



CAPITOLATO TECNICO

*CAPITOLATO TECNICO PER L’AFFIDAMENTO DEL SISTEMA DI
MONITORAGGIO E PROTEZIONE DELLA RETE DATI ASTPU*

Release 2.1 del 29/08/2023

1	PREMESSA.....	4
2	OGGETTO DEL CONTRATTO.....	5
2.1	FINALITÀ DEL SERVIZIO.....	5
2.2	TARGET OGGETTO DI ANALISI E AMBITO	5
2.3	CARATTERISTICHE GENERALI HARDWARE DELLE “APPLIANCE” MINIME OGGETTO DI FORNITURA.....	6
2.4	FUNZIONALITÀ RICHIESTE AL SERVIZIO MINIME PENA L’ESCLUSIONE	6
2.5	DICHIARAZIONI RICHIESTE PENA L’ESCLUSIONE	7
2.6	SUPPORTO STANDARD.....	8
2.7	DURATA DEL CONTRATTO.....	8
2.8	IMPORTO A BASE D’ASTA.....	8
2.9	SERVIZI ACCESSORI	9
2.9.1	REPORTISTICA.....	9
2.9.2	FORMALIZZAZIONE E PRESENTAZIONE DEI RISULTATI NEI REPORT TRIMESTRALI	9
2.9.3	FORMAZIONE.....	10
2.9.4	DOCUMENTAZIONE A CORREDO	10
3	MODALITÀ OPERATIVE, ORGANIZZAZIONE E PROCESSI.....	11
3.1	RISPETTO DELLE TEMPISTICHE AVVIO DEL SERVIZIO	11
3.2	ORARI DI LAVORO	11
3.3	MODALITÀ DI COMUNICAZIONE FORNITORE – AST-PU.....	11
3.4	DATI E INFORMAZIONI RACCOLTI	12
3.5	SERVIZIO DI MANUTENZIONE.....	12
3.5.1	MANUTENZIONE SOFTWARE	12
3.5.2	MANUTENZIONE HARDWARE	13
3.5.3	LIVELLI DI SERVIZIO MINIMI PENA L’ESCLUSIONE.....	14
4	SERVIZI RESI DISPONIBILI DA AST-PU AL FORNITORE.....	15
4.1	INFRASTRUTTURA	15
4.2	SERVIZI DI SUPPORTO DI AST-PU.....	15
4.3	SERVIZI DI SUPPORTO FORNITORE	16
5	SERVICE LEVEL AGREEMENT (SLA) E PENALI.....	17
5.1	VIGENZA DEI LIVELLI DI SERVIZIO	17
5.2	SLA.....	17
5.3	PENALI.....	17
6	OPZIONI	19
6.1	OPZIONE 1	19
6.2	OPZIONE 2	19
6.3	OPZIONE 3	19
7	STANDARD E FRAMEWORK METODOLOGICI.....	20
8	DOCUMENTAZIONE TECNICA DA PRESENTARE IN OFFERTA.....	21

1 Premessa

Il presente documento (di seguito, “*Capitolato Tecnico*”) descrive i requisiti che devono essere rispettati al fine di poter fornire un servizio di monitoraggio del traffico di rete, basato su *machine learning* e tecniche di *Artificial Intelligence*, al fine dell’individuare *anomalie nei comportamenti degli utenti e dei sistemi interni al perimetro Aziendale, tramite l’analisi dei modelli*. La piattaforma è stata individuata tra i sistemi e servizi disponibili, sia open source sia commerciali. Essa risulta leader di mercato nell’ambito dei progetti di cyber security privati internazionali, volti a proteggere organizzazioni complesse, mitigando i rischi e gli impatti di eventi informatici dannosi, attacchi e anomalie di sicurezza, sia in termini di efficacia che efficienza riducendo sensibilmente il tempo di rilevazione delle minacce e dando all’organizzazione modo di rispondere alla minaccia.

La UOC Servizio Informatico dell’Azienda Sanitaria Territoriale Pesaro Urbino (di seguito AST-PU) ai fini della Direttiva 2022/2555 del Parlamento Europeo e del Consiglio del 14 Dicembre 2022, ha necessità di aumentare la protezione dei dati contro minacce Cyber, attivando un servizio basato sulla soluzione “Darktrace enterprise Immune system AI versione 6 o sup.”, completa del modulo Antigena Network, prodotto dalla società Darktrace (avente sede a Cambridge, Regno Unito) **o equivalente**, purché il sistema offerto possieda caratteristiche di autoreponse intrinseche senza necessità di utilizzare sistemi di terze parti o utilizzo di “agent” ovvero componenti software su end point, **pena l’esclusione**.

I sistemi forniti dovranno supportare l’Azienda nella cybersecurity posture, mitigare in modo efficace i rischi di data-breach, essere aderenti alle misure minime Agid, garantire la *compliance* al GDPR, riversare log su un sistema centralizzato, prevedere ed implementare un’integrazione con i sistemi firewall perimetrali al fine di fronteggiare anche attacchi su protocolli individuati dai sistemi IDS a bordo dei medesimi.

La motivazione per la quale AST-PU intende proseguire nel mantenimento di tale servizio, piuttosto che installare sistemi open source o acquistare prodotti, trova le ragioni nella necessità di dotarsi di sistemi di monitoraggio avanzato, non pervasivo, tecnologicamente avanzati, costantemente aggiornati ed in grado di contrastare minacce in tempo reale senza intervento umano. AST-PU registra purtroppo l’assenza di figure tecniche interne con competenze specifiche di Security Analyst, senza le quali i sistemi classici richiederebbero un effort nettamente superiore in termini di configurazione e conduzione. Viceversa, Darktrace offre una soluzione “chiavi in mano”, in grado di colmare il gap interno, offrendo proattività e visibilità delle cyber-minacce in tempo reale, con componenti AI (di intelligenza artificiale) in continuo aggiornamento.

AST-PU include sia l’ex Azienda Ospedaliera Marche Nord che l’ex Area Vasta 1 ASUR. Al momento della stesura del presente capitolato il budget disponibile consente di coprire le esigenze alle sedi di ASTPU di Pesaro, Fano e Urbino per 7 mesi a partire dal 1.10.2023 al 30.04.2024. L’Azienda Sanitaria Territoriale di Pesaro e Urbino si riserva di attivare opzioni senza obbligo alcuno, per ulteriori 6+7 mesi, laddove siano disponibili ulteriori fondi ed economie in grado di sostenere i relativi costi.

Si premette in questa sede che l’Allegato 1 risulta parte integrante del presente capitolato e rappresenta l’insieme degli elementi da portare a monitoraggio attraverso il servizio di che trattasi.

2 Oggetto del contratto

2.1 Finalità del servizio

Il servizio dovrà includere una soluzione “Darktrace enterprise Immune system AI versione 6 o sup. compreso il modulo Antigena Network” agent-less o equivalente, che effettui l’attività di analisi del traffico di rete e azioni di autoresponse rispetto a comportamenti anomali, mediante algoritmi di machine learning AI (intelligenza artificiale). In particolare il modulo “Antigena Network” incluso nella fornitura deve essere configurato per permettere alle medesime appliance di non limitarsi alla sola individuazione delle minacce, ma di porre in essere contromisure ed azioni attacco-difesa che blocchino in tempo reale e in modo proattivo le minacce stesse senza utilizzo di sistemi di terza parti dell’ente.

La soluzione quindi dovrà garantire il servizio di monitoraggio e difesa in tempo reale, il reporting, la registrazione per almeno 3 mesi di tutto il traffico dati (comprensivo di eventi e log) per ciascuna sede, l’analisi e la segnalazione in tempo reale di quanto viene rilevato, la presenza di un’app per smartphone Android, da attivare con licenze illimitate, per tutto il team del Servizio Informatico.

La presenza in offerta della componente “Antigena” di risposta automatica alle minacce, agent-less risulta essere **obbligatoria vincolante, quindi l’assenza del modulo richiesto o soluzioni equivalenti porterà all’esclusione dell’offerta.**

Tutti i servizi sopra indicati sono parte del presente appalto a lotto unico.

2.2 Target oggetto di analisi e ambito

Per target oggetto di analisi si intendono tutti i dispositivi connessi in rete, siano essi apparati di rete, access point, controller, postazioni di lavoro, tablet, workstation, server fisici, server virtuali. La soluzione offerta dovrà prevedere la possibilità di poter monitorare fino a 3000 device licenziati.

I target oggetto dell’analisi saranno forniti in separata sede, secondo le modalità definite e concordate direttamente tra i referenti del *Fornitore* ed i referenti della UOC Servizio informatico di AST-PU.

