrale e degli accessi remoti, sistemi per la sicurezza degli end-point aziendali, sistemi per la sicurezza dei backup e dei server virtuali.

L'attuale infrastruttura dei Server fisici e virtuali, dei sistemi di virtualizzazione, dei sistemi per la Unufied communication presenti in azienda sono rappresentati sinteticamente di seguito:

2.1 I Data Center Aziendali:

L'azienda è provvista di n.2 Data Center CISCO® così distribuiti:

- Data Center CISCO® denominato CLU_HX_SB presso il CED del P.O. Santobono
- Data Center CISCO® denominato CLU_HX_CR presso il CED del P.O. Pausilipon

I due Data Center HX CISCO® sono composti ognuno da 3 nodi HyperFlex CISCO®, per fornire un cluster ad alta disponibilità.

Ogni cluster include un nodo Cisco® HyperFlex HX Data Platform controller che implementa un file system distribuito che sfrutta i dischi flash SSD presenti nei server per la memorizzazione dei dati.
I nodi HX sono server Cisco® UCS series-C nello specifico il modello è HX240M5 All Flash.
Ogni nodo HX dell'infrastruttura è equipaggiato con 2 processori Intel® Xeon® Gold 6230 (20 cores, 2.1 GHz) e n. 16 banchi di RAM da 32 GB (DDR4-2933-MHz) per un totale di RAM disponibile pari a 512 GB per server.
La componente networking di ogni nodo HX è demandata alla scheda mLOM (su slot mother-board), che è in grado di fornire quattro porte 10-Gbps.
La componente storage è composta da 6 dischi SSD da 3,8TB su un totale di 26 slot disponibili.
I 3 nodi sono collegati tra di loro mediante una coppia di Cisco® UCS 6454 Fabric Interconnect, che rappresentano il cuore in termini di connettività per fornire un layer di accesso integrato (storage network, ethernet network, management network) ai diversi server che verranno ad essi collegati.
Ogni Cisco® UCS 6454, in termini di alta affidabilità, possiede un meccanismo di boot ridondante composto dalla porzione attiva di software di boot ed il suo backup, in caso di malfunzionamento della porzione primaria di software di boot, il sistema è in grado di utilizzare e partire dalla porzione di boot di backup.
Ognuno dei Fabric Interconnect possiede porte dedicate per la clusterizzazione diretta tra i due apparati, inoltre il Cisco® UCS manager software che risiede all'interno dei Fabric Interconnect contiene meccanismi di controllo e gestione dell'heartbeat tra i due apparati, rilevamento e risoluzione di problemi e propagazione delle informazioni di configurazione, di conseguenza anche la componente software di gestione del sistema è soggetto ad alta affidabilità in quanto è presente una istanza di UCS Manager su ognuno dei Fabric Interconnect, sempre forniti in coppia in ogni soluzione Cisco® UCS.
Il sistema Cisco® UCS 6454 è collegato con porte a 40GE agli switch core per gestire le VLAN dedicate al sistema Hyperflex e l'accesso ai servizi da lui gestiti.

I dettagli dei due cluster sono:

HX-SERVER SANTOBONO				HX-SERVER PAUSILIPON			
Name	**PID**	**Model**	**Serial**	**Name**	**PID**	**Model**	**Serial**
Server 1	HXAF240 C-M5SX	Cisco HXAF240c M5SX	WZP240 1057T	Server 1	HXAF240C-M5SX	Cisco HXAF240c M5SX	WZP240 1058M
Server 2	HXAF240 C-M5SX	Cisco HXAF240c M5SX	WZP240 1058E	Server 2	HXAF240C-M5SX	Cisco HXAF240c M5SX	WZP240 1058H
Server 3	HXAF240 C-M5SX	Cisco HXAF240c M5SX	WZP240 1058D	Server 3	HXAF240C-M5SX	Cisco HXAF240c M5SX	WZP240 10EZ2

Tabella 1 – Dati Server HX

2.2 SISTEMA di Unified Wireless Network Solutions della Cisco® Systems

Il sistema ha la seguente architettura:

server	servizio	sito
Server #1 AIR-CT5520	Wireless LAN Controller	P.O. Santobono
Server #2 AIR-CT5520	Wireless LAN Controller	P.O. Santobono
140 AIR-AP1852I	Access Point	Tutti i presidi

La piattaforma **CUWSN**, ovvero **C**ISCO® **U**nified **W**ireless **N**etwork **S**olutions, prevede una gestione unificata dell'intera infrastruttura Wireless attraverso un'unica console di gestione centralizzata denominata **W**ireless **L**AN **C**ontroller (**WLC**).
La soluzione prevede anche la piattaforma **Cisco® ISE** (**I**dentity **S**ervices **E**ngine) per erogare un servizio di accesso controllato tramite Captive Portal del personale interno (utenza tecnica e non) e degli Account Guest.

2.3 SISTEMA di Unified Communication

Anche questo sistema è della Cisco® Systems abilitante la nuova Centrale Telefonica VoIP ed ha la seguente architettura:

La piattaforma Unified Communications è implementata in ambiente virtualizzato reso disponibile nell'infrastruttura di Data Center di proprietà dell'AORN.
Le Virtual Machine installate per mettere in produzione le Applicazioni Unified Communication contemplate nel progetto sono le seguenti:

- Cisco® Unified Communication Manager, n°3 server virtuali ognuno con 2vCPU, 6GB vRAM, 80 GB vHDU
- Unified CM IM and Presence n.1 server virtuale con 1vCPU, 4GB vRAM, 80 GB vHDU
- **C**isco® **U**nity **C**onnection (CUC) n°1 server virtuale con 2vCPU, 4GB vRAM, 160 GB vHDU
- Applicazioni di terze parti Imagicle; n°1 server virtuale con 4vCPU, 8GB vRAM, 160 GB vHDU

La soluzione proposta prevede un'unica centrale telefonica **IP Cisco® Communications Manager** distribuita su macchine virtuali installate su hardware distinto al fine di garantire un'architettura di Alta Affidabilità e bilanciamento di carico tra i servers che costituiscono il Cluster.
Il Communications Manager (C.U.C.M. Cluster) è stato dimensionato per gestire tutti i terminali telefonici installati in soluzione ad alta affidabilità e ridondata.

3 Fabbisogno progettuale

Malgrado i servizi di sicurezza che si sono attivati negli anni, sono ancora molte le aree che richiederebbero un incremento della sicurezza informatica aziendale, motivo per il quale il progetto che si vuole realizzare prevede l'inserimento di specifiche soluzioni hardware e software esclusivamente dedicate alla sicurezza delle seguenti aree:

a) Sicurezza dei servizi WEB aziendali esposti verso il mondo esterno
b) Sicurezza dei sistemi Elettromedicali e IoT
c) Sicurezza degli accessi e gestione delle identità
d) Sicurezza dei dispositivi.

L'analisi dei fabbisogni dell'AORN ha difatti evidenziato l'esigenza di incrementare la sicurezza informatica nelle suddette aree; pertanto, questa amministrazione vuole realizzare il seguente progetto introducendo le soluzioni per ogni area di interesse relativo la sicurezza informatica aziendale, così come di seguito riportato:

e) *Sicurezza dei servizi esposti verso il mondo esterno (WEB)*
1. Sistemi di sicurezza WAF (*Web Application Firewall*), capaci di difendere i servizi esposti da attacchi di tipo *SQL injection*, *XSS* (*Cross-Site Scripting*), *zero-day* e minacce verso i servizi http esposti.
2. Sistemi di analisi del traffico aziendale che attraverso algoritmi di verifiche comportamentali e supportati da *Threath Intelligence*, siano in grado di identificare minacce di tipo *phishing, malware, ransomware* ed esfiltrazione dei dati.
3. Sistemi dedicati al controllo dello SPAM e-mail e *anti-phishing* in ingresso e in uscita dai sistemi di posta elettronica aziendale.

f) *Sicurezza dei sistemi Elettromedicali e IoT*
1. La soluzione hardware che intendiamo adottare consiste nell'inserimento di specifiche appliance dedicate per la difesa di sistemi elettromedicali e IoT che consentano un *virtual patching* a livello infrastrutturale senza modificare gli endpoint e forniscano una protezione costante da attacchi di sicurezza. Tali sistemi verranno collocati all'interno dell'infrastruttura di rete in modo da individuare il traffico da e verso i dispositivi medici.

g) *Sicurezza degli accessi e gestione delle identità*
1. Sistema dedicato che ha come obiettivo la raccolta centralizzata della telemetria di rete, delle soluzioni predisposte alla sicurezza degli utenti e delle applicazioni. Grazie al machine learning le attività di correlazione e monitoraggio consentono di poter individuare in maniera tempestiva possibili vulnerabilità dei sistemi operativi/software, possibili attacchi informatici e potenziali *data breach*. Tale soluzione sarà predisposta non solo al rilevamento delle minacce ma anche della loro *remediation*.
2. SYSLOG server di tutti gli eventi di sicurezza collegati al firewall e al sistema AntiSPAM, il suo scopo è quello di fornire un'unica dashboard di gestione per visualizzare le attività registrate dai sistemi di sicurezza Aziendali.
3. Sistema dedicato per la gestione delle identità e degli accessi, al fine di garantire il corretto livello di permessi per il corretto accesso in rete ed agli applicativi aziendali, oltre a poter gestire tramite apposito portale il provisioning delle identità utente e delle piattaforme IoT.
4. Appliance dedicata alla gestione dell'utenza remota tramite VPN, agli accessi degli utenti a più fattori (App, SMS, etc.) di autenticazione sia per gli accessi al dominio che ai sistemi aziendali su specifiche applicazioni (ad esempio la posta elettronica).
5. Sistema dedicato al controllo e monitoraggio degli accessi con credenziali privilegiate, controllandone le sessioni e tenendone traccia in maniera sicura.

h) Sicurezza dei dispositivi
1. Soluzione dedicata al processo di prioritizzazione delle vulnerabilità di sicurezza presenti sull'infrastruttura ICT per minimizzare il rischio di esposizione agli attacchi informatici.

