POR CAMPANIA FESR 2014-2020

ASSE 2 "ICT E AGENDA DIGITALE"

OBIETTIVO SPECIFICO 2.2 "DIGITALIZZAZIONE DEI PROCESSI AMMINISTRATIVI E DIFFUSIONE DI SERVIZI DIGITALI PIENAMENTE INTEROPERABILI"

AZIONE 2.2.1 "SOLUZIONI TECNOLOGICHE PER LA DIGITALIZZAZIONE E L'INNOVAZIONE DEI PROCESSI INTERNI DEI VARI AMBITI DELLA PUBBLICA AMMINISTRAZIONE NEL QUADRO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ"

SCHEDA PROGETTO

PROGETTO DA AVVIARE **X**
PROGETTO IN CORSO **o**

SOGGETTO PROPONENTE	AORN SANTOBONO PAUSILIPON	
P.IVA	06854100630	
PEC	santobonopausilipon@pec.it	
REFERENTE PROGETTO	Ing. Gennaro Sirico	Mail: g.sirico@santobonopausilipon.it
		Telefono: 081 220 5266

TITOLO DEL PROGETTO
CYBER+ - Sicurezza informatica AORN Santobono Pausilipon

DESCRIZIONE DEL PROGETTO, CON EVIDENZA DEGLI ELEMENTI DI COERENZA CON LA DGR N. 354 DEL 19/06/2023 E CON L'AZIONE 2.2.1 DEL POR CAMPANIA FESR 2014-2020

1 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 sistemi per la sicurezza informatica, che per la maggior parte sono in comodato d'uso forniti mediante apposita sottoscrizione dell'accordo quadro CONSIP SPC2 connettività con la Fastweb SpA, è di seguito descritta nelle sue caratteristiche e rappresentata sinteticamente:

Premesso che, le linee guida relative alla sicurezza degli account utenti aziendali attualmente implementate su tutti i sistemi del dominio Active Directory dell'AORN Santobono Pausilipon sono:

a. Ogni utente aziendale è provvisto di una username, password e indirizzo e-mail personale.
b. Le password di dominio per gli account utenti hanno le seguenti configurazioni:
    - Scadenza ogni 90gg
    - Lunghezza password almeno 10 caratteri
    - Precedenti password ricordate: 10
    - Complessità password abilitata
    - Blocco dell'account dopo 10 tentativi falliti
    - Sblocco dell'account dopo intervento Amministrativo
c. I tecnici delle ditte esterne che devono operare all'interno della rete aziendale vengono identificati già durante la creazione dell'identità di rete con il suffisso *".guest"* apposto al loro nome, in base alle informazioni ricevute dall'ufficio richiedente l'account viene generato con una scadenza pre-impostata e ricevono delle regole di password più restrittive, che sono:
    - Scadenza ogni 60gg
    - Lunghezza password almeno 14 caratteri
    - Precedenti password ricordate: 24
    - Complessità password abilitata
    - Blocco dell'account dopo 5 tentativi falliti
    - Sblocco dell'account dopo intervento Amministrativo
d. Nessuno degli account utenti del personale medico è membro dei gruppi amministrativi di sistema, solo specifici utenti del reparto ICT sono membri del gruppo Domain Admins, Enterprise Admins, e Local Administrators group
e. L'account Administrator locale è disabilitato, e viene creato un account di servizio con privilegi amministrativi locale per accedere in ogni evenienza sui sistemi.
f. L'accesso alle risorse di rete condivise avviene sempre tramite permessi espliciti, e sono deprecati tutti gli accessi mediante uso di gruppi dalla membership non gestibile quali:

- Everyone
- Authenticated Users
- Domain Users

E che per la sicurezza dei dati, inclusi le basi dati, i documenti e le cartelle informatiche, le politiche di backup e le relative regole di conservazione sono:

Descrizione delle politiche di backup

L'attuale configurazione dei backup dei dati prevede il seguente processo:

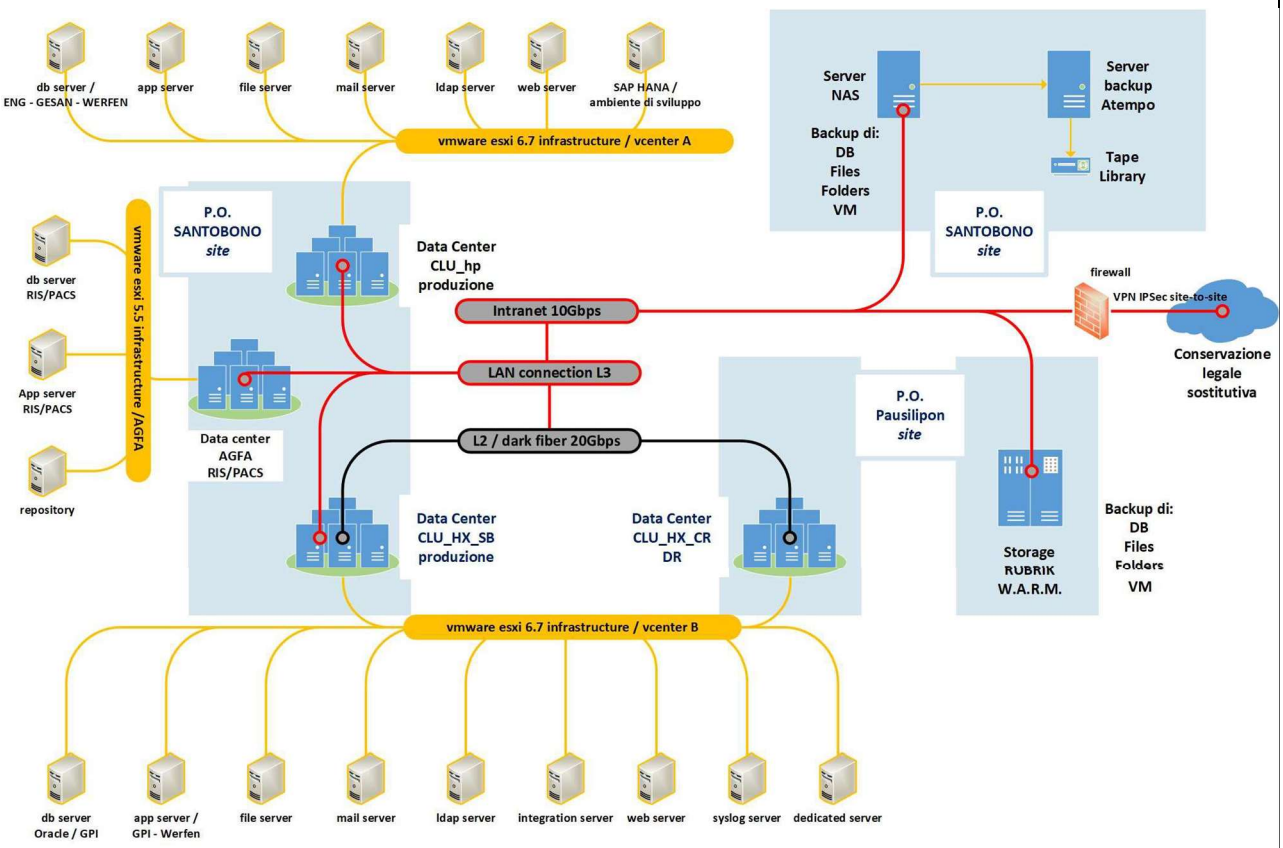
1) Ogni sistema server invia mediante servizio locale di backup i dati da esso gestiti, siano db o file contenuti in apposite cartelle, ad un repository di rete centrale NAS.
2) Nel caso dei documenti condivisi, sono abilitate sia sul server che ospita il servizio e sia sul NAS le funzioni di shadow copy dei dati, con retention di oltre 1 mese.
3) Il server di backup, con il sistema Atempo (TINA Backup) collegato alla tape library esegue il backup dei seguenti dati presenti sul NAS server con una retention di 14 gg:
    a. Cartelle contenenti i backup dei singoli db
    b. Cartelle contenenti i backup delle cartelle condivise e dei files
    c. Mailbox in formato .pst esportate singolarmente (solo per le mailbox prioritarie)
    d. Direttamente dal server di posta Exchange esegue il backup dei db presenti (al momento 3 db)
4) Il NAS server esegue anche il backup di alcune *virtual machine* strategiche, che sono:
    a. Server Active Directory PDC
    b. Server di posta elettronica
    c. Server Registro Tumori
    d. Server Wirgilio (ex cartella clinica), 5 servers
5) Server Rubrik per il backup di tutti i dati e di alcuni virtual server presenti in azienda all'interno di un'area sicura non accessibile, secondo logica WORM (Write Once Read Many) mediante strategia di backup incrementale continuo.

    I sistemi messi sotto backup sono:
    a. I principali server presenti nei tre data center aziendali
    b. Tutti i dati presenti sui file server
    c. Tutti i db esportati su NAS

    Lo storage al momento è di 60TB in linea ed è gestito da quattro server boxed in HA (High Availability) iperconvergenti.

    L'accesso ai dati avviene mediante autenticazione a due fattori e con il consenso di due account amministrativi contemporanei, la soluzione non è in dominio per evitare che in caso di compromissione degli account amministrativi centrali si possa superare questo controllo.
6) Tutti i dati provenienti dalle diagnostiche per immagini, compresi i referti, vengono archiviati e salvati sul data center AGFA del RIS/PACS, e ne viene inviata copia mediante link VPN\IPSec site-to-site in cloud Telecom per l'archiviazione legale sostitutiva.

Il design operativo è il seguente:



Per quanto concerne la sicurezza perimetrale e degli accessi, gli apparati e servizi presenti, il relativo diagramma operativo è:

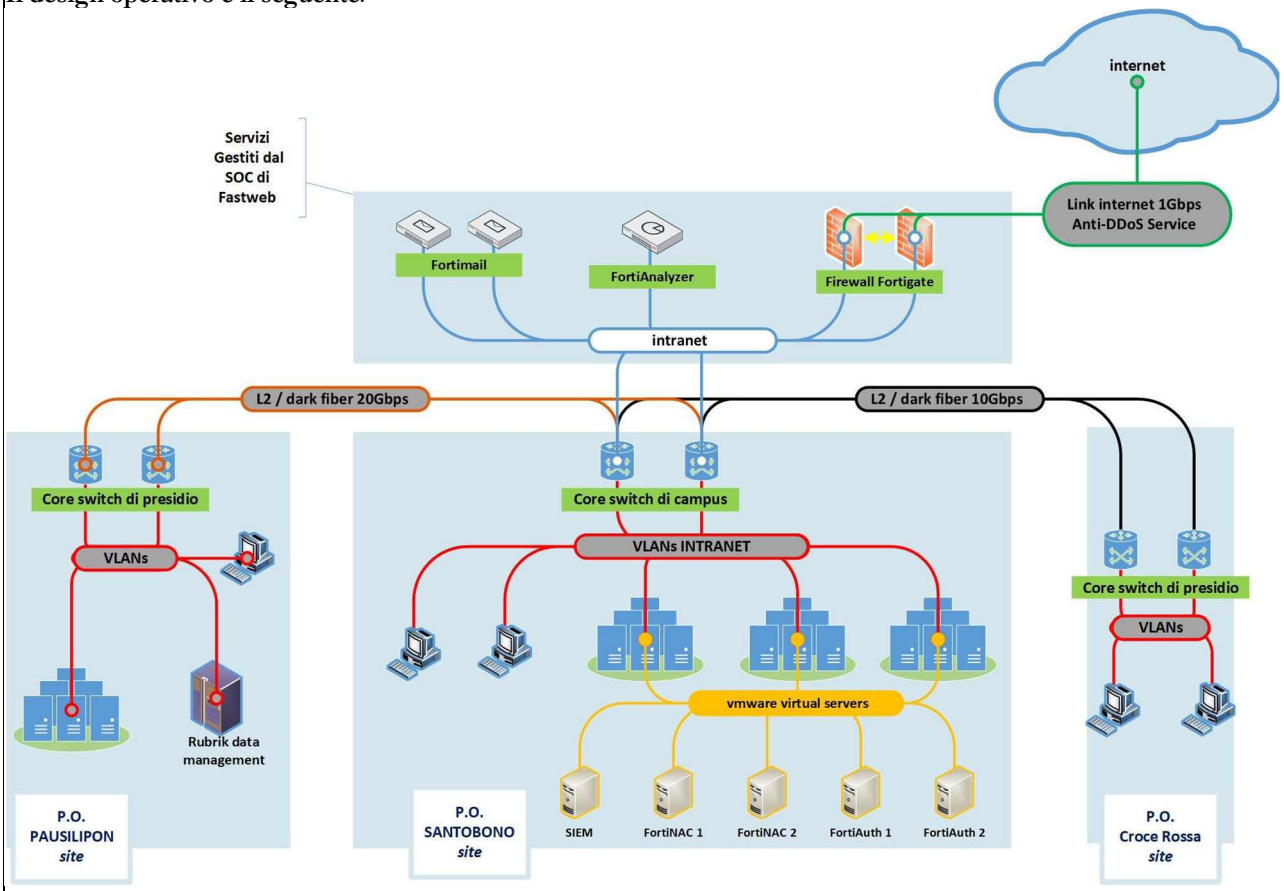
Per quanto riguarda i sistemi di sicurezza implementati al momento si evidenzia nella seguente tabella il tipo, la funzione e se in Alta Affidabilità (HA).

apparato	funzione	HA
Fortigate 501E (in comodato d'uso con l'AQ SCP2 – scaduto in proroga)	Firewall di rete perimetrale con funzionalità IPS / IDS e WAF abilitate. La sua funzione principale, oltre a difendere la rete interna dal traffico dati proveniente da Internet è quella di filtrare il traffico web, inibendo l'accesso ai siti ed ai contenuti malevoli.	SI
Fortimail (in comodato d'uso con l'AQ SCP2 – scaduto in proroga)	AntiSPAM aziendale, il compito di questa appliance è quello di limitare e filtrare la ricezione di e-mail identificate come SPAM, oltre che evitare che i nostri server di posta possano essere usati per inviare e-mail di SPAM in internet.	SI
FortiAnalyzer (in comodato d'uso con l'AQ SCP2 – scaduto in proroga)	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.	NO
SIEM / QRadar (in comodato d'uso con l'AQ SCP2 – scaduto in proroga)	Security information and event management, è un sistema che ha come obiettivo la raccolta centralizzata dei log e degli eventi generati da applicazioni e sistemi in rete. Grazie al machine learning le attività di correlazione e monitoraggio consentono di poter individuare possibili vulnerabilità dei sistemi operativi/software e potenziali data breach.	NO
FortiNAC (acquistato mediante gara MEPA)	Sistema di controllo degli accessi nella rete aziendale. Scopo di questo servizio è quello di monitorare tutti gli apparati di rete attivi (switch ed access point wireless), controllando tutti gli accessi alla rete da parte di computer o in generale di apparecchiature informatiche, applicando all'occorrenza regole restrittive nel caso di device non riconosciuti.	SI

Rubrik (acquistato mediante gara MEPA)	Sistema di backup dati, in modalità WORM (Write Once Read Many) per la messa in sicurezza e la protezione da eventuali attacchi di tipo Ransomware o di cancellazione dei backup. L'accesso alle appliance dedicate avviene solo mediante autenticazione a due fattori eseguita da due Amministratori concorrenti. Il salvataggio dei dati, delle vm e dei data base avviene secondo una logica di backup incrementale continuo.	SI

A difesa dai possibili attacchi di Distribuited Denial of Service (DDoS) è stato abilitato sul link internet di connessione alla rete aziendale, un servizio di Anti-DDoS, direttamente dal ISP Fastweb.

Il design operativo è il seguente:



Per quanto concerne la connettività, si precisa che tutti link di connessione della AORN Santobono Pausilipon sono ridondati, sia a livello di apparati di connessione alla rete (router e/o switch) sia dal punto delle connessioni, con cavi che seguono percorsi differenti e si attestato in centrali differenti.
Questo al fine di garantire la massima sicurezza possibile in caso di guasto.