L’appalto dovrà essere espletato al fine di monitorare e difendere tutte le sedi Aziendali, interconnesse in WAN (wide area network) ivi comprese le connessioni site-to-site extranet verso enti e aziende esterne. Parte delle sedi AST-PU (appartenenti alla precedente Azienda Ospedaliera “Ospedali Riuniti Marche Nord”) sono distribuite nel territorio della Provincia di Pesaro Urbino:

- Presidio di Pesaro, San Salvatore – Pesaro, piazzale Cinelli e magazzino Villa Fastiggi via brigata gap;
- Presidio di Pesaro, San Salvatore – Muraglia, via Cesare Lombroso;
- Presidio di Santa Maria della Misericordia – Urbino via Federico Comandino;
- Presidio di Fano, Santa Croce – Fano, via Vittorio Veneto.

Nel processo di ridefinizione dei budget della nuova Azienda AST-PU, si prevedono come opzioni della fornitura, la possibilità di dotarsi di ulteriori appliance, licenze agent per postazioni di lavoro e giornate di *cyber analyst* che potranno essere acquisiti solo e soltanto in presenza di budget dedicato, ad oggi indisponibile. Con tali elementi in opzione la UOC Servizio Informatico provvederà nell’estendere la piattaforma alle sedi di: Ospedale Urbino, Ospedale di Pergola e PPI Fossombrone Sedi e distretti, per fare alcuni esempi.

I target interessati dovranno essere sia tutti gli indirizzi IP appartenenti alla nuova Azienda, sia le minacce provenienti dai principali enti, Ditte e servizi a cui AST-PU. In particolare:

-
- Regione Marche: rete amministrativa, rete dati del Fascicolo Sanitario elettronico, rete 118;
 - Ex ASUR: rete dati dell'Azienda Sanitaria unica regionale;
 - Servizio CUP CASSA: rete dati del servizio prenotazioni esternalizzato;
 - Fornitori che per motivi di assistenza remota sono connessi (VPN): Ditte Exprivia, Ge Medical, Philips, Beckman, GPI, Dedalus, SCS Computers, ecc.

2.3 Caratteristiche generali hardware delle “appliance” minime oggetto di fornitura

In base all'ampiezza dell'Azienda, della topologia di rete e dei target da monitorare, si richiede al *Fornitore* di fornire un servizio di monitoraggio composto almeno da:

- *N. 2 medium appliance DCIP-M “Darktrace enterprise Immune system AI versione 6 o sup.” per le sedi di Pesaro piazzale Cinelli e Fano Via Vittorio Veneto;*
- *N. 2 small appliance DCIP-S “Darktrace enterprise Immune system AI versione 6 o sup.” per le sedi di Muraglia e Urbino;*
- *Rispettivi moduli su ogni appliance “Antigena Network”;*
- *Attivazione configurazione Antigena entro 20 gg solari consecutivi dall'installazione;*
- *APP IOS e Android per ricezione allarmi su smartphone in tempo reale per numero illimitato di utenti Aziendali;*
- *Supporto standard: configurazioni Antigena, aggiornamenti piattaforma, major release, di tutte le appliance, manutenzione hardware di tutte le parti hardware fornite, help desk da remoto tramite email, con presa in carico in orario ufficio, minimo dalle ore 10.00 – alle ore 18.00 – fuso orario Italiano;*
- *configurazione ed integrazione con Firewall Fortinet 500e al fine di mitigare attacchi sia TCP sia UDP che riversamento log su sistema centralizzato, e a valle di nuovi firewall successivamente adottati;*
- *monitoraggio di host esposti in DMZ AST-PU;*

La descrizione delle appliance DCIP-M e DCIP-S sono descritte nell'Allegato 2 parte integrante del presente Capitolato tecnico.

2.4 Funzionalità richieste al servizio minime pena l'esclusione

L'*Implementazione del servizio* comprende l'utilizzo di una soluzione basata su minimo di n.4 appliance, descritte nel capitolo 2.3, necessarie a monitorare la rete di AST-PU, con lo scopo di rilevare:

- rilevamento comportamenti e/o utilizzo anomalo di apparati/sistemi/risorse in tempo reale e contrasto (auto-response);
- presenza e contrasto di malware, ransomware, trojan sui sistemi Aziendali.

Il servizio offerto dovrà avere le seguenti **caratteristiche minime pena l'esclusione**:

- collezionare informazioni attraverso tutto il flusso di rete interno di AST-PU;
- analizzare le informazioni ed “imparare”, basandosi su quanto collezionato;
- segnalare in real-time in caso di anomalie o minacce rilevate;

- reagire in modo autonomo senza sistemi di terze parti, in tempo reale, agli incidenti, in base alla tipologia di minacce classificate con percentuali/comportamenti oltre la soglia condivisa e concordata con l'Azienda o nei periodi/tempi definiti e concordati con l'Azienda;
- fornire una visione grafica complessiva delle reti analizzate, mostrando a video le zone o target oggetto di attacco, anche in forma testuale, in tempo reale;
- offrire una visione centralizzata per l'analisi dei dati, nel caso in cui la soluzione sia composta di più componenti;
- integrare la profilazione degli utenti di Active Directory di AST-PU all'interno della soluzione software offerta, al fine di tracciare e monitorare i comportamenti sia degli utenti che delle postazioni di lavoro;
- tutte le regole, policy, modelli configurabili all'interno della soluzione devono poter essere personalizzabili secondo le esigenze di AST-PU;
- la/e soluzione/i individuata/e devono sottostare alle normative italiane ed europee nei vari ambiti pertinenti relativamente alla/e soluzione/i individuata/e, come esempio e non esaustivi, Privacy, Regolamento europeo 679/2016 GDPR e s.m.i, REGOLAMENTO (UE) 2019/881 e s.m.i;
- la fornitura dovrà essere comprensiva di tutto l'hardware e software a corredo necessario al funzionamento completo della soluzione offerta. Al termine dei 7 mesi, il Fornitore potrà recuperare l'hardware e software fornito a sue spese, comprese le attività di smontaggio imballaggio, senza ulteriori oneri per l'Azienda;
- il servizio proposto dovrà offrire soluzioni innovative che mettano a disposizione i più moderni algoritmi di machine learning, o di intelligenza artificiale o sistemi di autoapprendimento per rinforzo, utili a evidenziare e segnalare comportamenti interni alla rete LAN e WAN al fine sia di superare le logiche basate su pattern, sia poter minimizzare le problematiche di falsi negativi e positivi.

Tra le funzionalità richieste "preferenziali" (non soggette a "pena esclusione") da attivare, se fattibile, nel corso del contratto, si elencano i bisogni seguenti:

- integrazione LDAP al fine di rilevare nome utente della postazione che presenta anomalie, siano essi del dominio AOMN.intra o del dominio Sanitamarche.intra o altri;
- integrazione per tracciabilità utenti LDAP, in funzione della presenza in servizio degli utenti medesimi, attraverso incrocio di numero badge – codice fiscale, tramite analisi integrazione con sistemi gestionali (forniti dalla ditta *Engineering*) e marcatempo;
- analisi di traffico sospetto da e verso telecamere;
- analisi di traffico sospetto da e verso marcatempo;

2.5 Dichiarazioni richieste pena l'esclusione

In riferimento alle conformità richieste, in risposta al presente bando il Fornitore si impegna a fornire le seguenti dichiarazioni da includere nell'offerta tecnica, **pena l'esclusione** (sotto forma di compilazione dell'Allegato 3 al presente capitolato):

- che la soluzione offerta abbia caratteristiche di auto-response alle minacce in tempo reale e indipendenti da applicativi e sistemi di terze parti;
- dichiarazione di soddisfacimento di tutti i requisiti standard delle Misure minime di sicurezza (circolari Agid) applicate all'Azienda offerente il servizio;

-
- dichiarazione di disponibilità a fornire, in sede di aggiudicazione, almeno un nominativo incaricato dal legale rappresentante per il ruolo di responsabile al trattamento e almeno un nominativo incaricato per il ruolo di Amministratori di sistema (Ads);
 - dichiarazione di conformità del software/servizio offerto ai requisiti obbligatori vincolanti, pena l'esclusione, dettagliatamente riportati in ALLEGATO 1 "ABSC AGID BASIC SECURITY CONTROL(S) E CSC CRITICAL SECURITY CONTROL E NOTE OBBLIGATORIE VINCOLANTI PENA L'ESCLUSIONE";
 - conformità alla normativa vigente e alle circolari ACN ed AGID, in particolare a:
 - <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni> (circolare dell'Agenzia per l'Italia Digitale (AgID) n° 1/2017, recante le "Misure minime di sicurezza ICT per le pubbliche amministrazioni") e successive;
 - Circolare AgID n. 2/2018 e s.m.i.;
 - Circolare AgID n. 3/2018 e s.m.i.

Tra gli elementi che motivano l'introduzione della tecnologia di che trattasi, vi sono la necessità di strumenti necessari a supporto delle attività di sicurezza descritti nella Direttiva Europea NIS (UE) 2016/1148 e s.m.i., recepita dal Decreto Legislativo 18 maggio 2018, n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018.