Tutte le soluzioni riportate si integreranno nel sistema di gestione delle credenziali LDAP presente in azienda, al fine di migliorare la sicurezza degli accessi ed il controllo dell'infrastruttura.

Per quanto esposto finora risulta evidente che tutte le forniture hardware e software dovranno, pena esclusione, essere compatibili con l'infrastruttura preesistente per salvaguardare i molteplici investimenti fatti finora che hanno sempre visto l'AORN prediligere soluzioni posizionate in alto a destra nel Quadrante Gartner per preferire alta qualità, efficienza ed affidabilità rispetto al risparmio economico. In particolare, la totalità della fornitura dovrà essere, in continuità con il preesistente, sempre di tecnologia CISCO® e, quando non esistente di tale marca, compatibile ed immediatamente installabile (plug & play). Se la fornitura non rispetterà, anche una sola delle caratteristiche esposte, il concorrente sarà escluso, come più dettagliatamente esposto al prossimo paragrafo 6.2.

4 Specifiche della fornitura

4.1 Requisiti generali

Di seguito vengono indicate le specifiche tecniche delle varie componenti che costituiscono l'oggetto della fornitura. Tali specifiche devono intendersi come **caratteristiche minime**, alle quali le componenti **devono** rispondere. Il mancato soddisfacimento di un requisito minimo comporterà l'**esclusione dalla gara**.

Sarà cura del Fornitore indicare con maggior dettaglio tutte le funzionalità della soluzione proposta. Tutto il materiale dovrà essere completo di ogni accessorio (cavi di alimentazione, cavi di rete, cavi in fibra ottica, etc.) necessario al collegamento degli apparati oggetto della fornitura, al collegamento di tali apparati alle apparecchiature esistenti nei CED dell'AORN, al funzionamento delle attrezzature, dei driver, del sistema, oltre alle licenze d'uso inerenti apparati e software di gestione e/o amministrazione di base e di utilità.

Tutte le apparecchiature hardware dovranno rispettare le norme sugli standard tecnici, sugli standard di qualità, sicurezza, ergonomia e sugli standard di comunicazione indicati nella normativa italiana ed europea in vigore.

Inoltre, si fa presente che i materiali oggetto della fornitura si intendono **nuovi di fabbrica**, corredati di marchio CE, in produzione al momento dell'aggiudicazione, non usati o rigenerati, contenuti nella loro confezione originale, licenziati specificatamente per l'AORN Santobono Pausilipon, che sarà quindi il primo acquirente di tali prodotti e primo licenziatario di qualsiasi copia del software, compreso quello incluso negli apparati. L'AORN Santobono Pausilipon si riserva di potere richiedere al costruttore le verifiche per documentarne l'origine tramite il "*serial number*" degli apparati forniti.

4.2 L'infrastruttura *CyberSecurity* attuale

L'attuale infrastruttura di *CyberSecurity* dell'AORN risponde a quelle che sono state le esigenze immediate in termini di protezione dei dati e degli utenti.
Attualmente presso l'AORN è funzionante un servizio che utilizza il prodotto denominato SIEM, in dettaglio la suite IBM Security QRadar, la quale rappresenta una soluzione per correlare gli alert provenienti dai sistemi di sicurezza, progettata per unificare l'esperienza degli analisti di sicurezza e accelerare la loro velocità lungo l'intero ciclo di gestione degli incidenti. In particolare, si integra con prodotti di terze parti XDR e SOAR, si occupa della gestione dei log e della aggregazione degli stessi, log derivanti da tutte le soluzioni di sicurezza informatica presenti sul campo.
È presente anche una soluzione di *Firewalling* perimetrale ed una VPN per l'accesso remoto dedicata a consulenti esterni e a tutto il personale che ha la necessità di lavorare da remoto.
Questa amministrazione è dotata anche di una soluzione di protezione dei dati di carattere Enterprise e che subentra in casi di ripristino dopo attacco o in tematiche di *Disaster Recovery*.
Sono presenti, inoltre, anche altre soluzioni in fase di scadenza, tale per cui questa amministrazione ha dovuto procedere con una analisi dei fabbisogni ed una risultante architettura confacente a quanto richiesto dall'Azienda Ospedaliera per la protezione dei propri dati e dei propri utenti.
L'approccio al tema *CyberSecurity* evolutosi in questi ultimi anni è stato a Silos, seguendo quelle che erano le esigenze del momento, approccio che questa Amministrazione vuole cambiare per passare ad un discorso maggiormente architetturale basato sui concetti di prevenzione e di conoscenza delle minacce, più comunemente denominata *Threat Intelligence*.
Tale approccio architetturale è derivante dalle esperienze pregresse che hanno portato questa Amministrazione a non ragionare più in termini singoli come ad esempio:

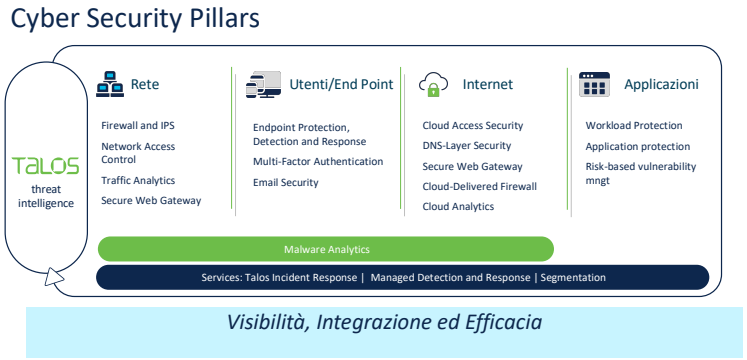
- Acquisire singoli prodotti o soluzioni dedicate a risolvere uno specifico incidente di sicurezza
- Attuare una comparazione sterile dei prodotti di sicurezza basata su caratteristiche specifiche
- Utilizzare Brand che non abbiano una solidità storica, questo per evitare il caso della cancellazione di prodotto, e quindi di supporto, con conseguente impatto economico sul budget dell'AORN.

5 La Nuova infrastruttura *CyberSecurity*

L'inserimento delle soluzioni citate nella descrizione del progetto incrementerà di molto la sicurezza informatica aziendale in quanto gli obiettivi che ci si è proposti di raggiungere ed i relativi risultati sono:
VISIBILITÀ: aumento del controllo della sicurezza aziendale, interna ed esterna, mediante sistemi di tracciamento e raccolta degli eventi, specialmente di quelli che utilizzano alti privilegi o che accedono ad aree critiche dei sistemi aziendali.
SEGMENTAZIONE: suddivisione delle aree di accesso e di traffico orizzontale e verticale, con relativo innalzamento del livello di protezione delle comunicazioni da e verso Internet o in generale verso le reti esterne, garantendo anche un maggiore livello di protezione dei servizi esposti, e funzionalità di reverse proxy e patch management dei sistemi.
CONTENIMENTO: Protezione di tutti gli apparati (end point), anche quelli che oggi risultano obsoleti o non gestibili mediante i consueti sistemi antivirus, ma che per motivi operativi non possono essere aggiornati o sostituiti, e che sono motivo di vulnerabilità per i sistemi informatici aziendali.

In sintesi, tutte le azioni descritte vanno nella medesima direzione, che è quella di garantire all'AORN un maggiore controllo dei propri sistemi aziendali ed una politica di ZERO TRUST, aumentando il livello di sicurezza interno ed esterno, e al tempo stesso inserendo sistemi di monitoraggio che riescano anche in maniera predittiva ad anticipare possibili attacchi ai sistemi o compromissione di dati critici aziendali.
Per poter realizzare tale obiettivo si è andati alla ricerca di soluzioni che fossero integrabili, programmabili e sicure. In particolare, seguendo le esigenze di:

- Avere informazioni in tempo reale sulle vulnerabilità di sicurezza critiche nel contesto ICT di riferimento;
- Avere a disposizione mappe dei dati sulla privacy per aver chiaro come i dati vengono gestiti, utilizzati e protetti;
- Avere notifiche tempestive e con chiare azioni di *remediation* in caso di violazione della sicurezza aziendale;
- Scegliere un *vendor* che misuri e renda pubbliche le politiche di progettazione ed i controlli per lo sviluppo sicuro delle soluzioni, la gestione delle vulnerabilità e la privacy e protezione dei dati.



Il modello di riferimento è basato su quattro concetti: protezione della rete, protezione degli End Point e degli utenti, protezione degli accessi ad internet, protezione delle applicazioni esposte, il tutto visibile ed integrato nativamente con una soluzione di XDR (Extended *Detection* and *Respond*) e che si avvale di una *threat intelligence* che rappresenti il *best of breed* nel campo della *Cybersecurity* mondiale.
Questa amministrazione si propone di blindare i dati aziendali realizzando con tale architettura un costrutto solido ed

esaustivo, in particolare monitorando la sicurezza basata sulla rete e sugli endpoint per migliorare la visibilità in tempo reale e retrospettiva delle minacce, individuando e isolando in caso di incidente informatico le macchine, i dipendenti, i clienti o i partner interessati.
Per quanto descritto sopra si richiede quindi la fornitura di:
SICUREZZA NETWORK

- **n.1 soluzione di controllo accessi alla rete LAN** per 3.000 utenti;
- **n.1 soluzione di VPN client** per 500 utenti;
- **n.1 soluzione di Secure Network Analytics** per 8.000 flussi *netfow* analizzati per secondo;

SICUREZZA UTENTI/END POINT

- **n.1 soluzione MFA** per 900 utenti;
- **n.1 soluzione di protezione end point** per 800 client con funzionalità di *Vulnerability Assessment*;
- **n.1 soluzione di *Vulnerability Management*** per n. 2.800 *device*;
- **n.1 soluzione di *Secure E-mail*** per n. 2.000 caselle di posta;

SICUREZZA INTERNET

- **n.1 soluzione WAF** per n.5 applicazioni protette;
- **n.1 soluzione protezione *host* via DNS** per n. 2.000 utenti;

SICUREZZA APPLICAZIONI

- **n.1 soluzione di *Incident Response*** per 36 mesi;
- **n.1 soluzione XDR** per 800 utenti.