2 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, oltre al fatto che molti dei servizi attualmente in uso sono ormai scaduti e dovranno essere ritirati dalla ditta fornitrice, lasciando così scoperte aree critiche per la sicurezza informatica aziendale, motivo per il quale il progetto che si vuole realizzare, a seguito dell'analisi dei fabbisogni effettuata, prevede l'inserimento di specifiche soluzioni hardware e software esclusivamente dedicate alla sicurezza delle seguenti aree:

- Sicurezza dei servizi WEB aziendali esposti verso il mondo esterno
- Sicurezza dei sistemi Elettromedicali e IoT
- Sicurezza degli accessi e gestione delle identità
- Sicurezza dei dispositivi.

Lo scenario tecnico informatico aziendale, dopo un'attenta analisi ha difatti evidenziato che:

- I sistemi informatici e informativi sono per lo più gestiti da ditte esterne, che operano con tecnici che condividono credenziali e identità amministrative (account administrator) su specifici sistemi.
- Che tali tecnici, per quanto da noi censiti non sono tracciabili nel loro operato.
- Che, sempre i servizi di assistenza, sono spesso composti da gruppi di tecnici dislocati anche geograficamente su più continenti, e non è possibile gestirli, questo per la natura stessa dei servizi offerti
- Tutti i consulenti esterni non hanno la possibilità di gestire le proprie credenziali di accesso, che essendo per regolamento temporanee, gravano come attività di assistenza sui sistemi interni.
- Tutti i sistemi IoT o Elettromedicali non sono patchabili o non è possibile proteggerli mediante i sistemi antivirus aziendali; pertanto, sono fortemente vulnerabili e spesso indicati nei nostri log come compromessi.
- La gestione delle informazioni e dei log derivanti dai molteplici sistemi aziendali non essendo centralizzata è di difficile utilizzo e non consente la possibilità di eseguire incroci dei dati per un'analisi più precisa.
- Non è possibile ad oggi proteggere in maniera forzata sui vari sistemi presenti account con privilegi particolari tramite l'utilizzo di sistemi di autenticazione a più fattori (MFA).

Questa analisi dei fabbisogni eseguita dall'AORN ha difatti evidenziato, in base all'opportunità del finanziamento POR FESR 2014-2020, la possibilità di acquisire software o appliance per risolvere tutti i problemi sopra elencati e per coprire aree relative alla sicurezza informatica affidate a contratti di comodato d'uso di hardware e di licenze ad oggi scaduti e in proroga tecnica.

Dall'analisi dei fabbisogni emerge che le soluzioni necessarie a garantire all'AORN un altissimo tasso di sicurezza informatica sono le seguenti:

1. Soluzione Firewall IPS/IDS - Firewall IPS (*Intrusion Prevention System*), progettata per fornire una difesa proattiva contro le minacce informatiche e proteggere le reti aziendali da intrusioni e attacchi malevoli. La soluzione deve operare tramite intelligence sulla minaccia con rilevazione delle intrusioni in tempo reale per identificare e prevenire attacchi particolarmente avanzati.
2. Soluzione di controllo Accessi *Identity Service Engine* - La soluzione di controllo Accessi Identity Service Engine è una soluzione indispensabile 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.
3. Soluzione VPN - Sistema per le 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.
4. Soluzione di Secure Network Analytics - Soluzione di controllo del cosiddetto traffico orizzontale ed interno, cioè di Secure Network Analytics.
   La soluzione garantirà un'avanzata analisi della rete e sarà 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.
5. Soluzione di *Multi Factor Authentication* - Sistema per il 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.
6. Soluzione di *Protezione End Point e Vulnerability Assesment* - Soluzione di protezione degli *End Point e Vulnerability Assessment* 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.
7. Soluzione di *Vulnerability Management* - Sistema 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 scanner e feed di intelligence sulle minacce.
8. Soluzione di *Secure E-mail* - 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.
9. Soluzione di Protezione host via DNS (Cisco Umbrella) - Sistema 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 e che non necessiti di modifiche infrastrutturali.
10. Soluzione WAF - Sistema WAF (*Web Application Filtering*) per la protezione avanzata delle applicazioni web basata su cloud. La soluzione deve fornire una difesa robusta e scalabile per le applicazioni web, proteggendole da attacchi

informatici e garantendo la sicurezza dei dati.

11. Soluzione di *Incident Response* - Sistema 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.
12. Soluzione XDR - Sistema 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 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.
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.
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.

Tutte le soluzioni riportate si integreranno nel sistema di gestione della sicurezza informatica aziendale, introducendo nuove funzionalità o reintegrando prodotti e licenze ad oggi non più coperti da contratto.
Per quanto esposto finora risulta evidente che tutte le forniture hardware e software dovranno, 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.

3 Descrizione del Progetto

L'architettura prescelta

L'architettura prescelta è quindi quella relativa alla protezione della rete, protezione degli utenti/end point, ove per end point si evidenziano quei dispositivi medicali che non possono essere modificati, protezione da 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 propria 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 *remendation* 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 progettuali che assolvono al fabbisogno aziendale:

4 Soluzione Firewall IPS/IDS

Acquisto di una soluzione *Firewall* IPS (*Intrusion Prevention System*), progettata per fornire una difesa proattiva contro le minacce informatiche e proteggere le reti aziendali da intrusioni e attacchi malevoli. La soluzione deve operare tramite *intelligence* sulla minaccia con rilevazione delle intrusioni in tempo reale per identificare e prevenire attacchi particolarmente avanzati. Le caratteristiche principali devono essere:

1. *Rilevazione delle intrusioni avanzata:* la soluzione deve utilizzare un'ampia gamma di metodi di rilevazione, disporre di un'ampia numerosità di signature aggiornate costantemente dal vendor, ma allo stesso tempo permettere la creazione di signature personalizzate per proteggere al meglio il contesto specifico;
2. *Discovery:* Discovery passivo dei sistemi operativi e applicazioni presenti in rete e tuning automatizzato delle regole IPS basandosi sulle informazioni raccolte dalla rete, con l'obiettivo di semplificare l'*operation* della soluzione
3. *Blocco e prevenzione delle intrusioni:* Una volta rilevata una minaccia, *il Firewall* deve poter intraprendere azioni immediate per bloccare l'attacco e impedire che si diffonda nella rete, proteggendo i dispositivi e i dati aziendali critici;
4. *Integrazione con l'ecosistema di sicurezza:* deve essere parte integrante dell'architettura di sicurezza espressa nei paragrafi precedenti, consentendo una gestione centralizzata e una collaborazione con altre soluzioni, le knowledge base di *Threat Intelligence*, per una protezione completa della rete;
5. *Intelligence sulla minaccia in tempo reale:* deve possedere funzionalità di *threat intelligence* sulle minacce aggiornate costantemente per identificare nuove varianti di malware e attacchi emergenti, garantendo una protezione efficace contro le minacce in evoluzione deve essere possibile l'integrazione anche con *Threat Intelligence* di terze parti attraverso protocollo STIX/TAXII
6. *Analisi forense avanzata:* La soluzione deve avere funzionalità di analisi forense avanzate, consentendo agli amministratori di investigare gli attacchi passati, analizzare le cause principali e prendere misure preventive per migliorare la sicurezza complessiva della rete;
7. *Reporting e visibilità:* deve fornire una panoramica completa delle attività di sicurezza, consentendo agli amministratori di ottenere una visione chiara degli eventi di sicurezza, generare report dettagliati e ottenere una comprensione approfondita delle minacce e delle violazioni di sicurezza.
8. *Traffico cifrato:* la soluzione deve essere in grado di decifrare il traffico cifrato TLS. Allo stesso tempo, non essendo possibile per motivi di privacy la decifratura di tutto il traffico, la soluzione deve poter essere in grado di identificare il traffico malevolo anche nel traffico cifrato, senza necessità di decifrarlo.

In sintesi, la soluzione *Firewall* individuata da questa AORN deve possedere una difesa proattiva e robusta contro le intrusioni e gli attacchi informatici, utilizzando un'ampia gamma di tecniche di rilevazione e prevenzione, integrazione con altre soluzioni e aggiornamenti costanti dell'intelligence sulle minacce.

La tabella seguente mostra le altre **caratteristiche minime:**

Caratteristica	Valore richiesto/minimo
Throughput FW+AVC+IPS	La soluzione deve supportare un throughput di almeno 33 Gbps
Sessioni concorrenti	La soluzione deve supportare un numero di sessioni concorrenti pari ad almeno 15 Milioni di sessioni
Throughput NGIPS	La soluzione deve supportare un throughput di almeno 33 Gbps
IPSec VPN Throughput	La soluzione deve supportare un throughput di almeno 12,5 Gbps
Management centralizzato	La soluzione deve prevedere una console di management centralizzato
Application e Visibility Control (AVC)	La soluzione deve avere funzionalità di *Application e Visibility Control* fino a 4.000 applicazioni diverse. Deve altresì avere funzionalità di visibilità geolocalizzate, di visibilità di utenti e di siti web
Security Instances	La soluzione deve supportare la capacità di instaurare sullo stesso HW istanze multiple con una scalabilità almeno pari a 7 istanze per piattaforma, a ciascuna istanza deve essere possibile allocare risorse computazionali (CPU, RAM, HD) dedicate.
High Availability	La soluzione deve prevedere architetture di alta affidabilità
Clustering	La soluzione deve prevedere la possibilità di mettere in cluster le appliance fino a 16 unità

Tabella 1.1 - Requisiti minimi per la soluzione Firewall

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

- Doppio alimentatore;
- Licenze per funzionalità di *Threat Defense*, *Malware* ed *URL filtering* per 36 mesi;
- N.4 ottiche a 1Gb in fibra GLC-SX-MMD=
- N.4 ottiche a 10Gb in fibra SFP-10G-SR-S=
- N.1 ottiche a 1Gb in rame GLC-TE

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
hardware: N. 6 Cisco Firepower 4115 con sistema di Management Firepower Management Center	386.657,28 €	85.064,60 €	471.721,88 €
licenze: N. 6 Licenze aggiuntive Virtual Patching	287.940,63 €	63.346,94 €	351.287,57 €
Installazione: Installazione per Cisco Firepower 4115 e Virtual Patching	58.760,00 €	12.927,20 €	71.687,20 €

Tabella 1.2 - Requisiti minimi per la soluzione Firewall

4.1 Soluzione di controllo Accessi *Identity Service Engine*

La soluzione di controllo accessi alla rete e di *Identity Service Engine*, è una soluzione indispensabile 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 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 deve poter dialogare con i dispositivi di LAN, WiFi e WAN per coordinare le operazioni di "*Policy Enforcement*" attraverso la tecnologia *Cisco TrustSec, tecnologies* 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**:

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 deve essere il controller di segmentazione che semplifica la gestione delle regole di switch, router, wireless e firewall.