2.6 Supporto Standard

Il servizio offerto deve comprendere obbligatoriamente un *Supporto Standard* finalizzato a ricevere chiamate di assistenza sia in caso di malfunzionamenti dell'*appliance* sia per richiedere chiarimenti circa l'interpretazione di segnalazioni di minacce o la comprensione dei report forniti. Tale attività di supporto, assimilabile a ritorno formativo, seguirà le medesime SLA in termini di presa in carico delle richieste di anomalia. Il supporto standard opera in orario di ufficio dal lunedì al venerdì dalle ore 10.00 alle 18.00.

2.7 Durata del contratto

Il contratto avrà una durata di 7 mesi a decorrere dalla data del verbale di avvio del servizio (che rappresenterà l'effettivo avvio del servizio), predisposto dal DEC Direttore del contratto, Ing. Carlo Reggiani o suo delegato, ed in accordo con la ditta aggiudicataria.

2.8 Importo a base d'asta

L'importo a base d'asta per 20 mesi, comprensive delle opzioni, è di € 213.500,00+ IVA al 22% (€ 260.470,00 ivato) di cui:

- € 71.750,00 + IVA al 22% (€87.535,00 ivato) per 7 mesi con fatturazione anticipata ove espressamente richiesto (dal 01/10/2023 al 30/04/2024);
- opzioni 1: di ulteriori 7 mesi € 71.750,00 + IVA al 22% (€87.535,00 ivato);
- opzione 2: di ulteriori 6 mesi € 61.500,00 + IVA al 22% (€75.030,00 ivato);
- opzione 3: 10 giornate (8 ore/gg) di attività consulenziali in ambito Cybersecurity € 8.500,00 + IVA al 22% (€10.370,00 ivato);

2.9 Servizi Accessori

Salvo diverso accordo tra le parti, espressamente pattuito nell'ordine (ovvero nel contratto specifico), sono compresi nella fornitura oggetto del presente *Capitolato* i servizi indicati nei sotto-paragrafi seguenti:

- reportistica;
- rendicontazione periodica del corretto e continuo funzionamento del sistema.

2.9.1 Reportistica

Il servizio di *Reportistica* comprende le seguenti attività, a carico del *Fornitore*:

- Reporting trimestrale sulle minacce rilevate: predisposizione, consegna e discussione di uno *Status report* trimestrale, concordata tra le *Parti*, nel quale sono indicate le minacce, i comportamenti anomali, i suggerimenti e le soluzioni consigliate, al fine di contenere, monitorare e ridurre gli eventi segnalati;
- Reporting creabile dagli utenti interni della UOC Servizio Informatico tramite l'appliance Master: gli operatori della UOC Servizio Informatico devono poter disporre di istruzioni operative e supporto, al fine di poter estrarre informazioni statistiche ed elementi di analisi inerente la cyber security, attraverso semplici passaggi, utilizzando l'interfaccia web o schedulandone l'esecuzione nonché l'invio mediante strumenti di comunicazione;

Il servizio di *Reportistica* sopra descritto è parte integrante dell'offerta ed incluso nel corrispettivo annuale.

2.9.2 Formalizzazione e presentazione dei risultati nei report trimestrali

A seguito delle attività di analisi periodiche, il *Fornitore* dovrà provvedere alla produzione di un report tecnico trimestrale di dettaglio da consegnare ad AST-PU in formato PDF interoperabile (testo evidenziabile, copiabile e stampabile, non immagine), riportante i risultati dell'analisi effettuata.

Il report di dettaglio trimestrale deve contenere perlomeno le seguenti sezioni / informazioni:

- un executive summary di taglio manageriale, contenente le anomalie individuate esposte con un linguaggio fruibile anche da personale non tecnico e che permetta al management di evincere il livello di rischio e gli eventuali interventi correttivi da implementare;
- la metodologia adottata per la conduzione dell'attività di analisi e per la valutazione delle anomalie e/o vulnerabilità rilevate;
- informazioni relative all'intervallo temporale di analisi, alle risorse interessate, agli strumenti utilizzati, ovvero ad ogni altra informazioni di contesto dell'attività di analisi;
- la descrizione degli scenari di attacco, laddove applicabile;
- le modalità, le indicazioni, gli strumenti ed i passi necessari da attuare per la verifica manuale della anomalia individuata;
- le modalità di risoluzione o le tecniche di mitigazione dell'anomalia individuata;
- eventuali scenari presenti di mitigazione delle vulnerabilità, ove applicabile.

2.9.3 Formazione

Il Fornitore potrà fornire almeno due (2) giornate (16 ore) di formazione ogni 7 mesi, da erogare ai tecnici della UOC Servizio Informatico, in modalità “training on the job” svolte da remoto, incluse nell’offerta, oltre ai normali corsi disponibili sulla piattaforma Darktrace. Tali attività formative verteranno nel fornire sia elementi conoscitivi delle nuove interfacce, incluso Antigena e sul loro utilizzo, nonché materiale, documenti e istruzioni operative utili allo svolgimento dei compiti di analisi quotidiana e interpretazione degli allarmi mostrati dalle appliance.

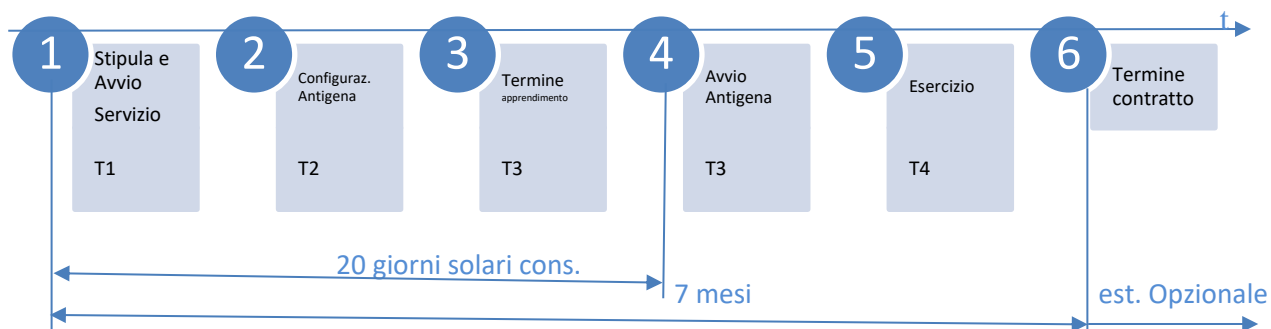
2.9.4 Documentazione a corredo

Il Fornitore dovrà fornire tutta la documentazione, mediante manuali o funzionalità web in lingua italiana o inglese, in forma comprensibile, presentabile ed accettabile (ad es. senza gravi errori grammaticali, ripetuti e grossolani refusi e/o errori di ortografia, etc.).

3 Modalità operative, organizzazione e processi

3.1 Rispetto delle tempistiche avvio del servizio

I Servizi descritti nel presente *Capitolato* dovranno rispettare le *milestone* seguenti:



	Descrizione	Indicatore	Giorni/Mesi
T1-T3	Configurazione Antigena	Massimo ritardo configurazione modulo Antigena e integrazioni Firewall	20 gg solari cons.
T7-T2	Servizio	Tempo Minimo di fruizione del servizio	7 mesi

Il tempo T3 decorre dalla comunicazione dell'avvenuta configurazione e parametrizzazione del modulo Antigena alla UOC Servizio Informatico;

Per mancato rispetto delle tempistiche indicate, saranno applicate le penali previste nel capitolo 5 "Service level agreement (SLA) e Penali" del presente capitolato.

3.2 Orari di lavoro

Salvo diverso accordo tra le *Parti*, espressamente pattuito nell'*Ordine* ovvero nel *Contratto specifico* ovvero nel *Capitolato Tecnico*, l'attività di *Implementazione della soluzione di analisi*, è di norma erogato dal *Fornitore* da lunedì a venerdì in orario compreso tra le ore 10.00 e le ore 18.00 (ora italiana), esclusi i festivi infrasettimanali ("*normale orario di lavoro*").

Fermo restando che tutte le attività relative al Supporto Specialistico agli operatori sono descritte negli orari lavorativi, la soluzione tecnica richiesta dovrà possedere un'opzione proattiva (opzionale) "Antigena" che permetta di attivare – se richiesto – un attacco-difesa H24, in modalità automatica non presidiata, escludibile dai tecnici della UOC Servizio Informatico.

3.3 Modalità di comunicazione Fornitore – AST-PU

Lo scambio di informazioni tra Fornitore e AST-PU potrà avvenire mezzo e-mail e/o PEC (posta elettronica certificata).

Si richiede l'adozione di specifici accorgimenti e meccanismi di sicurezza per lo scambio di informazioni riservate mezzo canali telematici (ad es. posta elettronica).