Tutta la fornitura dovrà essere installata e configurata a cura del l'aggiudicatario al fine del perseguimento del collaudo che si prevede debba avvenire plausibilmente entro la prima decade di dicembre 2023 per consentire a questa Amministrazione il pagamento all'Aggiudicatario ed il relativo recepimento delle fatture quietanzate. Ciò è necessario al fine di non pregiudicare il finanziamento del progetto.

5.1.1 L'architettura prescelta

L'architettura prescelta è quindi quella descritta nel paragrafo precedente, e cioè: protezione della rete, protezione degli utenti/end point, ove per end point si evidenziano quei dispositivi medicali che non possono essere modificati, protezione di Internet e protezione delle Applicazioni.
In tal senso la rete viene protetta da un sistema IPS/IDS che analizza il traffico passante, criptato e non, e senza violare alcunché di legato alla privacy del dato, verifica che in tale flusso non sia presente niente di malevolo, in caso contrario tale flusso viene bloccato e segnalato sia sul SIEM già presente presso AORN che sulla piattaforma XDR prevista in questa fornitura. Tale soluzione inoltre verrà utilizzata per operazioni di *virtual patching*, cioè, sarà specializzata per prevenire attacchi su specifiche vulnerabilità proteggendo gli endpoint tramite specifiche *signature*. Tale approccio è particolarmente critico per i sistemi non gestibili a livello di sistema operativo (ad esempio alcuni apparati elettromedicali). Sempre per la protezione del Network, avendo questa Amministrazione una infrastruttura LAN di marca Cisco, è stata scelta una soluzione di Identity Service Engine (controllo e segmentazione degli accessi alla rete) che ben si integra con tale infrastruttura. Per ottemperare inoltre ad una mancanza di visibilità sul cosiddetto traffico orizzontale, è oggetto di fornitura una soluzione di visibilità e controllo del cosiddetto traffico tra client e client o client e server all'interno della nostra organizzazione. È noto, infatti, che la maggior parte delle soluzioni informatiche di sicurezza si concentrano sull'analisi del traffico cosiddetto verticale, cioè quello che va da client verso internet e viceversa. Con tale soluzione l'AORN andrà a coprire un'area attualmente scoperta ed altrettanto importante, prevenendo e monitorando i movimenti laterali degli attaccanti.
Si è inoltre deciso, in un'ottica di *Zero Trust Architecture*, di introdurre un sistema di accesso al perimetro aziendale tramite una soluzione *Multi Factor Authentication* seguendo il paradigma di autenticazione con "qualcosa che si sa" (password) e "qualcosa che si ha" (tipicamente il proprio telefono cellulare).
Per la parte utenti si andrà a rinforzare la parte di sicurezza degli *End Point*, comprensiva anche della sua casella e-mail, con tool che espletano funzionalità di analisi delle vulnerabilità, arricchita da meccanismi basati su intelligenza artificiale di prioritizzazione delle stesse allo scopo di accelerare il *patching* di quelle più critiche abbassando il fattore di rischio da attacco informatico. È noto altresì che il tema dello Staff ridotto sia un problema per tutte le Pubbliche Amministrazioni, tali soluzioni permetteranno all'AORN di dare massima priorità a minacce, operazioni di *patching* ed altro, sulla base del contesto e dell'importanza della minaccia.
Sul tema Internet l'AORN applicherà tecnologie leader di mercato per la protezione delle applicazioni quali il Web Application *Firewalling* e protezione tramite analisi del traffico DNS effettuato da un endpoint. Quest'ultima, tramite meccanismi di Threat Intelligence ed evoluti algoritmi di sicurezza, è in grado di bloccare tutti gli scambi tra client infetto ed internet relativi a minacce conosciute ed anche Zero-Day. In tal modo si aggiunge una protezione dalle minacce di malware e ransomware unica per efficacia e semplicità di implementazione in grado di proteggere gli utenti sia all'interno che all'esterno del perimetro aziendale.
Allo scopo di massimizzare la fase di *detection* di un attacco informatico e di garantire una *remediation* efficace tutte le soluzioni di sicurezza si integreranno con una piattaforma di XDR.

Tale componente si affiancherà ed integrerà al SIEM già presente presso l'AORN per completare gli strumenti di correlazione degli eventi a disposizione dello staff che si occupa della sicurezza informatica dell'AORN.
Segue dettaglio ed elenco delle soluzioni oggetto di fornitura.

5.1.2 Soluzione di controllo Accessi *Identity Service Engine*

Si richiede la fornitura di una soluzione di controllo accessi alla rete e di *Identity Service Engine*, una soluzione come detto sopra per rispondere alle moderne necessità di identificazione dell'utenza e dei dispositivi connessi alla rete, che deve essere parte integrante di un framework più ampio SDN, e che interagisce nativamente con l'infrastruttura di rete oltre che in grado di distribuire in modo consistente le Policy d'accesso sia per la rete LAN e quella WiFi, che per quella VPN, con possibilità di definire ambienti ad elevata sicurezza anche per ospiti e conferenze (*Guest Access*).
La soluzione richiesta ISE si deve configurare come la piattaforma centralizzata d'eccellenza per la definizione ed il controllo delle politiche d'accesso per tutta la rete. Deve consentire di impostare regole automatizzate che determinino chi può accedere alla rete, tramite quale dispositivo, in quali fasce orarie, da quale luogo.

Le funzioni principali della soluzione da offrire sono:

- Definizione e Gestione delle *Policy* d'accesso alla rete
- Autenticazione, Autorizzazione ed *Accounting* (AAA) di utenti e dispositivi
- Interazione con i sistemi di *Directory* già presenti (*Active Directory*, LDAP, RADIUS, …)
- Visibilità in real-time e storicizzata di chi accede alla rete, con cosa, per quanto, da dove
- Profilazione di utenti e dispositivi, non solo in base alle credenziali ma anche grazie ad una tecnologia avanzata di riconoscimento attuata tramite "*Probing*", "*Scanning*", "*Listening*" dei client che si collegano in rete, con dizionari specifici per i client biomedicali
- Gestione Ospiti (*Guest Access*)
- Integrazione con la soluzione di NG IPS e *Secure Network Analytics* per automatizzare la messa in quarantena di un dispositivo che è coinvolto in un attacco informatico individuato dalle altre soluzioni
- Completa integrazione nell'infrastruttura di rete Cisco; la soluzione proposta deve poter dialogare con i dispositivi di LAN, WiFi e WAN per coordinare le operazioni di "*Policy Enforcement*" attraverso la tecnologia *Cisco® TrustSec, technologies* che permette di:
    - Segmentare e/o Micro-Segmentare la rete in accordo con le politiche d'accesso, definite sulla base dei gruppi d'utenza.
    - Applicare consistentemente le policy di sicurezza attraverso strumenti avanzati quali i "*Security Group Tag*" (SGT) senza la necessità di moltiplicare il numero di VLAN, complicando il design di rete. Si semplificano così "*Provisioning*" e Gestione;
    - Contenere le minacce di sicurezza, limitando la diffusione di potenziali Malware, grazie al controllo e alla prevenzione di spostamenti non autorizzati di *Endpoint* in rete.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Management centralizzato	La soluzione deve avere una console web-based per configurare e gestire centralmente profili, *policy, posture*, accesso guest, altro
Contenuti delle Policy	La soluzione deve supportare un modello di policies basato su regole e attributi per politiche di controllo dell'accesso basate su attributi come l'identità dell'utente e dell'endpoint, i protocolli di autenticazione, l'identità del dispositivo e altri attributi esterni. Questi attributi possono essere creati dinamicamente e salvati per un uso successivo.
Integrazione con sistemi esterni di autenticazione	La soluzione deve supportare l'integrazione con diversi repository di identità esterni come Microsoft Active Directory (On-Prem o Azure AD), *Lightweight Directory Access Protocol* (LDAP), RADIUS, RSA One-Time Password (OTP), *certification authority* sia per l'autenticazione che per l'autorizzazione, Open Database Connectivity (ODBC) e fornitori SAML.
Access Control	La soluzione deve supportare una serie di opzioni di controllo dell'accesso, tra cui liste di *downloadable Acces Control List* (dACL), Virtual LAN (VLAN), reindirizzamenti URL, *named* ACL e *Security Group* ACL (SGACL) configurati tramite tecnologia *Cisco Security Group*.
Cisco Security Group Policy	Essendo presente una infrastruttura LAN Cisco, la soluzione deve prevedere meccanismi di segmentazione più semplice mediante l'uso di *Security Group Tags* (SGT). Tale tecnologia è una tecnologia aperta nell'IETF, disponibile all'interno di *OpenDaylight* e supportata su piattaforme di terze parti e Cisco. Con tale tecnologia le informazioni di gruppo propagano gli SGT su dispositivi di rete nei flussi dati (inline tagging) o tramite *Security Group Tag Exchange Protocol* (SXP) per l'associazione IP-a-SGT dove i dispositivi non hanno la capacità di eseguire il tagging dei pacchetti con gli SGT.
Controller di segmentazione	La soluzione fornita deve essere il controller di segmentazione che semplifica la gestione delle regole di switch, router, wireless e firewall.