Tabella 2.1 - Requisiti minimi per la soluzione ISE

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

- Soluzione virtualizzata e virtualizzabile su piattaforma *Vmware 6.7 o superiore*;
- N.3.000 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 3.000 licenze Identity Service Engine Advantage	115.769,94 €	25.469,39 €	141.239.33 €
Installazione: Installazione per licenze Identity Service Engine Advantage	14.164,43 €	3.116,17 €	17.280,60 €

Tabella 2.2 - Requisiti minimi per la soluzione ISE

4.2 Soluzione VPN

Sistema per le 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 **Firewall**.
È necessario che la soluzione abbia 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**:

Caratteristica	Valore richiesto/minimo
Integrazione	La soluzione deve essere integrabile con la piattaforma *Firewall* 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 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 3.1 - Requisiti minimi per la soluzione 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

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 300 licenze Cisco Secure Client Premier	4.452,69 €	979,59 €	5.432,28 €
Installazione: Installazione per licenze Cisco Secure Client Premier	3.714,29 €	817,14 €	4.531,43 €

Tabella 3.2 - Requisiti minimi per la soluzione VPN

4.3 Soluzione di *Secure Network Analytics*

Soluzione di controllo del cosiddetto traffico orizzontale ed interno, cioè di *Secure Network Analytics*.
La soluzione garantirà un'avanzata analisi della rete e sarà 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 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:* 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 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**:

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 4.1 - Requisiti minimi per la 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*

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 8.000 licenze Cisco Secure Network Analytics Flow Rate	259.740,26 €	57.142,86 €	316.883,12 €
Installazione: Installazione per licenze Cisco Secure Network Analytics Flow Rate	19.680,14 €	4.329,63 €	24.009,77 €

Tabella 4.2 - Requisiti minimi per la soluzione Security Network Analytics

4.4 Soluzione di *Multi Factor Authentication*

Sistema per il *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**:

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 5.1 - Requisiti minimi per la soluzione MFA

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

- N.300 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 300 licenze Cisco Duo Advantage	111.317,25 €	24.489,80 €	135.807,05 €
Installazione: Installazione per licenze Cisco Duo Advantage	30.711,57 €	6.756,55 €	37.468,12 €

Tabella 5.2 - Requisiti minimi per la soluzione MFA

4.5 Soluzione di Protezione *End Point e Vulnerability Assesment*

Soluzione di protezione degli *End Point e Vulnerability Assessment* 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**:

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 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 consentano di eseguire rapidamente interrogazioni complesse su uno o tutti gli *endpoint*.

Tabella 6.1 - Requisiti minimi per la soluzione Protezione degli End Point

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

- N.1000 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 1.000 licenze Premier Cisco Secure End Point	182.560,30 €	40.163,27 €	222.723,56 €
Installazione: Installazione per licenze Premier Cisco Secure End Point	41.743,00 €	9.183,46 €	50.926,46 €

Tabella 6.2 - Requisiti minimi per la soluzione Protezione degli End Point

4.6 Soluzione di *Vulnerability Management*

Sistema 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**:

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 7.1 - Requisiti minimi per la soluzione Vulnerability Management

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

- N.2.800 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 2.800 Cisco Kenna Vulnerability Management Advantage	192.949,91 €	42.448,98 €	235.398,89 €
Installazione: Installazione per Cisco Kenna Vulnerability Management Advantage	11.230,14 €	2.470,63 €	13.700,77 €

Tabella 7.2 - Requisiti minimi per la soluzione Vulnerability Management

4.7 Soluzione di *Secure E-mail*

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 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 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 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 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 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**:

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 8.1 - Requisiti minimi per la soluzione Secure E-mail

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

- N.2.000 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 2.000 licenze Cisco Secure Email Advantage	271.614,10 €	59.755,10 €	331.369,20 €
Installazione: Installazione per licenze Cisco Secure Email Advantage	23.171,57 €	5.097,75 €	28.269,32 €

Tabella 8.2 - Requisiti minimi per la soluzione Secure E-mail

4.8 Soluzione di Protezione *host* via DNS

Sistema 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 la soluzione si basi sull'analisi del DNS, essendo questa una componente cruciale dell'accesso ad Internet, la soluzione deve poter consentire un enforcement, rapido, trasparente per l'utente, e privo di latenza. La soluzione deve poter essere realizzata 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. La soluzione 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**:

Caratteristica	Valore richiesto/minimo
No hardware	La soluzione deve essere attivata puntando il DNS autoritativo, e/o i *proxy* in uso verso i data center del fornitore, senza necessità di installare *hardware* aggiuntivo.
Copertura mondiale	La soluzione dovrà appoggiarsi su una rete di *data center* globale esterna. Si richiede difatti una copertura globale da parte della *Threat Intelligence*.
Indipendenza di protocollo	La soluzione deve essere in grado di rilevare le minacce recate da malware avanzato, indipendentemente dalla porta o dal protocollo utilizzato.
RFC 1918	La soluzione 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 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	La soluzione fa uso di intelligenza predittiva e non utilizza solo *signature* o *blacklist* statiche.

Tabella 9.1 - Requisiti minimi per la soluzione Protezione host via DNS

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

- N.2.000 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 2.000 licenze Cisco Umbrella Advantage	253.803,34 €	55.836,73 €	309.640,07 €
Installazione: Installazione per licenze Cisco Umbrella Advantage	14.697,43 €	3.233,43 €	17.930,86 €

Tabella 9.2 - Requisiti minimi per la soluzione Protezione host via DNS

4.9 Soluzione WAF

Sistema WAF (*Web Application Filtering*) per la protezione avanzata delle applicazioni web basata su cloud. La soluzione 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 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 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 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 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 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 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.