Sono da considerare riservate ad es.:

- gli esiti dell'attività di analisi contenute nei report inviati e periodici o nelle eventuali presentazioni di sintesi;
- le comunicazioni, anche in forma non strutturata, riportanti informazioni rispetto a anomalie o criticità di sicurezza individuate nell'ambito di conduzione delle analisi;
- le informazioni / dati di proprietà del AST-PU / o della Clientela, ovvero tutte le informazioni / dati cui il Fornitore è venuto in possesso nell'ambito delle attività definite nel presente Capitolato o concordate con i referenti AST-PU;
- le altre informazioni di natura riservata e confidenziale.

I meccanismi da implementare dovranno assicurare la confidenzialità e l'integrità delle informazioni scambiate.

3.4 Dati e informazioni raccolti

Il *Fornitore* è tenuto alla conservazione, con criteri di diligenza e con modalità sicure e riservate, degli eventuali dati e informazioni del AST-PU, raccolte nel corso dell'attività di analisi. Per nessun motivo potrà cedere a terzi dette informazioni.

Resta inteso che AST-PU avrà possibilità di poter estrarre report mediante l'apppliance senza limite di numero e periodicità. La piattaforma dovrà rendere possibile l'analisi dei dati storici per almeno 120 giorni solari, continui e precedenti per 3300 dispositivi e al massimo 6 mesi. Si citano, a titolo meramente esemplificativo, il traffico di rete ed in generale qualsiasi altra informazione raccolta nel corso dell'attività di analisi dai sistemi oggetto di fornitura.

Qualora per numerosità di device o di dati registrati non fosse possibile disporre di almeno 120 giorni di data retention con i sistemi forniti sarà onere del Fornitore adeguare la data retention, senza ulteriori oneri e con attività ricomprese nel servizio.

3.5 Servizio di Manutenzione

La manutenzione hardware e software è parte integrante del servizio offerto e verrà descritta nei capitoli successivi, dovrà decorrere dal momento della consegna ed installazione dei sistemi "appliance" per tutta la durata del contratto.

3.5.1 Manutenzione Software

Tutte le attività relative e necessarie alla manutenzione delle componenti oggetto della fornitura saranno a carico del Fornitore.

Il servizio deve comprendere:

- la manutenzione correttiva, rivolta a ripristinare il corretto funzionamento del software in manutenzione e comprensiva di analisi e soluzione del problema con relativo supporto di specialisti nazionali ed internazionali;
- la manutenzione evolutiva, rivolta a migliorare il servizio, le prestazioni e le funzioni del software in manutenzione;
- l'aggiornamento tecnico del software;
- l'aggiornamento automatico delle signatures di eventuali motori di analisi del traffico;

Il servizio deve comprendere la correzione di malfunzionamenti riscontrati nel software o discordanze rispetto a quanto indicato nella relativa documentazione.

Per ovviare a eventuali vizi e/o difetti riscontrati durante il funzionamento del software, non può essere imposto dal Fornitore il passaggio a successivi aggiornamenti e/o release; sarà facoltà di AST-PU decidere in merito all'installazione degli aggiornamenti, per adeguarsi all'evoluzione del software.

Si precisa che ai fini della valutazione dei tempi di ripristino della funzionalità, il tempo della richiesta d'intervento coincide con quello in cui la struttura AST-PU preposta effettua la richiesta.

Il servizio deve comprendere la fornitura dell'assistenza sistemistica da realizzarsi attraverso il servizio di assistenza, con eventuale successivo intervento del personale tecnico e dei soggetti interessati al servizio, per l'individuazione, la risoluzione del malfunzionamento del prodotto software.

Il servizio deve inoltre includere l'assistenza sistemistica per l'installazione delle nuove versioni del software, delle correzioni ed in generale degli aggiornamenti, ove necessario.

Il servizio deve comprendere la fornitura di tutti gli aggiornamenti del prodotto software che il Fornitore ogni volta annunci come disponibili tramite il proprio listino o analoga fonte di informazione. Tale fornitura include la documentazione (manuali d'uso, d'installazione e tecnici) relativi all'intero prodotto software.

Si precisa che gli aggiornamenti riguarderanno:

- tutte le successive versioni e release dei prodotti programma oggetto della fornitura che vanno rese disponibili per ripristinare il corretto funzionamento del software, per migliorarne il servizio, le prestazioni e le funzioni;
- gli eventuali prodotti, con i loro successivi aggiornamenti, che dovessero sostituire commercialmente i prodotti programma oggetto della presente (e successivi aggiornamenti) inglobandone le funzioni di interesse per AST-PU;
- la fornitura in prova, su richiesta del cliente, delle successive versioni prototipali (versioni e release beta) dei prodotti programma.

La fornitura dei suddetti aggiornamenti si intende completa della relativa licenza di utilizzo valevole, nel caso di effettivo utilizzo degli stessi, in sostituzione della licenza di utilizzo del software originario cui l'aggiornamento si riferisce, qualora l'aggiornamento inglobi anche il software originario.

3.5.2 Manutenzione Hardware

Tutte le attività relative e necessarie alla manutenzione delle componenti DCIP oggetto della fornitura saranno totalmente a carico del Fornitore.

Il servizio deve comprendere:

- la manutenzione correttiva, rivolta a ripristinare il corretto funzionamento dell'hardware in manutenzione e comprensiva di analisi e soluzione del problema con relativo supporto di specialisti nazionali ed internazionali;
- la manutenzione evolutiva, rivolta a migliorare il servizio, le prestazioni e le funzioni dell'hardware in manutenzione;
- l'aggiornamento tecnico dell'hardware definito;
- la sostituzione dell'hardware in caso di guasti, senza esclusioni di parti (hard disk, controller, alimentatori, schede di rete, ecc.)

Il servizio deve comprendere la correzione di malfunzionamenti riscontrati nell'hardware o discordanze rispetto a quanto indicato nella relativa documentazione (dimensionamento, prestazioni, affidabilità, etc.)

Per ovviare a eventuali guasti/difetti riscontrati durante il funzionamento dell'hardware, il Fornitore si occuperà della consegna e dell'installazione di quanto necessario, delle attività di smontaggio, imballo, spedizione dell'hardware difettoso, riducendo al minimo i tempi di fermo ed i tempi di ripristino, entro i limiti indicati nelle SLA, garantendo la configurazione e la sostituzione entro 48 ore lavorative successive all'apertura della richiesta formale da parte di AST-PU. Laddove fosse necessario supporto da parte dei tecnici del Servizio Informatico o di ditte a supporto, sarà necessaria una dichiarazione di manleva da ricevere da parte del Fornitore.

Non sarà cura di AST-PU richiedere al Fornitore l'intervento di manutenzione correttiva sulle appliance, ma sarà a carico del Fornitore la rilevazione proattiva da remoto, attivando un intervento manutentivo e mantenendo aggiornato il Servizio Informatico sulla stima dei tempi di risoluzione. Si precisa che ai fini della valutazione dei tempi di ripristino della funzionalità, il tempo della richiesta d'intervento coincide con quello in cui la struttura AST-PU preposta riceve la segnalazione della necessità di intervento da parte del Fornitore.

Il servizio deve comprendere la fornitura di tutti gli upgrade hardware necessari per garantire lo stesso livello di servizio della soluzione acquistata a fronte di evoluzione tecnologica del prodotto dettata dal Fornitore. Tale fornitura include la documentazione (manuali d'uso, d'installazione e tecnici) relativi all'intero prodotto.

3.5.3 Livelli di Servizio minimi pena l'esclusione

Il *Fornitore* si impegna a prestare il servizio di manutenzione e aggiornamento tecnico per l'hardware e il software secondo la modalità 5x8, dal lunedì al venerdì dalle ore 10:00 alle 18:00.

I tempi di risoluzione di malfunzionamenti software e hardware, bloccanti le funzionalità *dell'appliance*, non devono superare il secondo giorno lavorativo, successivo all'invio della segnalazione da parte di AST-PU al *Fornitore*, pena l'applicazione delle penali previste.

In caso di apertura di chiamate di assistenza per eventi cybersecurity, o per chiarimenti su allarmi o malfunzionamenti dei prodotti software, dovrà essere garantita la presa in carico delle richieste **entro 4 ore dalla apertura del ticket**, mediante apposito portale del servizio di assistenza standard, in orario di ufficio, dal Lunedì al Venerdì dalle 10.00 alle 18.00, al fine di assicurare il necessario supporto all'utilizzo del servizio offerto e a supporto delle azioni di difesa necessarie a mitigare minacce.

4 Servizi resi disponibili da AST-PU al Fornitore

AST-PU si impegna a rendere disponibili al Fornitore, per quanto strettamente necessario all'esecuzione di quanto previsto nel presente Capitolato, i servizi di cui ai paragrafi seguenti.