Tabella 3 - Requisiti minimi per la soluzione ISE

Si richiede la fornitura di n.1 soluzione software ISE.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- Soluzione virtualizzata e virtualizzabile su piattaforma *Vmware*;
- N.3.000 licenze *Advantage*

5.1.3 Soluzione VPN

Si richiede la fornitura di una soluzione di VPN client, che, nell'ottica della semplificazione operativa, deve essere inclusa all'interno di un unico client, che possa espletare le diverse funzionalità di sicurezza dettagliate nel resto del documento, tra cui la soluzione di protezione dell'endpoint e la protezione dagli attacchi DNS. Questo permetterebbe di ridurre il numero di client installati sui dispositivi oltre che la gestione degli stessi. La soluzione deve essere compatibile e/o dello stesso *vendor* relativamente a quanto descritto al paragrafo 4.1.1..
La soluzione proposta deve avere diverse opzioni per connettere, riconnettere o disconnettere automaticamente le sessioni VPN. Queste opzioni devono consentire di selezionare automaticamente il punto di accesso di rete ottimale e adattare il protocollo di tunneling al metodo più efficiente, incluso il protocollo *Datagram Transport Layer Security* (DTLS) per il traffico sensibile alla latenza. La soluzione deve anche supportare la tecnologia di tunneling IP Security Internet Key Exchange versione 2 (IPsec IKEv2) e l'accesso VPN selettivo dell'applicazione deve poter essere applicato anche su Apple iOS e Google Android.
La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Integrazione	La soluzione deve essere integrabile con la piattaforma *Firepower* sopra descritta, in termini di terminatore del flusso VPN
Sistema operativo	La soluzione deve supportare tutti i sistemi operativi client maggiormente diffusi, tra cui sicuramente Windows, macOs, IOS ed Android.
Protocolli di tunneling	La soluzione proposta deve supportare i seguenti protocolli di Tunneling: • SSL (TLS 1.2 and DTLS 1.2) e next-generation IPsec IKEv2 • Protocolli *latency-sensitive traffic* come DTLS • TLS 1.2 (HTTP over TLS or SSL) • IPsec IKEv2

Tabella 4 - Requisiti minimi per la soluzione VPN

Si richiede la fornitura di n.1 soluzione software VPN.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- Soluzione client per tutte le piattaforme;
- N.500 licenze Apex

5.1.4 Soluzione di *Secure Network Analytics*

Si richiede la fornitura di una soluzione di controllo del cosiddetto traffico orizzontale ed interno, cioè di *Secure Network Analytics*.
La soluzione da fornire deve essere una soluzione avanzata di analisi della rete progettata per rilevare e mitigare le minacce informatiche in modo efficace. Deve combinare intelligenza artificiale (AI) e *machine learning* (ML) per effettuare una continua analisi comportamentale del traffico di rete e identificare deviazioni dalla normalità o comportamenti interni sospetti che potrebbero indicare attività dannose.
Le caratteristiche principali che deve avere la soluzione di *Secure Network Analytics* sono:

1. *Rilevamento avanzato delle minacce:* la soluzione dovrà utilizzare modelli di machine learning per rilevare automaticamente le minacce informatiche, compresi attacchi di *exfiltration*, data *hoarding*,, attacchi DDoS e comportamenti anomali nella rete;
2. *Infrastruttura di rete come sensore:* la soluzione dovrà essere in grado di sfruttare la visibilità degli apparati di rete, collezionando informazioni sotto forma di metadato (*Netoflow*/IPFIX, altri), non richiedendo quindi necessariamente la presenza di sonde/SPAN;
3. *Analisi approfondita del traffico di rete:* La soluzione *Secure Network Analytics* dovrà analizzare in modo approfondito il traffico di rete per identificare pattern di attacco, anomalie di comportamento e indicatori di compromissione. Questo dovrà consentire di individuare rapidamente le minacce e rispondere in modo tempestivo;
4. *Visibilità completa della rete:* La soluzione dovrà offrire una visibilità completa su tutti ii flussi di traffico della rete, consentendo di individuare rapidamente comportamenti che non sono in compliance con le policy di segmentazione adottate

5. *Indagini forensi avanzate*: La soluzione proposta dovrà registrare e conservare un registro dettagliato delle attività di rete per consentire indagini forensi approfondite in caso di incidenti di sicurezza. Questo aiuterà a identificare la causa principale degli attacchi e a prendere misure per prevenirli in futuro;
6. *Integrazione con soluzioni di sicurezza Cisco:* La soluzione si dovrà integrare con altre soluzioni di sicurezza, come i firewall ed i sistemi di gestione degli eventi e delle informazioni sulla sicurezza (SIEM), per una protezione completa e coordinata della rete. Si dovrà altresì integrare con la soluzione di controllo degli accessi, per permettere la messa in quarantena di un dispositivo coinvolto in un comportamento malevolo in maniera automatizzata;
7. *Automazione e risposta agli incidenti:* La soluzione proposta dovrà automatizzare la risposta agli incidenti, consentendo di implementare misure correttive e mitigare rapidamente le minacce in modo automatico o guidato dall'operatore.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Ottimizzazione dei flussi	La soluzione deve poter gestire un numero elevato di flussi, attuando azioni di data *stitching* e data *deduplication* al fine di ottimizzare la mole di flussi frammentati raccolti in dei flussi bidirezionali e univoci
Gestione delle componenti esterne	La soluzione deve essere in grado di gestire componentistica esterna quali *Flow Collector*, *Flow Sensors*
Utilizzo di flussi di dati differenti	La soluzione deve essere in grado di gestire flussi di dati di diversa natura quali flussi *Netflow*, IPFIX e *sFlow*.
Mappe di flusso personalizzabili	La soluzione deve consentire la creazione di mappe di utenti e relativi flussi di traffico, per poter meglio monitorare il traffico comportamentale di gruppi di utenti e di agire quindi nello specifico
Threat Detection	La soluzione deve prevedere l'acquisizione dei record del *proxy* e l'associazione ai record di flusso per fornire le informazioni sull'utente, sull'applicazione e sull'URL per ciascun flusso, al fine di aumentare la comprensione contestuale del traffico. Questo processo migliora la capacità dell'organizzazione di individuare le minacce e riduce il cosiddetto *Meat Time To Know* (MTTK).

Tabella 5 - Requisiti minimi per la soluzione Security Network Analytics

Si richiede la fornitura di n.1 soluzione *Security Network Analytics*.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.8.000 *Flows per second*

5.1.5 Soluzione di *Multi Factor Authentication*

Si richiede la fornitura di una soluzione di *Multi Factor Authentication* (MFA) che offra una protezione avanzata per l'accesso alle applicazioni aziendali. Con l'obiettivo di migliorare la sicurezza dell'identità digitale, deve garantire un'esperienza di autenticazione sicura e semplice per gli utenti, proteggendo le applicazioni aziendali da accessi non autorizzati.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Autenticazione multi-fattore (MFA):* la soluzione da fornire deve supportare l'autenticazione a più fattori, che richiede agli utenti di verificare la propria identità utilizzando più elementi, come *token* fisici o virtuali, biometria (come le impronte digitali) e notifiche *push* sul dispositivo mobile;
2. *Accesso sicuro da qualsiasi luogo:* la soluzione da fornire deve consentire agli utenti di autenticarsi e accedere alle risorse aziendali in modo sicuro da qualsiasi posizione, sia che si trovino in ufficio, in remoto o in mobilità;
3. *Gestione centralizzata delle identità:* la soluzione da fornire deve offrire un pannello di controllo centralizzato che consente agli amministratori di gestire in modo efficiente le politiche di accesso e le autorizzazioni;
4. *Integrazione con una vasta gamma di applicazioni:* la soluzione da fornire deve integrarsi con numerosi servizi e applicazioni, tra cui SaaS (Software as a Service), *on-prem* come VPN (*Virtual Private Network*), servizi di autenticazione remota, portali web e molto altro;
5. *Authentication basata sul rischio:* la soluzione deve essere in grado di cambiare dinamicamente le politiche di accesso, sulla base di segnali di rischio. Ad esempio, quando l'utente si sposta dal WiFi aziendale su un nuovo WiFi pubblico non facente parte dell'azienda;
6. *Reporting e monitoraggio:* la soluzione da fornire deve produrre un reporting dettagliato e un monitoraggio in tempo reale delle attività di autenticazione, consentendo agli amministratori di identificare potenziali anomalie o tentativi di accesso non autorizzati.

7. *Integrazione con la soluzione di Protezione dell'Endpoint:* La soluzione deve essere in grado di recepire dalla soluzione di *Endpoint* che un dispositivo risultato infetto, e di conseguenza in maniera automatica negare l'accesso di quel dispositivo alle applicazioni aziendali sulla base delle policy definite.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Sistema Operativo	La soluzione deve supportare entrambi i sistemi operativi mobili Apple iOS e Google Android
Tecniche di autenticazione	La soluzione deve supportare come tecnologie di autenticazione App mobile, SMS, chiamata telefonica, *token hardware*, sistemi biometrici
Gestione autonoma	La soluzione deve avere dei meccanismi di *self-enrollment* e *self-management*
Monitoraggio ed identificazione di rischi del device	La soluzione deve consentire di verificare se il device utilizzato per la MFA authentication è sottoposto a rischi ed in tal caso avere degli strumenti di comunicazione verso l'utente riguardo tali rischi
Renforcement	La soluzione deve prevedere meccanismi di enforcement riguardo all'accesso sicuro a singole applicazioni oppure su tematiche globali

Tabella 6 - Requisiti minimi per la soluzione MFA

Si richiede la fornitura di n.1 soluzione MFA.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.300 licenze Advantage