La tabella seguente mostra le altre **caratteristiche minime richieste**:

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

Tabella 10.1 - Requisiti minimi per la 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

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 10 licenze Application Cisco Radware Cloud WAF	252.319,11 €	55.510,20 €	307.829,31 €
Installazione: Installazione per licenze Application Cisco Radware Cloud WAF	16.188,71 €	3.561,52 €	19.750,23 €

Tabella 10.2 - Requisiti minimi per la soluzione WAF

4.10 Soluzione di *Incident Response*

Sistema 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 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 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 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**:

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

Tabella 11.1 - Requisiti minimi per la 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*

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 36 licenze Cisco Incident Response	237.476,81 €	52.244,90 €	289.721,71 €
Installazione: Installazione per N. 36 licenze Cisco Incident Response	59.369,20 €	13.061,22 €	72.430,42 €

Tabella 11.2 - Requisiti minimi per la soluzione di Incident Response

4.11 Soluzione XDR

Sistema 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 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 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 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 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 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 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.
6.

La tabella seguente mostra le altre **caratteristiche minime richieste**:

Caratteristica	Valore richiesto/minimo
Visibilità unificata	La soluzione deve unificare tutte le viste relative alle soluzioni di sicurezza, correlando i dati e semplificando l'individuazione di minacce
Correlazione	La soluzione 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 dovrà avere meccanismi di automazione sulla risposta alle minacce e raccomandazioni e guide per le azioni guidate da operatore umano
Priorità	La soluzione dovrà effettuare la prioritizzazione degli incidenti sulla base del livello di rischio e del valore dell'asset.

Tabella 12.1 - Requisiti minimi per la soluzione XDR

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

- N.800 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 800 Cisco XDR (Secure-X)	222.634,51 €	48.979,59 €	271.614,10 €
Installazione: Installazione per Cisco XDR (Secure-X)	9.939,43 €	2.186,67 €	12.126,10 €

Tabella 12.2 - Requisiti minimi per la soluzione XDR

4.12 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**:

Caratteristica	Valore richiesto/minimo
Gestione degli accessi	Deve garantire il controllo degli accessi ai sistemi o ai software attraverso metodi MFA o 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
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 13.1 - Requisiti minimi per la soluzione IAM

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

- ❖ N.3000 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 1 Piattaforma IAM per 3000 user	38.038,40 €	8.368,45 €	46.406,85 €
Installazione: Installazione per Piattaforma IAM per 3000 user	9.224,43 €	2.029,37 €	11.253,80 €

Tabella 13.2 - Requisiti minimi per la soluzione IAM

4.13 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**:

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 14.1 - Requisiti minimi per la soluzione PAM

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

- N.500 licenze

La tabella seguente mostra le **caratteristiche economiche:**

DESCRIZIONE	IMPONIBILE	IVA	IMPORTO COMPLESSIVO
licenze: N. 1 Piattaforma PAM per 500 sistemi target	211.548,03 €	46.540,57 €	258.088,60 €
Installazione: Installazione per Piattaforma PAM per 500 sistemi target	23.916,29 €	5.261,58 €	29.177,87 €

Tabella 14.2 - Requisiti minimi per la soluzione PAM

OBIETTIVI DEL PROGETTO E RISULTATI ATTESI

Premesso che l'inserimento delle soluzioni hardware e software sopra citate nella descrizione del progetto, incrementeranno di molto la sicurezza informatica aziendale; gli obiettivi che ci si propone di raggiungere e i relativi risultati sono:

- 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.
- Innalzamento del livello di protezione del traffico di rete 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.
- Protezione di tutti gli apparati 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 oggi motivo di vulnerabilità per i sistemi informatici aziendali.
- Miglioramento del sistema di controllo delle versioni e delle vulnerabilità degli apparati informatici, applicando in automatico quelle che sono le necessarie azioni per evitarne la compromissione.
- Gestione semplificata delle password mediante autenticazione a più fattori, che ne consenta una applicazione più sicura e al tempo stesso più semplice da parte dell'utenza, consentendo anche la possibilità di una gestione personale delle impostazioni in completa autonomia.

In sintesi tutte le azioni descritte vanno nella medesima direzione, che è quella di garantire all'AORN un maggiore controllo dei propri sistemi aziendali, un incremento dell'attuale livello di sicurezza, interno ed esterno e, al tempo stesso, di introdurre sistemi di monitoraggio che riescano, anche in maniera predittiva, ad anticipare possibili attacchi ai sistemi o compromissione di dati critici aziendali operando: in modalità automatica bloccando porte e/o sistemi sotto attacco oppure evidenziandone tramite dashboard la presenza di minacce che pretendono l'intervento dell'operatore.

Per l'acquisizione delle soluzioni, come si può evincere dalla tabella seguente, si procederà con l'indizione di una gara aperta utilizzando la piattaforma SIAPS di SoReSa e, contestualmente, con l'adesione alla Convenzione CONSIP "*Cybersecuruty 2*" per l'acquisto delle licenze in essa previste.