4.1 Infrastruttura

AST-PU mette a disposizione i rack presenti nei locali tecnici. Qualora siano necessari locali arredati e disponibilità di connettività Aziendale per eventuali attività on site da parte del Fornitore per attività di implementazione, è necessario darne evidenza nell'offerta e preventiva con congruo anticipo. Qualora il Fornitore richieda postazioni di lavoro messe a disposizione da AST-PU, dovrà farne esplicita formalizzazione in sede d'offerta. Il Fornitore potrà utilizzare, salvo diverso accordo comunque esplicitato e formalizzato, proprie apparecchiature informatiche per la predisposizione e conduzione delle attività, purché queste siano comunicate e mappate dalla UOC Servizio informatico, nel contesto delle misure minime di sicurezza.

AST-PU assicurerà il buon funzionamento delle proprie infrastrutture informatiche e del software eventualmente messe a disposizione del *Fornitore*.

In particolare, qualora le verifiche di sicurezza debbano essere effettuate da una delle sedi di AST-PU, l'Azienda assicurerà:

- la disponibilità e la connettività per l'accesso al sistema, secondo le *policy di sicurezza* adottate da AST-PU, nel caso fosse necessario per l'esercizio del servizio;
- la disponibilità di strumenti / software utili all'esecuzione dell'attività oggetto di fornitura, secondo quanto concordato tra i referenti AST-PU e i referenti del *Fornitore*;
- le credenziali di accesso personali alla VPN Aziendale per i tecnici individuati dal Fornitore.

4.2 Servizi di Supporto di AST-PU

AST-PU garantirà al *Fornitore* servizi di supporto relativamente:

- all'installazione fisica delle *appliance* nei rack e locali tecnici Aziendali;
- alla configurazione degli apparati dati, al fine di configurare le porte in SPAN da dedicare all'intercettazione del traffico dati negli switch di core di ciascuna sede;
- alla condivisione di regole ed esclusioni in riferimento a quali comportamenti di traffico si possano considerare "normali" ai fini della riduzione dei falsi positivi;
- alle problematiche relative a SW di proprietà di AST-PU necessari per la conduzione delle attività di analisi;
- all'interfacciamento con i referenti AST-PU di applicazioni e/o sistemi, al fine di reperire informazioni utili all'attività di analisi;
- all'interpretazione degli standard tecnici di AST-PU.

4.3 Servizi di Supporto Fornitore

Il Fornitore dovrà:

- assicurarsi che le medesime *appliance* siano attivate e completino le fasi di apprendimento di tutte le componenti, compreso il modulo Antigena network, entro il termine massimo di 20 giorni dalla stipula del contratto;
- verificare la rispondenza della corretta configurazione delle *appliance*, in riferimento alla topologia di rete, VLAN, trunk ecc. entro i medesimi 20 giorni dalla stipula del contratto;
- assicurare il corretto funzionamento delle *appliance* stesse;
- attivare le integrazioni con i sistemi firewall e log server, entro il termine massimo di 20 giorni dalla stipula del contratto.

5 Service Level Agreement (SLA) e Penali

Il *Fornitore*, nella realizzazione di quanto previsto nel presente *Capitolato*, si impegna a rispettare e rendicontare trimestralmente il rispetto dei *Livelli di Servizio* ("SLA") indicati nel paragrafo che segue.

In caso di mancato rispetto da parte del *Fornitore* di Livelli di Servizio concordati, AST-PU avrà la facoltà di richiamare in forma scritta il Fornitore, segnalando le inadempienze ed irrogando le *Penali* indicate nel presente *Capitolato*, secondo le modalità definite nell'ambito delle relative clausole del *Contratto Specifico* e/o dell'*Ordine* cui accede il presente *Capitolato*.

5.1 Vigenza dei Livelli di Servizio

Le parti condividono che l'applicazione degli SLA indicati nel presente capitolato decorrerà a partire da n. 15 giorni solari successivi dalla data di consegna delle applicance.

5.2 SLA

Il Fornitore si impegna a garantire i seguenti Livelli di Servizio:

- rispettare i tempi di consegna dei sistemi;
- aggiornare tempestivamente le appliance all'ultima release e major release;
- rispettare i tempi di risposta delle richieste di supporto aperte dai tecnici di AST-PU.

La periodicità di misurazione e la verifica del rispetto dei Livelli di Servizio erogati dal Fornitore è trimestrale.

5.3 Penali

Qualora la Ditta Aggiudicataria venga meno agli obblighi assunti con l'aggiudicazione dell'appalto ovvero alle specifiche di cui al presente Capitolato, potrà essere applicata a suo carico una penale per ogni ritardo e/o non conformità contrattuale rilevata.

Nel caso di reiterazione di tali ritardi e/o non conformità della stessa casistica (ovvero di medesimi inadempimenti contrattuali) che hanno comportato l'applicazione di 3 penali all'anno, la AST-PU si riserva la facoltà di risolvere il contratto ed addebitare i costi per l'eventuale espletamento di una nuova gara alla Ditta Aggiudicataria.

È fatta salva in ogni caso la facoltà della AST-PU di agire giudizialmente per il risarcimento dell'eventuale ulteriore danno subito e/o delle spese sostenute a seguito dell'inadempimento.

L'applicazione delle penali avverrà, di norma, a seguito di controlli svolti dal DEC, attraverso verifiche puntuali o a campione delle prestazioni eseguite dalla Ditta Aggiudicataria, nonché a seguito di reclami pervenuti dai clienti interni/esterni del Servizio Informatico. Le penali potranno essere applicate anche senza bisogno di diffida e messa in mora. Di esse sarà data comunicazione scritta alla Ditta Aggiudicataria la quale, entro 10 (dieci) giorni lavorativi dal ricevimento della contestazione, potrà esibire controdeduzioni. A fronte di una posizione discordante tra le parti, sarà applicata la penale.

Il pagamento della penale avverrà tramite emissione di fattura o nota di credito da parte della AST-PU. Le penalità saranno notificate alla Ditta Aggiudicataria, restando escluso qualsiasi avviso di costituzione in mora. La AST-PU si riserva, comunque, di addivenire ad altre forme di incameramento con le modalità che l'Ufficio Legale Aziendale riterrà opportuno. Le suddette penali non esimono la Ditta

Aggiudicataria dal rispondere di eventuali danni e/o dall'effettuazione di interventi di ripristino su richiesta della AST-PU. In tutte le ipotesi di cui sopra, la AST-PU si riserva altresì la facoltà di affidare ad altra Impresa l'esecuzione del servizio, restando a carico della Ditta Aggiudicataria inadempiente sia la differenza per l'eventuale maggiore prezzo rispetto a quello convenuto, sia ogni altro maggiore onere o danno comunque derivante alla AST-PU a causa dell'inadempienza. Nel caso di minore spesa, nulla spetta all'Impresa inadempiente.

Le Penali sono correlate al mancato raggiungimento degli indicatori e livelli di servizio così come sopra definiti per cause imputabili al Fornitore.

Le Penali saranno calcolate trimestralmente e conguagliate nella fattura a saldo, qualora si verifichino ritardi di consegna, o tramite emissione di fatture successive qualora si ravvedano inadempienze nei termini di presa in carico delle richieste di assistenza.

Penali per ritardata attivazione modulo "Antigena network" su tutte le *appliance*

item	indicatore	%	Tempo massimo	Entità Penale
Tempo di configurazione ed avvio delle appliance complete del modulo Antigena	In giorni	Nel 100% dei casi	Tempo massimo di configurazione modulo Antigena entro 20 giorni solari consecutivi dalla data della stipula	100 € per ogni giorno di ritardo

Penali per il mancato espletamento del servizio

item	indicatore	%	Tempo massimo	Entità Penale
Tempo di presa in carico delle richieste di assistenza verso il supporto standard in orario ufficio 10.00 – 18.00 dal Lunedì al Venerdì	In ore	Nel 100% dei casi	Tempo massimo di presa in carico è di 4 ore	100 € per ogni ora di ritardo

Penali per mancato ripristino/attivazione delle appliance

item	indicatore	%	Tempo massimo	Entità Penale
Tempo di ripristino per guasto bloccante software o hardware di una delle appliance (nota 1)	In ore	Nel 100% dei casi	Tempo massimo di ripristino entro il secondo giorno lavorativo successivo (nota 2)	100 € per ogni ora di ritardo

Penali per tempo di disponibilità Up time *appliance*

item	indicatore	%	Tempo massimo	Entità Penale
Tempo di disponibilità delle <i>appliance</i> , al netto delle attività di manutenzione programmate e concordate (nota 1)	In ore	Nel 99,90% del tempo	Tempo massimo di 8h 45m 57.0s all'anno di indisponibilità	100 € per ogni ora di ritardo

Nota 1: si intendono esclusi guasti causati da mancanza di energia elettrica.