5.1.6 Soluzione di Protezione *End Point e Vulnerability Assesment*

Si richiede la fornitura di una soluzione di protezione *End Point e Vulnerability Assesment* che offra una avanzata protezione degli endpoint, progettata per difendere i dispositivi degli utenti finali da minacce informatiche avanzate. La soluzione deve offrire una protezione completa, in tempo reale per mitigare le minacce e garantire la sicurezza dei dispositivi endpoint all'interno di un'organizzazione.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Protezione contro malware avanzato*: la soluzione da fornire deve utilizzare tecnologie di rilevamento avanzate per identificare e bloccare *malware, ransomware, exploit* e altre minacce informatiche. Questo include la scansione in tempo reale dei file, l'analisi comportamentale e la reputazione dei file per rilevare e prevenire attacchi;
2. *Protezione in tempo reale:* la soluzione da fornire deve offrire una protezione in tempo reale, con capacità di rilevamento e risposta alle minacce istantanee. La soluzione dovrà monitorare costantemente i dispositivi endpoint per identificare attività sospette e rispondere prontamente per mitigare le minacce;
3. *Gestione centralizzata:* la soluzione da fornire dovrà permettere una gestione centralizzata degli *endpoint* attraverso un pannello di controllo intuitivo. Gli amministratori dovranno poter applicare politiche di sicurezza, monitorare lo stato di sicurezza dei dispositivi e gestire le minacce in modo efficiente;
4. *Protezione contro exploit:* la soluzione da fornire dovrà protegge i dispositivi endpoint contro gli exploit noti e zero-day, fornendo una difesa in profondità che include la prevenzione delle intrusioni e il controllo delle applicazioni
5. *Risposta automatizzata alle minacce:* la soluzione da fornire una risposta automatizzata alle minacce, consentendo di implementare misure correttive in modo rapido e automatizzato per mitigare gli attacchi e limitare l'impatto delle minacce;
6. *Visibilità sulle vulnerabilità:* la soluzione offerta dovrà avere funzionalità di visibilità sulle vulnerabilità, da utilizzare in congiunzione con la soluzione di Vulnerability Management al fine di definire un livello di rischio reale e contestuale associato ad una vulnerabilità.
7. Integrazione con la soluzione di MFA: La soluzione deve essere in grado di comunicare alla soluzione di MFA un dispositivo risultato infetto, e di conseguenza la soluzione di MFA in maniera automatica negherà l'accesso di quel dispositivo alle applicazioni aziendali sulla base delle policy definite.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Analisi dinamica	La soluzione deve includere un ambiente di *sandboxing* integrato e altamente sicuro, alimentato da tecnologia *Threat Grid*, per analizzare il comportamento dei file sospetti. L'analisi dei file deve fornire informazioni dettagliate, tra cui i comportamenti osservati, una mappatura di aderenza *al framework Mitre Attack*, e la possibilità di interagire durante l'esecuzione del malware (*glovebox*).
Sicurezza retrospettiva	La soluzione deve utilizzare una tecnologia che individui automaticamente le minacce avanzate che sono penetrate nel proprio ambiente. Alimentato dal monitoraggio continuo, la soluzione deve correlare le nuove informazioni sulle minacce con la storia precedente ed effettuare

	quarantena automaticamente dei file nel momento in cui iniziano a manifestare comportamenti dannosi.
Visibilità della riga di comando	La soluzione deve essere in grado di ottenere visibilità riga di comando aiuta, in modo ad esempio di determinare se applicazioni legittime, incluse le *utility* di Windows, vengano utilizzate a scopi maligni. La soluzione deve essere in grado di individuare comportamenti difficili da rilevare, come l'uso di *vssadmin* per eliminare *shadow copies* o disabilitare il *secure boot, exploit* basati su *PowerShell, privilage escalation*, modifiche alle ACL o tentativi di calcolare il numero dei sistemi.
Isolamento dell'end point	La soluzione deve consentire di isolare gli *endpoint* compromessi per fermare la diffusione delle minacce e impedire loro di comunicare con il comando e controllo (C&C), consentendo allo stesso tempo lo scambio di informazioni con risorse attendibili. Tale funzionalità deve consentire l'isolamento con un solo clic di un *endpoint* infetto, insieme alla possibilità di inserire nella *whitelist* risorse di rete attendibili.
Investigazione avanzata	La soluzione deve prevedere meccanismi di ricerca avanzata progettata per semplificare le indagini sulla sicurezza e la caccia alle minacce. La soluzione fornita deve avere come predefinite almeno cento query basate su *OSQuery* che consentono di eseguire rapidamente interrogazioni complesse su uno o tutti gli *endpoint*.

Tabella 7 - Requisiti minimi per la soluzione Protezione degli End Point

Si richiede la fornitura di n.1 soluzione Protezione di *End Point* e *Vulnerability Assesment*.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N. 1.000 licenze Premier

5.1.7 Soluzione di *Vulnerability Management*

Si richiede la fornitura di una soluzione di *Vulnerability Management* che rappresenti una piattaforma di gestione del rischio che aiuti l'AORN a rilevare, valutare e mitigare le minacce alla sicurezza. La piattaforma deve integrare i dati da una varietà di fonti, tra cui strumenti di gestione della sicurezza, *vulnerability scanners* e *feed* di *intelligence* sulle minacce, ed utilizzare questi dati per creare un quadro completo del rischio per un'organizzazione. Tale soluzione dovrà quindi aiutare le organizzazioni a identificare e classificare le vulnerabilità, definendo le priorità per la mitigazione e monitorare l'efficacia delle attività di mitigazione.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Migliorare la visibilità sul rischio:* la soluzione offerta dovrà fornire una panoramica completa del rischio per l'AORN, combinando dati da una varietà di fonti. Ciò consentirà all'AORN di identificare e classificare le vulnerabilità in modo più efficiente e dinamico nel tempo e prendere decisioni più informate su come mitigare il rischio;
2. *Migliorare la mitigazione del rischio:* la soluzione offerta dovrà aiutare l'AORN a identificare e classificare le vulnerabilità in modo più efficiente, basandosi sia sulla probabilità che quella vulnerabilità sia effettivamente utilizzata, sia sul valore che gli asset vulnerabili hanno nel contesto specifico;
3. *Migliore conformità:* la soluzione offerta dovrà aiutare le organizzazioni a conformarsi agli standard di sicurezza pertinenti, tracciando le attività di sicurezza e generando *report* sulla conformità;
4. *Migliore collaborazione:* la soluzione offerta dovrà aiutare AORN a collaborare in modo più efficace sulla sicurezza, integrandosi anche con sistemi di ticketing.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Vulnerability data ingestion	La soluzione deve essere in grado di raccogliere e integrare informazioni sulle vulnerabilità presenti nei sistemi, applicazioni o dispositivi di un'organizzazione. Questi dati possono provenire da varie fonti, come *vulnerability scanner, feed* di *threat intelligence, database* di vulnerabilità pubblici o interni all'organizzazione.
Metriche di rischio	La soluzione deve poter definire ed utilizzare metriche di rischio basate sugli *asset* e/o gruppi di *asset* aziendali
Scoring	La soluzione deve essere in grado di calcolare una classifica di rischio tenendo in considerazione la combinazione di info sugli *asset*, sulle vulnerabilità e sulle metriche predefinite
Ticketing	La soluzione deve consentire l'integrazione con sistemi di *ticketing*

Tabella 8 - Requisiti minimi per la soluzione Vulnerability Management

Si richiede la fornitura di n.1 soluzione di *Vulnerability Management*.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.2.800 licenze *Advantage*

5.1.8 Soluzione di *Secure E-mail*

Si richiede la fornitura di una soluzione di *Secure E-mail* che metta in sicurezza la posta elettronica di AORN basata su tecnologia *Microsoft Exchange on-prem* e che aiuti l'AORN a proteggersi da attacchi di *phishing, ransomware* e altre minacce derivanti tramite canale posta elettronica.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Filtro antispam:* la soluzione proposta dovrà essere in grado di filtrare i messaggi di posta elettronica indesiderati, come *spam, phishing* e *Business E-mail Compromise* (BEC);
2. *Protezione da phishing:* la soluzione proposta dovrà identificare e bloccare i messaggi di phishing, che sono messaggi di posta elettronica progettati per ingannare gli utenti a rivelare informazioni personali o finanziarie;
3. *Protezione da allegati malevoli:* la soluzione proposta dovrà identificare e bloccare i messaggi di posta elettronica con allegati malevoli, analizzandoli anche con tecnologie di *sandboxing* se necessario
4. *Prevenzione della perdita dei dati (DLP):* la soluzione proposta dovrà essere utilizzata per impedire agli utenti di condividere informazioni sensibili tramite la posta elettronica;
5. *Autoremediation:* Possibilità di automatizzare la rimozione di una mail contenuta nella *inbox Outlook* di un utente, quando si scopre (a posteriori) che il contenuto (es. allegato) è stato identificato dalle *Threat Intelligence* come malevolo;
6. *Sandbox unificata*: Utilizzo di *sandbox* per l'analisi degli allegati sconosciuti. La soluzione di *sandbox* dovrà essere unificata per tutte le soluzioni (IPS, *E-mail, Endpoint*), in modo da avere una *repository* unica e centralizzata di tutti i file detonati;
7. *Reportistica e analisi:* la soluzione proposta dovrà fornire una serie di report e strumenti di analisi che possono essere utilizzati per monitorare l'efficacia della soluzione e identificare aree di miglioramento.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Global Threat Intellgence	La soluzione deve basarsi su meccanismi di *Threat Intelligence* che gestisca almeno 600 miliardi di e-mail al giorno, per avere una base dati larga ed esaustiva
Reputation filtering	La soluzione deve supportare meccanismi di *Threat Intelligence* basate sulla *Reputation*, ad esempio la reputazione del dominio mittente
Spam Protection	La soluzione deve avere dei meccanismi *Context Adaptive Scanning Engine* (CASE) per esaminare il contesto dell'e-mail e scartare almeno il 99% delle *e-mail di Spam*
Greymail filtering	La soluzione deve consentire la *detection* ed il *filtering* di e-mail derivanti da azioni *marketing, social network, e-mail* quindi di scarso interesse a cui l'amministratore deve poter dare il giusto peso
Malware defense	La soluzione deve prevedere meccanismi di analisi e blocco dei *malware* multilivello con interazione e scambio info tra soluzioni diverse
URL protection	La soluzione deve prevedere meccanismi di URL *protection* contro URL malevoli o *zero-day*; quindi, sospetti