QUADRO ECONOMICO DEL PROGETTO			
VOCI DI SPESA	**IMPONIBILE**	**IVA**	**IMPORTO COMPLESSIVO (comprensivo di IVA se non recuperabile)**
SERVIZI DI DIGITALIZZAZIONE DELLA DOCUMENTAZIONE SANITARIA A SUPPORTO DEGLI OPERATORI SANITARI E DEGLI ASSISTITI	€	€	€
ATTREZZATURE PER LA DIGITALIZZAZIONE DEI RISULTATI DIAGNOSTICI	€	€	€
SISTEMI DI CYBER SECURITY	3.365.333,19 €	740.373,30 €	**4.105.706,49** €
TOTALE PROGETTO			**4.105.706,49** €

SISTEMI DI CYBER SECURITY				
DESCRIZIONE *(dettagliare componenti hardware, componenti software ed eventuali spese necessarie per l'installazione; sono escluse le spese relative a manutenzione ordinaria, aggiornamenti, assistenza periodica, formazione del personale)*	**IMPONIBILE**	**IVA**	**IMPORTO COMPLESSIVO (comprensivo di IVA se non recuperabile)**	**MODALITA' DI ACQUISTO**
N. 6 Cisco Firepower 4115 con sistema di Management Firepower Management Center	386.657,28 €	85.064,60 €	471.721,88 €	Convenzione Cybersecurity 2
N. 800 Cisco XDR (Secure-X)	222.634,51 €	48.979,59 €	271.614,10 €	Gara
N. 2.000 licenze Cisco Secure Email Advantage	271.614,10 €	59.755,10 €	331.369,20 €	Gara
N. 1.000 licenze Premier Cisco Secure End Point	182.560,30 €	40.163,27 €	222.723,56 €	Gara
N. 300 licenze Cisco Duo Advantage	111.317,25 €	24.489,80 €	135.807,05 €	Gara
N. 3.000 licenze Identity Service Engine Advantage	115.769,94 €	25.469,39 €	141.239,33 €	Gara

N. 8.000 licenze Cisco Secure Network Analytics Flow Rate	259.740,26 €	57.142,86 €	316.883,12 €	Gara
N. 300 licenze Cisco Secure Client Premier	4.452,69 €	979,59 €	5.432,28 €	Gara
N. 2.000 licenze Cisco Umbrella Advantage	253.803,34 €	55.836,73 €	309.640,07 €	Gara
N. 36 licenze Cisco Incident Response	237.476,81 €	52.244,90 €	289.721,71 €	Gara
N. 10 licenze Application Cisco Radware Cloud WAF	252.319,11 €	55.510,20 €	307.829,31 €	Gara
N. 2.800 Cisco Kenna Vulnerability Management Advantage	192.949,91 €	42.448,98 €	235.398,89 €	Gara
N. 6 Licenze aggiuntive Virtual Patching	287.940,63 €	63.346,94 €	351.287,57 €	Convenzione Cybersecurity 2
N. 1 Piattaforma IAM per 3.000 users	38.038,40 €	8.368,45 €	46.406,85 €	Gara
N. 1 Piattaforma PAM per 500 sistemi target	211.548,03 €	46.540,57 €	258.088,60 €	Gara
Installazione per Cisco Firepower 4115 e Virtual Patching	58.760,00 €	12.927,20 €	71.687,20 €	Convenzione Cybersecurity 2
Installazione per Cisco XDR (Secure-X)	9.939,43 €	2.186,67 €	12.126,10 €	Gara
Installazione per licenze Cisco Secure Email Advantage	23.171,57 €	5.097,75 €	28.269,32 €	Gara
Installazione per licenze Premier Cisco Secure End Point	41.743,00 €	9.183,46 €	50.926,46 €	Gara
Installazione per licenze Cisco Duo Advantage	30.711,57 €	6.756,55 €	37.468,12 €	Gara
Installazione per licenze Identity Service Engine Advantage	14.164,43 €	3.116,17 €	17.280,60 €	Gara
Installazione per licenze Cisco Secure Network Analytics Flow Rate	19.680,14 €	4.329,63 €	24.009,77 €	Gara

Installazione per licenze Cisco Secure Client Premier	3.714,29 €	817,14 €	4.531,43 €	Gara
Installazione per licenze Cisco Umbrella Advantage	14.697,43 €	3.233,43 €	17.930,86 €	Gara
Installazione per licenze Application Cisco Radware Cloud WAF	16.188,71 €	3.561,52 €	19.750,23 €	Gara
Installazione per N.36 licenze Cisco Incident Response	59.369,20 €	13.061,22 €	72.430,42 €	Gara
Installazione per Cisco Kenna Vulnerability Management Advantage	11.230,14 €	2.470,63 €	13.700,77 €	Gara
Installazione per Piattaforma IAM per 3000 users	9.224,43 €	2.029,37 €	11.253,80 €	Gara
Installazione per Piattaforma PAM per 500 sistemi target	23.916,29 €	5.261,58 €	29.177,87 €	Gara
TOTALE	**3.365.333,19 €**	**740.373,30 €**	**4.105.706,49 €**	

CRONOPROGRAMMA			
Sequenza	**Descrizione**	**Data Avvio**	**Data Conclusione (entro il 31/12/2023)**
1	Procedure di affidamento	15 Settembre 2023	30 Settembre 2023
2	Stipula contratto	01 Ottobre 2023	30 Ottobre 2023
3	Esecuzione contratto	01 Novembre 2023	31 Novembre 2023
4	Collaudo	01 Dicembre 2023	15 Dicembre 2023

Il Referente del Progetto
Ing. Gennaro Sirico

Firmato digitalmente da: Gennaro Sirico
Data: 14/09/2023 08:57:38

Il Direttore Generale
Dott. Rodolfo Conenna

Firmato digitalmente da: Rodolfo Conenna
Data: 14/09/2023 12:53:42