Nota 2: in caso di guasto appliance bloccante alle 18.00 di Venerdì X, il tempo massimo di ripristino è entro le ore 18 del Martedì successivo;

In caso di guasto appliance bloccante alle 8.00 di Lunedì Y, il tempo massimo di ripristino senza penali è entro le ore 8.00 del Mercoledì successivo;

6 OPZIONI

Il Fornitore si impegna a fornire nel contesto della fornitura di prodotti e servizi di che trattasi le seguenti opzioni:

OPZIONI	DESCRIZIONE OPZIONE	validità
Opzione 1	Servizio descritto a capitolato e nr. 4 appliance descritte nel capitolo "2.3 Caratteristiche generali hardware delle appliance minime oggetto di fornitura per mesi 7	Attivabile entro 24 mesi dal verbale di avvio del servizio
Opzione 2	Servizio descritto a capitolato e nr. 4 appliance descritte nel capitolo "2.3 Caratteristiche generali hardware delle appliance minime oggetto di fornitura per mesi 7	Attivabile entro 24 mesi dal verbale di avvio del servizio
Opzione 3	Opzione pacchetto nr. 80 ore di attività consulenziali in ambito Cyber security	Attivabile entro 24 mesi dal verbale di avvio del servizio

Resta inteso che AST-PU, non ha nessun obbligo di attivare le opzioni, per le quali al momento della redazione del presente capitolato, risulta assente budget dedicato. È facoltà di AST-PU attivare le opzioni indipendentemente dall'ordine in sequenza delle medesime.

6.1 Opzione 1

Questa opzione include estensione contrattuale del servizio composto di nr. 4 appliance ad Urbino, Pesaro, Muraglia e Fano come descritto nel capitolo, per durata di ulteriori 7 mesi attivabili al termine dei primi 7 mesi.

6.2 Opzione 2

Questa opzione include estensione contrattuale del servizio composto di nr. 4 appliance ad Urbino, Pesaro, Muraglia e Fano come descritto nel capitolo, per durata di ulteriori 7 mesi attivabili al termine dei 7 mesi relativi all'Opzione 1.

6.3 Opzione 3

Questa opzione include fino a nr. 10 giornate di attività "Analisti di sicurezza senior" per un totale di 80 ore/uomo da svolgere da remoto. Il numero minimo di 1 ora/uomo rappresenta l'unità minima di attività che dovesse rendersi necessaria a seguito richieste da parte di AST-PU per approfondimenti e/o incidenti di sicurezza sia in orario lavorativo diurno che in orario esteso notturno/festivo alla medesima tariffa giornaliera. Per Analista di sicurezza senior si intende esperti di comprovate capacità con almeno 10 anni di esperienza, certificazioni in ambito Cyber security come OSCP *Offensive security certified professional* o equivalenti.

Sono comprese nel contesto di tale Opzione: riconfigurazioni / riparametrizzazioni del sistema a seguito di nuovi segmenti di rete da monitorare, analisi contrasto su minacce ed attacchi in corso, supporto all'analisi degli IoC indicatori di compromissione e supporto alle attività di remediation;

7 Standard e framework metodologici

Il Fornitore si impegna ad applicare le regole definite all'interno di AST-PU, o pubblicate da organizzazioni esterne da quest'ultima riconosciute, allo scopo di condurre analisi di sicurezza che soddisfino i necessari requisiti di qualità stabiliti e riconosciuti da AST-PU. Con il consenso di AST-PU ed in assenza di framework individuati, il Fornitore proporrà l'adizione di framework basati su regole e standard di settore.

Salvo diverso accordo tra le Parti espressamente pattuito nell'Ordine ovvero nel Contratto Specifico, il Fornitore dovrà rispettare gli standard previsti da AST-PU o eventualmente proposti e condivisi con l'Azienda, indipendentemente dalla tipologia di analisi di sicurezza, si richiede al Fornitore di adottare standard e metodologie riconosciuti a livello internazionale.

8 Documentazione tecnica da presentare in offerta

La Ditta Aggiudicataria dovrà presentare in offerta tecnica la seguente documentazione senza prezzi:

- breve relazione su quanto richiesto a capitolato e che illustri il progetto tecnico, evidenziando la rispondenza alle caratteristiche minime richieste a capitolato pena l'esclusione, e un tempogramma delle attività, delle risorse impiegate e dei livelli di servizio offerti;
- l'Allegato 3 debitamente compilato nella parte "compilazione a cura della ditta";
- depliant illustrativi e/o documentazione tecnica di tutti i componenti offerti, espandibilità del sistema e certificazioni.

ALLEGATO 1 - ABSC AGID BASIC SECURITY CONTROL(S) E CSC CRITICAL SECURITY CONTROL E NOTE OBBLIGATORIE VINCOLANTI PENA L'ESCLUSIONE

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Obbligatorio vincolante pena esclusione
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Obbligatorio vincolante pena esclusione
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete(1) con allarmi in caso di anomalie.	Obbligatorio vincolante pena esclusione
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Obbligatorio vincolante pena esclusione
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Obbligatorio vincolante pena esclusione
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Obbligatorio vincolante pena esclusione
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Obbligatorio vincolante pena esclusione
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Obbligatorio vincolante pena esclusione
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP .	Obbligatorio vincolante pena esclusione
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine , la funzione del sistema , un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	preferenziale
1	4	3	A	Dispositivi come telefoni cellulari, tablet, lapstops e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione .	preferenziale
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	preferenziale
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	preferenziale

Nota 1: Il sistema deve obbligatoriamente registrare e mappare passivamente i dispositivi attivi di una rete, inclusi il loro MAC, l'indirizzo IP, tipo di dispositivo e nome host tramite il traffico DHCP e DNS. Il sistema deve permettere di poter essere configurato per l'importazione di DHCP log. Tutti i risultati devono essere completamente esportabili e aggiornati in tempo reale . Deve obbligatoriamente registrare quando tutti i dispositivi (approvati e non) vengono visualizzati per la prima volta e per l'ultima volta nella rete.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	preferenziale
2	2	1	S	Implementare una "thitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "thitelist" può essere molto ampia per includere i software più diffusi.	Obbligatorio vincolante pena esclusione
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "thitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "thitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	Obbligatorio vincolante pena esclusione
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "thitelist" non siano state modificate.	Obbligatorio vincolante pena esclusione
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non Autorizzato (2).	Obbligatorio vincolante pena esclusione
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Obbligatorio vincolante pena esclusione
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Obbligatorio vincolante pena esclusione
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	preferenziale

Nota 2: Il sistema deve fornire la visibilità del tipo e della versione del sistema operativo del dispositivo, dei programmi utente e della versione, degli avvisi su elementi vulnerabili e possono essere utilizzati per tracciare la gestione delle patch – Il sistema deve essere proattivo ovvero deve poter impedire ai programmi non autorizzati di effettuare connessioni ad altri dispositivi interni / esterni basati su utenti, porte e protocolli utilizzati.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	preferenziale
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). (3)	Obbligatorio vincolante pena esclusione

Nota 3: Il sistema deve, pena l'esclusione, fornire visibilità e avviso di tutti i protocolli di amministrazione remota non sicuri utilizzati. Deve poter identificare l'amministrazione remota inaspettata e l'uso di utenti / credenziali insoliti

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Obbligatorio vincolante pena esclusione
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Obbligatorio vincolante pena esclusione
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Obbligatorio vincolante pena esclusione
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione .	Obbligatorio vincolante pena esclusione
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Obbligatorio vincolante pena esclusione
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Obbligatorio vincolante pena esclusione
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite(4	Obbligatorio vincolante pena esclusione

Nota 4: Il sistema deve fornire , pena l'esclusione, informazioni sugli attacchi per la correlazione con i dispositivi e la scansione delle vulnerabilità precedenti. Deve avvisare circa attività di scansione in atto, al di fuori delle attività pianificate e scansioni eseguite da dispositivi /utenti non autorizzati. Il sistema deve , pena l'esclusione,informare in caso trovi dei dispositivi non rilevati dai regimi di patching e quelli che utilizzano elementi vulnerabili.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Obbligatorio vincolante pena esclusione
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Obbligatorio vincolante pena esclusione
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Obbligatorio vincolante pena esclusione
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Obbligatorio vincolante pena esclusione
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Obbligatorio vincolante pena esclusione

Nota 5: Il sistema deve consentire, pena l'esclusione, di effettuare l'audit delle credenziali dell'amministratore per il primo utilizzo in rete e fornisce consigli di utilizzo insolito, avvisare sull'utilizzo delle credenziali dell'amministratore e utilizzo su nuovi dispositivi e fallimento accesso con credenziali di amministratore i

CSC 6: MANUTENZIONE, MONITORAGGIO E ANALISI DEI REGISTRI DI CONTROLLO

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 6.1, 6.4, 6.5:

- Le anomalie di sincronizzazione del tempo sono facilmente modellate e avvisate se desiderato
 - Anomalia identificazione in tempo reale e fornitura di rapporti di anomalia su richiesta
 - Registra tutto il traffico interno ed esterno che arriva ai dispositivi
 - Le informazioni sulla sicurezza e la gestione degli eventi devono essere da una specifica messa a fuoco sull'attività insolita, riducendo i falsi positivi, rapida identificazione delle anomalie in tempo reale,
- e prevenzione del sovraccarico di analisi minimizzando e prioritarizzando gli allerts;