Tabella 9 - Requisiti minimi per la soluzione Secure E-mail

Si richiede la fornitura di n.1 soluzione *Secure E-mail.*
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.2.000 licenze Advantage

5.1.9 Soluzione di Protezione *host* via DNS

Si richiede la fornitura di una soluzione di Protezione *host* via DNS che deve essere efficace contro i *malware* avanzati mirati o opportunistici, ed attuare la protezione mediante l'utilizzo di algoritmi di rilevamento predittivi non basati su componenti statiche. La soluzione deve allo stesso tempo consentire una applicazione estesa semplice e pervasiva, che non necessiti di modifiche infrastrutturali (ad esempio installazione di componenti *hardware*) o modifiche dell'esperienza utenze (ad esempio utilizzo di *file proxy*). Per soddisfare i requisiti sopra riportati di protezione e trasparenza, si richiede che il Servizio si basi sull'analisi del DNS, essendo questa una componente cruciale dell'accesso ad Internet, il servizio richiesto deve poter consentire un enforcement, rapido, trasparente per l'utente, e privo di latenza. Il servizio deve poter essere realizzato puntando il DNS autoritativo e/o i Proxy i Data Center dell'AORN, senza necessità di installare hardware aggiuntivo e con lo stesso livello di copertura per tutte le tipologie di utenze (wired, fisso e mobile). Gli algoritmi di rilevamento del malware devono utilizzare tecnologie predittive *signatureless* in grado di predire e prevenire gli attacchi prima che questi diventino attivi su larga scala, fornendo protezione automatica in modalità *any device anywhere* (qualsiasi dispositivo indipendentemente da dove esso si connetta). La soluzione deve essere in grado di bloccare le minacce su ogni porta, protocollo o applicazione.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. Visualizzare le nuove attività di sicurezza dei dispositivi in tempo reale con report aggregati globalmente;
2. Evidenziare i dispositivi infetti o gli utenti colpiti da attacchi avanzati, riducendo il tempo per il contenimento e la *remediation*;
3. Garantire la conformità con le policy interne o le normative di riferimento, avendo eventualmente la possibilità di effettuare URL filtering con 60 categorie.
4. La soluzione deve utilizzare tecnologie di big-data analisi e machine learning per proteggere contro minacce note o sconosciute;
5. Aggiungere un livello di sicurezza predittiva per complementare le tecnologie basate su signature o analisi del comportamento;
6. Espandere la *situational awareness* ben oltre l'attività di rete per ogni sito o dispositivo, mediante visibilità globale delle minacce espande;
7. Garantire la protezione anche degli utenti che si trovano all'esterno della rete aziendale. Questo deve essere reso possibile senza l'aggiunta di un *client* aggiuntivo, oltre a quello già previsto per le altre funzioni di sicurezza descritte sopra (VPN, Protezione Endpoint), ovvero un client unico;
8. Il servizio non deve introdurre nessuna latenza, pertanto non deve rigirare le connessioni utente attraverso un *proxy o gateway* VPN per rendere sicuri gli utenti interni, esterni, e gli uffici remoti.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
No hardware	La soluzione proposta deve essere attivata puntando il DNS autoritativo, e/o i *proxy* in uso verso i data center del fornitore del servizio, senza necessità di installare *hardware* aggiuntivo.
Copertura mondiale	La soluzione offerta dovrà appoggiarsi su una rete di *data center* globale esterna a quella dell'aggiudicatario. Si richiede difatti una copertura globale da parte della *Threat Intelligence*. A questo scopo non sono ammesse soluzioni contestualizzate ad una specifica area geografica o nazione. In tale ottica, si richiede che la disponibilità del servizio sia 99.999%
Indipendenza di protocollo	La soluzione proposta deve essere in grado di rilevare le minacce recate da malware avanzato, indipendentemente dalla porta o dal protocollo utilizzato.
RFC 1918	La soluzione proposta deve essere in grado di bloccare, mediante apposita *policy* configurabile dall'utente, richieste DNS sospette che restituiscano indirizzi conformi con il piano di indirizzamento definito nell'RFC 1918 (quindi non ruotabili su Internet), o che siano dirette verso domini appartenenti a servizi di DNS dinamico.
C&C defense	La soluzione proposta deve essere in grado di prevenire le infezioni, bloccando le richieste DNS verso domini di distribuzione malware o siti drive-by, e contenere le infezioni preesistenti bloccando le richieste DNS verso infrastrutture di comando e controllo.
No signature statiche	Si richiede che la soluzione proposta faccia uso di intelligenza predittiva e non utilizzi solo *signature* o *blacklist* statiche.

Tabella 10 - Requisiti minimi per la soluzione Protezione host via DNS

Si richiede la fornitura di n.1 soluzione Protezione host via DNS.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.2.000 licenze *Advantage*

5.1.10 Soluzione WAF

Si richiede la fornitura di una soluzione WAF (*Web Application Filtering*) avanzata di protezione delle applicazioni web basata su cloud. La soluzione proposta deve fornire una difesa robusta e scalabile per le applicazioni web, proteggendole da attacchi informatici e garantendo la sicurezza dei dati.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Protezione delle applicazioni web:* la soluzione proposta dovrà essere in grado di rilevare e proteggere le applicazioni web da una vasta gamma di minacce, come attacchi di injection, cross-site scripting (XSS), furti di informazioni sensibili, attacchi DDoS e altro ancora. La soluzione dovrà utilizzare regole di sicurezza predefinite, personalizzabili e aggiornate costantemente per identificare e bloccare le vulnerabilità delle applicazioni;
2. *Scalabilità e disponibilità:* la soluzione proposta dovrà offrire la flessibilità e la scalabilità necessarie per proteggere le applicazioni web anche in ambienti ad alto traffico o in rapida crescita. La soluzione dovrà essere in grado di adattarsi dinamicamente alla domanda e garantire un'alta disponibilità delle applicazioni web;

3. *Gestione centralizzata:* la soluzione proposta dovrà offrire un pannello di controllo centralizzato che consentirà agli amministratori di gestire in modo efficiente le regole di sicurezza, monitorare le attività di protezione e analizzare le minacce in tempo reale;
4. *Intelligenza contro le minacce:* La soluzione proposta dovrà sfruttare i meccanismi di threat intelligence per identificare e mitigare le minacce emergenti. La soluzione dovrà altresì utilizzare meccanismi di analisi comportamentali, di machine learning e algoritmi avanzati per rilevare e bloccare le nuove varianti di attacchi informatici in modo proattivo;
5. *Monitoraggio e reporting:* la soluzione proposta dovrà offrire funzionalità di monitoraggio in tempo reale e generazione di report dettagliati sulle attività di protezione delle applicazioni web. Gli amministratori potranno e dovranno ottenere una visione chiara delle minacce identificate, delle azioni intraprese e delle prestazioni complessive delle applicazioni web protette;
6. *Integrazione con l'architettura presente e futura dell'AORN:* la soluzione proposta si dovrà integrare con altre soluzioni di sicurezza già presenti ed inserite in questo documento, consentendo una protezione completa e coordinata dell'intera infrastruttura di sicurezza. Ciò dovrà includere l'integrazione con le soluzioni IPS descritte in precedenza, il SIEM aziendale dell'AORN e altre soluzioni di sicurezza terze.
7.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Security policy Multicloud	La soluzione proposta deve poter definire delle *policy multicloud* consistenti per ridurre i costi ed i rischi
OWASP	La soluzione offerta dovrà appoggiarsi sulle tematiche di carattere globale OWASP e relative alle tematiche delle applicazioni web, in particolare la soluzione proposta dovrà poter respingere le cosiddette OWASP 10 Top, cioè le 10 più importanti minacce per le applicazioni web definite dalla comunità OWASP
Bot protection	La soluzione proposta dovrà essere in grado di identificare i Bot che hanno comportamenti human-like e che aggirano le tecnologie di *fingerprint*
Fully manager	La soluzione proposta deve essere *Fully Managed* e proattiva.
Autodiscovery	La soluzione proposta dovrà continuamente applicare controlli in *auto-discovery* sulle applicazioni web per intercettare cambiamenti ed ottimizzare in tempo reale le policy di sicurezza

Tabella 11 - Requisiti minimi per la soluzione WAF

Si richiede la fornitura di n.1 soluzione WAF.

La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.1 licenza WAF 50 Mbps
- N.1 licenza per 5 Applicazione protette WAF
- N.1 licenza Bot Manager 20M
- N.1 licenze Bot Manager per 5 applicazioni
- N.6 licenze ERT Premium per Application
- N.6 licenze ERT Premium Add On

5.1.11 Soluzione di *Incident Response*

Si richiede la fornitura di una soluzione di *Incident Response* che aiuti l'AORN a pianificare, rilevare, rispondere e recuperare da incidenti di sicurezza, questo in tempi velocissimi necessari per affrontare gli attacchi incombenti o in essere.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Gestione degli incidenti:* la soluzione di *Incident Response* dovrà aiutare AORN a sviluppare un piano di risposta agli incidenti che definisce i ruoli e le responsabilità, i processi e le procedure da seguire in caso di incidente;
2. *Rilevamento degli incidenti:* la soluzione proposta dovrà aiutare l'AORN a rilevare gli incidenti di sicurezza utilizzando una serie di tecniche, tra cui il monitoraggio delle minacce, la rilevazione delle intrusioni e la gestione degli eventi di sicurezza;
3. *Risposta agli incidenti:* la soluzione proposta dovrà aiutare le organizzazioni a rispondere agli incidenti di sicurezza in modo efficace, efficiente e veloce. Le risorse umane tenutarie di skill di *threat management* di altissimo livello dovranno essere in grado di operare velocemente utilizzando una serie di tecniche, tra cui l'isolamento dell'incidente, l'indagine sull'incidente e la mitigazione dell'incidente;
4. *Recupero dagli incidenti:* la soluzione proposta dovrà aiutare l'AORN a recuperare da incidenti di sicurezza in modo rapido ed efficiente, ripristinando l'infrastruttura e i dati colpiti dall'incidente.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Incident Response Plan (24x7)	La soluzione offerta dovrà aiutare e consentire all'AORN di definire un piano di azione e recupero in tempi brevissimi durante un attacco
Threat Hunting	La soluzione proposta deve essere in grado attuare dei meccanismi e delle azioni di *Threat Hunting*
Compromise Assessment	La soluzione proposta deve essere in grado di tracciare ed individuare gli *asset* compromessi durante un attacco

Tabella 12 - Requisiti minimi per la soluzione di Incident Response

Si richiede la fornitura di n.1 soluzione di *Incident Response*.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.1 licenze *Incident Response Medium*

5.1.12 Soluzione XDR

Si richiede la fornitura di una soluzione XDR (*Extended Detection and Response*) che integri i dati da una varietà di fonti, tra cui *endpoint*, rete, *cloud e e-mail*, per fornire una visibilità completa delle minacce e accelerare la risposta agli incidenti.