CSC 7: E-MAIL E PROTEZIONI DEL BROWSER WEB

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 7.1, 7.2, 7.4, 7.6:

- Deve facilitare l'identificazione di brotser non supportati e client di posta elettronica, plug-in o componenti aggiuntivi Applicazioni;
- Tutte le richieste di URL fallite e di successo per tutti i dispositivi sono registrate per identificarle attività potenzialmente dannose e assistere i gestori di incidenti con l'identificazione di sistemi potenzialmente compromessi;
- Essere proattivo nel bloccare i siti non approvati dall'organizzazione per impostazione predefinita;

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Obbligatorio vincolante pena esclusione
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Obbligatorio vincolante pena esclusione
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Obbligatorio vincolante pena esclusione
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Obbligatorio vincolante pena esclusione
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Obbligatorio vincolante pena esclusione
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento (8).	Obbligatorio vincolante pena l'esclusione

Nota 8: Il sistema deve, pena l'esclusione, monitora continuamente il traffico di rete per workstation, server, IoT, industriale e dispositivi mobili e fornire funzionalità IPS avanzate con sistema proattivo e difensivo in grado di individuare e bloccare tentativi di utilizzo di dispositivi esterni e fornisca alert; Identifichi e blocchi gli eseguibili in tutto il traffico di rete e utilizzano non firme e basato su regole non autorizzate con tecniche per identificare e filtrare i contenuti dannosi.

Il sistema deve permettere la registrazione delle query del DNS (Domain Name System) per rilevare la ricerca del nome host noti domini C2 dannosi, utilizzando la funzione dei domini osservati .

CSC 9: LIMITAZIONE E CONTROLLO DI PORTE, PROTOCOLLI E SERVIZI DI RETE

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 9.1, 9.4:

- Deve identifica l'uso insolito / proibito di porte, protocolli e servizi e aiuta a mantenere la configurazione approvata da business di questi servizi
- Deve identificare qualsiasi server che sta ricevendo connessioni da Internet o da una rete non affidabile
- Il sistema deve essere proattivo e può essere configurato per avvisare e prevenire attivamente bloccando qualsiasi servizio non autorizzato o traffico verso server critici

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud (10).	Obbligatorio vincolante pena esclusione

Nota 10: Il sistema deve , pena l'esclusione, proteggere i sistemi di backup, durante i trasferimenti di dati non sono crittografati, il sistema proattivo deve poter essere configurato al fine di impedire accesso non autorizzato e impedire attivamente e automaticamente attacchi di malware durante l'archiviazione e il trasferimento.

CSC 11: CONFIGURAZIONI SICURE PER DISPOSITIVI DI RETE COME FIREWALL, ROUTER E SWITCH

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 11.3, 11.6, 11.7

- Deve permettere l'individuare l'errata configurazione e la conferma delle modifiche per la configurazione del dispositivo
- Identifica automaticamente le modifiche insolite alla configurazione del dispositivo in base a nuovo / insolito le connessioni di rete
- Confermare la corretta configurazione del dispositivo di amministrazione segregata
- Fornire visibilità sull'intera struttura della rete per confermare e gestire la separazione di rete

CSC 12: DIFESA DEL CONFINE

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 12.1, 12.2, 12.3, 12.4, 12.8, 12.9, 12.10

- Il sistema proattivo deve poter essere configurato per impedire l'accesso a noti indirizzi IP dannosi
- deve poter monitorare completamente gli ambienti DMZ e fornisce l'identificazione e la prevenzione di intrusioni attraverso i vettori di attacco noti e sconosciuti per tutti i dispositivi di rete
- Il sistema proattivo deve poter essere configurato per bloccare minacce conosciute, oltre a identificare nuovi o minacce zero-day senza firme, o regole
- il sistema deve poter identificare in tempo reale tutte le connessioni esterne back-channel
- il sistema deve poter offrire miglioramenti significativi rispetto alla raccolta Netflow tradizionale in rilevamento di attività anomale
- il sistema deve dare visibilità e allerta (e prevenzione) di connessioni anomale, lunghe o sessioni, così come altri metodi di estrusione di dati segreti

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Condizione OV o PREF
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Obbligatorio vincolante pena esclusione
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Obbligatorio vincolante pena esclusione
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Obbligatorio vincolante pena esclusione
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	Obbligatorio vincolante pena esclusione
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi of line.	Obbligatorio vincolante pena esclusione
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto (10).	Obbligatorio vincolante pena esclusione
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Obbligatorio vincolante pena esclusione

Nota 10: Il sistema deve , pena l'esclusione,

- identificare automaticamente tutti i trasferimenti di dati non crittografati di documenti sensibili, inclusi tentativi di exfiltrazione e bloccare tali connessioni in modo proattivo.
- Identificare l'uso di dispositivi USB non autorizzati quando vengono fatte richieste di driver
- Monitorare e bloccare attivamente (funzioni proattive) il flusso di dati all'interno delle reti, con eventuali anomalie che superano i normali schemi di traffico e vengono prese le misure appropriate indirizzarli automaticamente
- Monitorare tutto il traffico che lascia l'organizzazione e rileva qualsiasi utilizzo anomalo di crittografato protocolli
- L'uso di funzioni proattive deve poter bloccare l'accesso ai siti di trasferimento file e di e-mail di trasferimento noti

CSC 14: ACCESSO CONTROLLATO BASATO SULLA NECESSITÀ DI SAPERE

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 14.1, 14.2, 14.3, 14.4, 14.6:

- Il sistema deve permettere l'identificazione di errata configurazione o elusione della segregazione di rete
- Il sistema deve permettere l'identificazione di informazioni sensibili trasferite come testo in chiaro
- Il sistema deve permettere di identifica e impedire ai tentativi di bruteforce di accedere a file system o condivisioni
- Il sistema deve permettere visibilità dell'accesso a dati non pubblici e dati sensibili

CSC 15: CONTROLLO DI ACCESSO WIRELESS

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 15.1, 15.9:

- Il sistema proattivo deve poter essere configurato per impedire a qualsiasi dispositivo non autorizzato di connettersi alla rete
- deve permettere il monitoraggio dell'utilizzo di VLAN separate per l'identificazione e la segnalazione di errori di configurazione consentendo ai dispositivi non fidati di accedere alla rete aziendale.

CSC 16: MONITORAGGIO E CONTROLLO DEGLI ACCOUNT

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 16.3, 16.7, 16.8, 16.9, 16.10, 16.13:

- Il sistema proattivo deve poter essere configurato in modo da disabilitare l'accesso alla rete per dipendenti terminati sulle credenziali osservate sulla rete
- Il sistema deve permettere l'identificazione della configurazione errata del blocco dell'account e l'account disattivato tentativi di accesso
- Il sistema deve poter essere integrato con LDAP per l'autenticazione e l'uso
- Il sistema deve permettere l'identificazione di dispositivi anormali o anomali e utilizzo delle credenziali
- Il sistema deve permettere l'identificazione di credenziali e password che transitano in rete in chiaro

CSC 18: SICUREZZA DEL SOFTWARE APPLICATIVO

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 18.1:

- Il sistema deve permettere visibilità della versione dell'applicazione / degli agenti utente e dei dispositivi che utilizzano utenti agenti vulnerabili

CSC 20: TEST DI PENETRAZIONE ED ESERCIZI CON LA SQUADRA ROSSA

Il sistema deve, pena l'esclusione essere in grado di supportare i controlli 20.1, 20.2:

- Il sistema deve poter essere utilizzato insieme ai test di penetrazione per identificare vulnerabilità e attacchi i vettori che possono essere utilizzati con successo per sfruttare i sistemi aziendali
- Il sistema deve poter fornire visibilità degli account utente o di sistema utilizzati per eseguire test di penetrazione e avvisando sull'uso anomalo di questi account



ALLEGATO 2 - Darktrace Cyber Intelligence Platform (DCIP)

Release 1.1 del 12.11.2020

Allegato 2 Darktrace Cyber Intelligence Platform (DCIP)

Le Appliance Darktrace sono componenti hardware server configurati e parametrizzati al fine di poter rispondere ai più alti livelli di performance e sicurezza (hardening) agli attacchi. Tali apparecchiature che rappresentano l'ossatura del sistema ad alte prestazioni, ospitano la piattaforma Darktrace "on premise". Ce ne sono molti tipi di dispositivi Darktrace, con diverse capacità di throughput e opzioni di configurazione.