La soluzione proposta dovrà utilizzare meccanismi di intelligenza artificiale (AI) per correlare i dati da queste diverse fonti e identificare minacce che potrebbero non essere rilevabili da una singola soluzione. Ciò consentirà all'AORN di identificare e rispondere alle minacce più rapidamente e in modo più efficace.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. *Ingestione e correlazione:* la soluzione proposta dovrà fornire una visibilità completa delle minacce, combinando dati sugli eventi individuati sulle altre componenti dell'architettura di sicurezza, ed effettuare correlazione di tutti gli eventi per determinare gli incidenti di alto profilo che necessitano l'attenzione degli operatori di sicurezza;
2. *Prioritizzazione:* la soluzione proposta dovrà assegnare delle priorità degli incidenti basata su rischio e impatto per concentrare l'analista su ciò che deve essere affrontato con urgenza;
3. *Risposta agli incidenti accelerata:* La soluzione proposta dovrà essere in grado di generare una risposta automatizzata e guidata anche attraverso azioni suggerite che sono rilevanti per l'incidente oggetto di indagine;
4. *Orchestrazione e automazione:* la soluzione proposta dovrà permettere la creazione di *workflow* di integrazione con le varie soluzioni dell'architettura, in modalità *zero-code*, per permettere l'efficientamento delle operazioni di sicurezza nel contesto specifico attraverso azioni automatiche personalizzate;
5. *Migliore collaborazione:* la soluzione proposta dovrà aiutare gli analisti di sicurezza a collaborare in modo più efficace sugli incidenti di sicurezza, fornendo una piattaforma comune per condividere le informazioni e prendere decisioni.

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Visibilità unificata	La soluzione proposta deve unificare tutte le viste relative alle soluzioni di sicurezza proposte, correlando i dati e semplificando l'individuazione di minacce
Correlazione	La soluzione offerta correlare sfruttando meccanismi di threat intelligence, intelligenza artificiale ed analisi comportamentali tutti i dati derivanti dalle piattaforme firewall, ISE, IPS, protezione DNS ed altri
Automazione	La soluzione proposta dovrà avere meccanismi di automazione sulla risposta alle minacce e raccomandazioni e guide per le azioni guidate da operatore umano
Priorità	La soluzione proposta dovrà effettuare la prioritizzazione degli incidenti sulla base del livello di rischio e del valore dell'asset.

Tabella 13 - Requisiti minimi per la soluzione XDR

Si richiede la fornitura di n.1 soluzione XDR.
La **configurazione minima richiesta**, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.800 licenze *Advantage*.

5.1.13 Piattaforma IAM

Sistema IAM (Identity Access Management) dedicato per la gestione delle identità e degli accessi, al fine di garantire il corretto livello di permessi per il corretto accesso in rete ed agli applicativi aziendali, oltre a poter gestire tramite apposito portale il provisioning delle identità utente e delle piattaforme IoT.

Le principali funzionalità richieste da questa piattaforma sono sintetizzate di seguito:

- Reimpostazione autonoma delle password.
- Gestione sblocco account.
- Notifica scadenza password/account agli utenti.
- Single sign-on aziendale.
- Sincronizzatore di password.
- Accesso a Windows con l'autenticazione a due fattori.
- Aggiornamento delle informazioni personali su AD.
- Ricerca dei dipendenti nella directory.
- Cambio password in Active Directory.
- Gestione delle password attraverso dispositivo mobile
- Reimpostazioni password in Winlogon (CTRL+ALT+CANC)
- Autenticazione multifattore
- Sottoscrizione a gruppi di e-mail
- Personalizzazione desktop e app mobili
- Applicazione di criteri di password

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Gestione degli accessi	Deve garantire il controllo degli accessi ai sistemi o ai software attraverso metodi MFAo Single Sign-on
Integrazione con i Servizi di Directory	Deve integrarsi con sistemi di gestione delle identità Microsoft Active Directory e sistemi di posta elettronica quali Microsoft Exchange 2016 o superiore on-prem o Microsoft O365
Managing degli utenti	Deve consentire un portale di self service per le funzioni di reset password
Analytics delle identità	Deve utilizzare strumenti di Machine Learning per prevenire accessi anomali ai sistemi o ai software aziendali
Analytics delle identità	Deve utilizzare strumenti di Machine Learning per prevenire accessi anomali ai sistemi o ai software aziendali
Autenticazione con più fattori (MFA, Multi Factor Authentication	Deve utilizzare metodi di MFA per l'accesso, integrandosi con le più comuni piattaforme di rilascio quali ad es. Microsoft Authenticator, Google Authenticator etc.
Autenticazione basata su rischio	Deve utilizzare algoritmi per calcolare i rischi delle azioni degli utente. Blocca e segnala le azioni con punteggi di rischio elevati.

Tabella 14 - Requisiti minimi per la soluzione IAM

La configurazione minima richiesta, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- ❖ N.3.000 licenze

5.1.14 Piattaforma PAM

Sistema PAM (Privileged Access Management) dedicato al controllo e monitoraggio degli accessi con credenziali privilegiate, controllandone le sessioni e tenendone traccia in maniera sicura, le principali attività svolte dal sistema sono di proteggere le identità privilegiate quali gli Amministratori di sistema e in generale le utenze che accedono a dati sensibili, inserendole in repository a prova di manomissione.

Le caratteristiche principali della soluzione richiesta devono essere le seguenti:

1. Tracciabilità delle sessioni e protezione con password
2. Riduzione della superficie di attacco
3. Monitoraggio delle sessioni
4. Criptazione dei dati
5. Semplificazione di accesso dall'esterno
6. Principio del minimo privilegio
7. Rotazione delle password degli Account locali
8. Anti-Ransomware

9. Gestione centralizzata
10. Distribuire una struttura Zero- Trust
11. Identificazione unificata, sicura e semplificata
12. Reportistica per audit

La tabella seguente mostra le altre **caratteristiche minime richieste, pena esclusione**:

Caratteristica	Valore richiesto/minimo
Gestione delle credenziali privilegiate	Integrazione automatica delle credenziali privilegiate e dei segreti utilizzati dalle identità umane e non umane. Capacità di determinare quali utenti possano accedere a cosa
Gestione automatica per la rotazione delle password	Isola e monitora le sessioni. Registrazione degli eventi chiave e agli audit a prova di manomissione, registrazione di tutta l'attività durante la sessione stessa. Gli utenti finali non si collegano mai direttamente ai sistemi target. Salvataggio sicuro e centralizzato delle registrazioni delle sessioni.
Rilevamento delle minacce e reazione	Onboarding degli account privilegiati non gestiti e delle relative credenziali. Rilevazione dei comportamenti anomali, blocco o isolamento delle minacce grazie alle funzionalità di remediation basate sulle policy
Autenticazione MFA adattiva	Convalida delle sessioni degli utenti privilegiati mediante autenticazione a Multi Fattori

Tabella 15 - Requisiti minimi per la soluzione PAM

La configurazione minima richiesta, fermo restando le caratteristiche minime richieste in precedenza, è la seguente:

- N.500 licenze

5.2 Elenco del materiale da fornire

Per quanto espresso finora si richiede che la fornitura rispetti le caratteristiche richieste, pena esclusione.
La tipologia dei componenti selezionati, la descrizione e le quantità sono riassunte nella tabella che segue:

Part Number	Descrizione	Durata (mesi)	Qtà
CSEMAIL-SEC-SUB	Cisco Secure Email XaaS Subscription	36	1
CES-MA-ULTD-LIC	Cisco Secure Email Cloud Malware Analytics Unlimited License	36	1
CES-ADV-LIC	Cisco Secure Email Cloud Advantage, Essential+ GSU+DLP+ENC	36	2.000
CES-IMD-LIC	Cisco Internal Mailbox Defense License	36	2.000
SVS-EMAILC-SUP-P	Premium Support for Cisco Email Security	36	1
AMP4E-SEC-SUB	Cisco Secure Endpoint XaaS Subscription	36	1
SVS-AMPE-SUP-P	Cisco AMP for Endpoints Premium SW Service	36	1
AMP4E-PRE-CL-LIC	Cisco Secure Endpoint Premier Tier Subscription	36	800
TG-AMPADV-K9	Cisco Secure Malware Analytics Cloud for Endpoint Advantage	36	3
ISE-SEC-SUB	Cisco Identity Service Engine Subscription	36	1
SVS-ISE-SUP-E	Enhanced Support for Identity Service Engine Subscription	36	1
ISE-A-LIC	Cisco Identity Service Engine Advantage Subscription	36	3.000
R-ISE-VMC-K9=	Cisco ISE Virtual Machine Common PID	36	4
CON-ECMU-RISE9KVM	SWSS UPGRADES Cisco ISE Virtual Machine Common PID	36	4
L-ISE-TACACS-ND=	Cisco ISE Device Admin Node License	36	2
ST-SEC-SUB	Cisco Stealthwatch Enterprise XaaS Subscription	36	1
SVS-ST-SEC-SUP-P	Premium Support for Stealthwatch Security	36	1
ST-FR-LIC	Cisco Secure Network Analytics Flow Rate License	36	8.000
L-ST-SMC-VE-K9	Cisco Secure Network Analytics Mgmt Console Virtual Edition	36	1
L-ST-FC-VE-K9	Cisco Secure Network Analytics Flow Collector Virt Edition	36	1
L-LC-TI-FC2K=	Cisco Secure Network Analytics Threat Intelligence -FC2K Lic	36	1
L-LC-TI-FC2K-3Y	Cisco Secure Network Analytics Threat Intelligence 3Y FC2K	36	1
L-AC-APX-LIC=	Secure Client Premier Term License, Total Unique Users	36	500
L-AC-APX-3Y-S3	Cisco AnyConnect Apex License, 3YR, 250-499 Users	36	500
DUO-SUB	Cisco Duo subscription	36	1
SVS-DUO-SUP-P	Cisco Duo Premium Support	36	1
DUO-ADVANTAGE	Cisco Duo Advantage edition (formerly Access)	36	900
UMB-SEC-SUB	Cisco Umbrella Security Subscription	36	1
SVS-UMB-SUP-E	Enhanced Support for Umbrella	36	1
UMB-DNS-ADV-K9	Cisco Umbrella DNS Security Advantage	36	2.000
XDR-SEC-SUB	Cisco XDR	36	1
SVS-XDR-SUP-E	Enhanced Support Service for XDR	36	1
XDR-ADV	Cisco XDR Advantage Tier subscription	36	800
L-RDB-20M-LIC=	Bot Manager 20M - Yearly Subr	36	1
L-RDB-20M-3Y	Bot Manager 20M - 3Y Subr	36	1
L-RDCWE-ERTA-LIC=	Cloud WAF Enterprise - ERT Premium per Application	36	6
L-RDCWE-ERTA-3Y	Cloud WAF Enterprise - ERT Premium per Application	36	6
L-RDCWE-ERT-LIC=	Cloud WAF Enterprise - ERT Premium Add-on	36	1
L-RDCWE-ERT-3Y	Cloud WAF Enterprise - ERT Premium Add-on	36	1

L-RDCBT-5A-LIC=	Cloud Bot Manager - 10 additional policy add-on	36	2
L-RDCBT-5A-3Y	Cloud Bot Manager - 10 additional policy add-on - 3Y	36	2
RD-CWAF-BUN	Cisco Radware Cloud WAF Bundle	36	1
L-RDCWF-50M-LIC=	50M Cloud WAF Enterprise	36	1
L-RDCWF-50M-3Y	50M Cloud WAF Enterprise - 3Y	36	1
L-RDCWA-5A-LIC=	5 Application Add-On for Cloud WAF Enterprise	36	1
L-RDCWA-5A-3Y	5 Application Add-On for Cloud WAF Enterprise - 3Y	36	1
KENNA-SUB	Cisco Vulnerability Management Subscription	36	1
SVS-KENNA-SUP-E	Cisco Vulnerability Management Enhanced Support	36	1
SVS-KENNA-OB-P	Cisco Vulnerability Management Plus Onboarding	36	1
KENNA-VM	Cisco Vulnerability Management - Advantage	36	2.800
CTIR-SUB	Cisco Talos Incident Response Subscription	36	1
SVS-CTIR-M	Cisco Talos Incident Response Retainer - Medium	36	1
SVS-CTIR-CON	Service Contract for Cisco Talos Incident Response Retainer	36	1
Piattaforma **IAM** che sia rigorosamente compatibile con la tecnologia CISCO descritta in narrativa	1. per gestione 3.000 Utenti di Dominio; 2. per creazione per 3.000 Utenti di Dominio; 3. per supporto per 3.000 Utenti di Dominio; 4. *Multy Factor Authentication* per 3.000 Utenti di Dominio;	36	1
Piattaforma **PAM** che sia rigorosamente compatibile con la tecnologia CISCO descritta in narrativa	Licenze Piattaforma PAM per gestione amministratori di sistemi	36	50
VPF – Virtual Patching Firewall	Licenze aggiuntive Virtual Patching	36	6

Questa amministrazione accetterà anche una formulazione di proposta sotto forma di Enterprise Agreement, purché includa tutto quanto specificato nella tabella precedente.

5.3 Il servizio di Installazione e supporto al collaudo

Come anticipato, sarà obbligo del Fornitore prevedere la posa in opera di tutto quanto richiesto per il corretto funzionamento e collaudo delle soluzioni proposte.
A valle della fornitura il Fornitore dovrà:

1. realizzare tutte le azioni necessarie preliminari per l'avvio in esercizio della nuova infrastruttura di *Cybersecurity* quali, a titolo non esaustivo, installazione e configurazione dei prodotti individuati dal Fornitore, supportare l'AORN nella fase di collaudo del progetto, necessario all'erogazione del finanziamento.
2. interfacciare i nuovi apparati ai sistemi esistenti minimizzando i disservizi per l'utenza;
3. prevedere l'ottimizzazione degli spazi nei rack oggetto di installazione.

5.4 Garanzia

Tutti gli apparati devono essere coperti da garanzia per la durata di **n.36 mesi** solari a partire dallo startup del progetto. La garanzia dovrà essere registrata a nome della Stazione Appaltante e non dovrà appoggiarsi a contratti globali siglati da terzi.

6 Informazioni generali sulla fornitura

6.1 Base d'asta

La base d'asta dell'appalto per la fornitura di hardware, licenze software e servizi di installazione e configurazione per il potenziamento dell'infrastruttura di Cybersecurity dell'AORN Santobono Pausilipon è pari ad **€ 2.919.915,91 oltre IVA, € 3.562.297,41 IVA compresa.**

6.2 Obblighi di tipo generale

Il Concorrente dovrà essere un reseller CISCO® **almeno GOLD Partner**, riconosciuto dalla Casa Madre CISCO, **pena l'esclusione**.
I prodotti forniti dovranno essere:

1. Prodotti originali recanti il marchio di fabbrica del costruttore;

2. Prodotti nuovi nel loro packaging originale, e saranno acquistati e licenziati tramite Canali Autorizzati dal costruttore e specificatamente per il cliente Azienda Ospedaliera Santobono-Pausilipon, che sarà la prima acquirente dei prodotti e prima licenziataria di qualsiasi copia di Software, compreso quello incluso dei prodotti;
3. La ditta aggiudicataria si impegna a fornire licenze software originali rilasciate per l'Azienda Ospedaliera Santobono-Pausilipon ed apparati idonei allo scopo;
4. La ditta aggiudicataria non potrà fornire materiali di provenienza illegale, o prodotti usati e rigenerati o prodotti provenienti da mercati paralleli;
5. L'AORN, in caso qualsiasi necessità legata ad ispezioni e/o controlli da enti terzi, non dovrà essere messa in condizioni di dover pagare:
    a. Tariffe di ispezione dei prodotti del costruttore
    b. Tariffe di relicenziamento del software aggiuntive, che in ogni caso dovranno essere pagate dal fornitore, fatto salvo il diritto di maggior danno della Azienda Ospedaliera Santobono-Pausilipon di contro la ditta aggiudicataria;

L'AORN, a tutela dei propri interessi, si riserva comunque di effettuare verifiche dirette con la Casa Madre e di richiedere alla Ditta Aggiudicataria conferma scritta di quanto sopra e/o dichiarazione scritta dalla Casa Madre.

6.3 Obblighi di tipo particolare

Questo progetto sarà finanziato dal POR Campania FESR 2014-2020 solo se verrà rispettato il suo cronoprogramma che prevede, quale data ultima per il collaudo e successivo relativo pagamento quietanzato della fornitura, il 15/12/2023.

Per tale milestone si auspica che la fornitura di tale appalto debba avvenire entro e non oltre il 15/11/2023 per garantire le successive installazioni, configurazioni, e collaudi. Consegne oltre tale data potrebbero pregiudicare il finanziamento.

Il concorrente che vorrà partecipare a tale gara di appalto dovrà quindi essere confidente circa la conclusione positiva della fornitura nel suo complesso entro una data utile per espletare, dopo la fornitura, l'installazione ed il collaudo per ciascuna delle voci, per consentire all'AORN di emettere entro un tempo utile il pagamento del dovuto e di riportare gli esiti alla Regione Campania, erogatore del finanziamento.

6.4 Penali

Il mancato rispetto delle tempistiche di cui al punto precedente non consentirà all'AORN di accedere al finanziamento e, di conseguenza, comporterà l'escussione della cauzione e la restituzione dell'intera fornitura all'aggiudicatario che non avrà nulla a pretendere. Questa Amministrazione, infatti, non ha nella sua disponibilità a bilancio aziendale il valore economico necessario.

6.5 Modalità dell'offerta

Il Concorrente, in fase di offerta, dovrà esprimere un unico ribasso alla base d'asta posta a gara.

6.6 Sedi e riferimenti amministrativi e tecnici

Le sedi dell'AORN presso cui consegnare l'hardware ed installare le licenze software, secondo le disposizioni del Direttore di Esecuzione del contratto (DEC), sono riportate di seguito:

1. **Presidio Santobono** – Via Mario Fiore, 6 – 80127 Napoli. Il CED si trova presso il piano rialzato del Padiglione Ravaschieri.
2. **Presidio Pausilipon** – Via Posillipo 226 – 80122 Napoli. Il CED si trova al livello -2 rispetto all'ingresso principale.
3. **Sede Amministrativa** – Via Teresa Ravaschieri, 8 – 80122 Napoli. Il CED si trova al piano terra della palazzina centrale.

Il RUP dell'appalto è l'ing. Ornella De Cristofaro
Il DEC dell'appalto è il Geom. Alessandro Orlando

Il Direttore della UOC Tecnico Patrimoniale e ICT
Ing. Gennaro Sirico