La configurazione minima pena l'esclusione prevede la fornitura di

- n. 1 DCIP-S ovvero un appliance small, per la sede con numero inferiore di dispositivi, sede di Muraglia, configurata come sonda "slave" a una Medium configurata come "Master", posizionata nella sede centrale Cinelli;
- n. 2 DCIP-M appliance Medium nelle restanti sedi; La Medium della sede di Fano dovrà essere configurata come sonda "slave" a una Medium configurata come "Master", posizionata nella sede centrale Cinelli;

L'appliance di tipo DCIP-S deve normalmente contenere le seguenti porte:

- 1 x interfaccia fuori banda (OOB)
- 1 interfaccia di amministrazione da 1Gbe
- 3 porte di analisi da 1Gbe



L'appliance di tipo DCIP-M deve normalmente contenere le seguenti porte:

- 1 interfaccia di amministrazione da 1Gbe
- 1 x interfaccia fuori banda
- 3 porte di analisi da 1 GB
- 2 porte di analisi SFP +



Negli apparati di core o centro stella ridondati (Centrale Pesaro e Fano) si dovranno porre in essere tutte le porte necessarie contemporaneamente attive al fine di intercettare tutto il traffico di rete da analizzare e monitorare.

Il fornitore ha possibilità di fornire soluzioni migliorative ovvero appliance di livello superiore come DCIP-X2-11G o DCIP-Z

	DCIP-S	DCIP-M	DCIP-X2-11G	DCIP-Z
Form factor	1U rack mountable (half-depth)	1U rack mountable	2U rack mountable	2U rack mountable
Dimensions (in)	17.32" x 14.57" x 1.73"	17.32" x 29.33" x 1.73"	17.32" x 29.33" x 3.46" H	17.32" x 29.33" x 3.46"
Dimensions (cm)	44cm x 37cm x 4.4cm	44cm x 74.5cm x 4.4cm	44cm x 74.5cm x 8.8cm	44cm x 74.5cm x 8.8cm
Weight (lbs / Kg)	13.3 lbs / 6 Kg	33 lbs / 15 kg	51 lbs / 23 Kg	51 lbs / 23 Kg
Racking	Fits 19" Rack	Fits 19" rack	Fits 19" rack	Fits 19" rack
Interface admin ports	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T
Remote management ports	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T
Copper analysis ports	3 x 10/100/1000 BASE-T	3 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T 2 x 10 GBASE-T	1 x 10/100/1000 BASE-T 2 x 10 GBASE-T
SFP+ analysis ports	n/a	2 x 10Gbe/1Gbe SFP+	2 x 10Gbe/1Gbe SFP+	2 x 10Gbe/1Gbe SFP+
Peak sustained throughput	Up to 300 Mbps	Up to 2Gbps	Up to 5Gbps	Up to 5Gbps
Maximum unique internal devices	Up to 1000 devices analyzed	Up to 8,000 devices analyzed	Up to 36,000 devices analyzed	Up to 50,000 devices analyzed
Maximum connections per minute	2,000	50,000	100,000	250,000
Power supply	Single 350W IEC 13C 100/240V	Dual 750W IEC 13C 100/240V	Dual 1100W IEC 13C 100/240V	Dual 1100W IEC 13C 100/240V
Power consumption	Idle 26 W - 89 BTU/hr	Idle 120 W - 409 BTU/hr	Idle: 128 W - 436 BTU/hr	Idle: 128 W - 436 BTU/hr
	85% 89 W - 305 BTU/hr Max 105 W – 358 BTU/hr	85% 359 W - 1224 BTU/hr Max 418 W – 1426 BTU/hr	85%: 365 W - 1245 BTU/hr Maximum: 426 W - 1453 BTU/hr	85%: 365 W - 1245 BTU/hr Maximum: 426 W - 1453 BTU/hr
Supported Expansion Modules	Can support one expansion model: • 2-port 1G/10G SFP+ • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	Can support one expansion model: • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	Can support up to three expansion models: • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	Can support up to three expansion models: • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T
Safety certificate	UL 60950-CSA 60950, EN 60950, IEC 60950 CB Certificate & Report, IEC 60950			
EMI Certification	FCC Part 15, Class A (CFR 47) (USA), ICES-003 Class A			

ALLEGATO 3 AL CAPITOLATO - check list pena l'esclusione				
n°	DESCRIZIONE	MIN/PRE	COMPILAZIONE A CURA DELLA DITTA	
			SI/NO	esprimere brevemente esplicitando "si conferma" o dettagliando eventuali condizioni migliorative)
1	FORNITURA DI UN SISTEMA SISTEMA "Enterprise immune system AI versione 4"	MIN		
2	fornitura del modulo attacco-difesa "Antigena Network" proattivo in grado di intercettare minacce con reazione in RT	MIN		
3	FORNITURA come da capitolo 2.3 <ul style="list-style-type: none"> N. 2 medium appliance DCIP-M "Dark trace Enterprise immune system AI versione 4" N. 1 small appliance DCIP-S "Dark trace Enterprise immune system AI versione 4" configurazione e apprendimento entro 15 gg successivi dall'installazione; APP IOS e Android per ricezione allarmi su smartphone in tempo reale per numero illimitato di utenti Aziendali; Supporto standard: aggiornamenti piattaforma, major release, di tutte le appliance, manutenzione hardware di tutte le parti hardware fornite, help desk da remoto tramite email, con presa in carico in orario ufficio minimo dalle ore 10.00 – alle ore 18.00 - fuso orario Italiano; 	MIN		
4	Fornitura conforme al cap. 2.4: <ul style="list-style-type: none"> Collezionare informazioni attraverso tutto il flusso di rete interno di AST-PU Analizzare le informazioni e "imparare" basandosi su quanto collezionato Segnalare in real-time in caso di anomalie o minacce rilevate reagire in modo autonomo senza sistemi di terze parti, in tempo reale, agli incidenti, in base alla tipologia di minacce classificate con percentuali/comportamenti oltre la soglia condivisa e concordata con l'Azienda o nei periodi/tempi definiti e concordati con l'Azienda; Fornire una visione grafica complessiva delle reti analizzata, mostrando a video le zone o target oggetto di attacco, anche in forma testuale, in tempo reale; Offrire una visione centralizzata per l'analisi dei dati, nel caso in cui la soluzione sia composta di più componenti Integrare la profilazione degli utenti di Active Directory all'interno della soluzione software offerta, al fine di tracciare e monitorare i comportamenti sia degli utenti che delle postazioni di lavoro; Tutte le regole, policy, modelli configurabili all'interno della soluzione devono poter essere personalizzabili secondo le esigenze di AST-PU La/e soluzione/i individuata/e devono sottostare alle normative italiane ed europee nei vari ambiti pertinenti relativamente alla/e soluzione/i individuata/e, come esempio e non esaustivi, Privacy, Regolamento europeo 679/2016 GDPR s.m.i La fornitura dovrà essere comprensiva di tutto l'hardware e software a corredo necessario al funzionamento completo della soluzione offerta. Al termine dei 12 mesi, salvo espressa indicazione in offerta, il fornitore potrà recuperare l'hardware e software fornito a sue spese, comprese le attività di smontaggio imballaggio, senza ulteriori oneri per l'Azienda Ospedaliera. Il servizio proposto dovrà offrire soluzioni innovative che mettano a disposizione i più moderni algoritmi di machine learning, o AI (intelligenza artificiale) o sistemi di autoapprendimento per rinforzo, utili a evidenziare e segnalare comportamenti interni alla rete Lan e Wan al fine sia di superare le logiche basate su pattern, sia poter minimizzare le problematiche di falsi negativi e positivi; 	MIN		
6	Confermare le dichiarazioni cap. 2.5: <ul style="list-style-type: none"> Dichiarazione di soddisfacimento di tutti i requisiti standard delle Misure minime di sicurezza (circolari Agid) applicate all'Azienda offerente il servizio; Dichiarazione di disponibilità a fornire, in sede di aggiudicazione almeno un nominativo incaricato dal legale rappresentate per il ruolo di responsabile al trattamento e almeno un nominativo incaricato per il ruolo di Amministratori esterni di sistema (Ads) Dichiarazione di conformità del software/servizio offerto ai requisiti dettagliatamente riportati in ALLEGATO 1 "ABSC AGID BASIC SECURITY CONTROL(S) E CSC CRITICAL SECURITY CONTROL E NOTE OBBLIGATORIE VINCOLANTI PENA L'ESCLUSIONE" Conformità alla normativa vigente e alle circolari AGID , in particolare a: <ul style="list-style-type: none"> 1. http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni (circolare dell'Agenzia per l'Italia Digitale (AgID) n° 1/2017, recante le "Misure minime di sicurezza ICT per le pubbliche amministrazioni") e successive; 2. Circolare AgID n. 2/2018 e s.m.i 3. Circolare AgID n. 3/2018 e s.m.i 	MIN		
9	Formazione: n.r 2 (due) giornate di formazione ogni 12 mesi comprese nel contratto di servizio	MIN		
10	Dichiarazione di fornire Livelli di servizio conformi a quanto descritto nel Cap. 3.5.3	MIN		