CENTRO NEUROLESI BONINO PULEJO
IRCCS MESSINA
Istituto di Ricovero e Cura
a Carattere Scientifico
U.O.C. Servizio Provveditorato
Direttore: Dott. Salvatore A. Mingrino

ISO 9001: 2015 - n. 10271

CONSULTAZIONE PRELIMINARE DI MERCATO

(ai sensi dell'art. 77 del D.lgs. n. 36/2023 e ss.mm.ii.)

Fornitura di una soluzione di protezione avanzata degli endpoint (EPP) con funzionalità di rilevamento e risposta (EDR/XDR)

1. Premessa

L'IRCCS Centro Neurolesi "Bonino di Pulejo" di Messina, con sede in Strada Statale 113 – C.da Casazza, 98124 Messina (ME), in qualità di stazione appaltante, intende avviare una consultazione preliminare di mercato ai sensi dell'art. 77 del D.lgs. 36/2023, al fine di acquisire informazioni utili alla corretta preparazione di una futura procedura di gara avente ad oggetto:

la fornitura di una soluzione di protezione avanzata degli endpoint (Endpoint Protection Platform – EPP) integrata con funzionalità di rilevamento e risposta sugli endpoint (Endpoint Detection and Response – EDR), eventualmente estese a logiche di Extended Detection and Response (XDR).

L'iniziativa si inquadra nel percorso di adeguamento dell'Ente agli obblighi in materia di cybersicurezza derivanti dalla Direttiva (UE) 2022/2555 ("NIS2"), recepita in Italia con il D.lgs. 4 settembre 2024, n. 138, e dalle specifiche e determinazioni adottate dall'Agenzia per la Cybersicurezza Nazionale (ACN). In quanto soggetto operante nel settore sanitario (settore "altamente critico" ai sensi dell'Allegato I della Direttiva), l'IRCCS è tenuto all'adozione di misure tecniche e organizzative adeguate a gestire i rischi per la sicurezza delle reti e dei sistemi informativi, tra cui figurano espressamente soluzioni di protezione e di rilevamento/risposta sugli endpoint.

La consultazione è finalizzata a comprendere le soluzioni presenti sul mercato, le caratteristiche tecniche e funzionali disponibili, i modelli di licenza ed erogazione del servizio e le condizioni economiche praticate.

2. Finalità della consultazione

La presente consultazione non costituisce avvio di una procedura di affidamento né impegna in alcun modo l'Amministrazione all'espletamento della stessa. Essa ha lo scopo di acquisire elementi informativi utili a:

- verificare l'esistenza di soluzioni idonee a soddisfare le esigenze di sicurezza, organizzative e operative dell'IRCCS;
- raccogliere informazioni su architetture, capacità di rilevamento e risposta, livelli di sicurezza, interoperabilità (es. con SIEM/SOC) e conformità normativa, con particolare riferimento alla NIS2;
- acquisire indicazioni su modelli di licenza, modalità di erogazione (cloud/SaaS, on-premise, ibrida), assistenza, manutenzione ed eventuali servizi gestiti (MDR);
- individuare le fasce di prezzo e le condizioni economiche di mercato per il perimetro indicato;

- supportare la definizione dei requisiti tecnici e dei criteri di impostazione della futura procedura di gara.

3. Oggetto della consultazione

La consultazione riguarda la **fornitura di una piattaforma di sicurezza degli endpoint che unisca protezione preventiva (anti-malware di nuova generazione) e capacità di rilevamento e risposta (EDR/XDR), erogata preferibilmente in modalità cloud/SaaS con conservazione dei dati all'interno dell'Unione Europea, comprensiva delle relative licenze, dei servizi di supporto e manutenzione e degli aggiornamenti, per una durata indicativa di 36 (trentasei) mesi.**

Perimetro indicativo da proteggere:

- circa 400 postazioni di lavoro (PC desktop e notebook), con sistemi operativi Windows e, in misura minore, macOS/Linux;
- circa 15 server fisici;
- circa 50 macchine virtuali;
- sono esclusi, allo stato attuale, dispositivi mobili (smartphone/tablet) e postazioni collegate ad apparecchiature biomedicali.

I quantitativi sopra indicati sono forniti a fini meramente dimensionali e non vincolanti, e potranno essere rideterminati in sede di gara.

3.bis Caratteristiche tecniche e funzionali (non vincolanti)

La soluzione oggetto della consultazione dovrà possedere, a titolo esemplificativo e non esaustivo, le seguenti caratteristiche, raggruppate per ambito funzionale.

A. Protezione degli endpoint (EPP – anti-malware di nuova generazione)

- protezione multi-livello combinata: motore a firme, analisi euristica, machine learning e analisi comportamentale (behavioral analysis);
- protezione in tempo reale (on-access) e su richiesta/pianificata (on-demand), con scansioni a basso impatto sulle prestazioni;
- protezione specifica anti-ransomware, con capacità di blocco, contenimento e ripristino automatico dei file cifrati (rollback/remediation);
- protezione da minacce fileless, da exploit e attacchi alla memoria, con tecniche di anti-exploit e application/memory protection;
- protezione web e di navigazione: filtraggio URL, anti-phishing, blocco di domini e contenuti malevoli;
- controllo dei dispositivi periferici (device control, es. porte USB e supporti rimovibili) e controllo applicativo (application control / whitelisting);
- firewall a livello di host e sistema di prevenzione delle intrusioni host-based (HIPS);
- supporto multi-piattaforma: sistemi operativi Windows client e server, principali distribuzioni Linux server e macOS;

- ottimizzazione per ambienti virtualizzati (es. VMware, Microsoft Hyper-V), con architettura a impatto contenuto (light agent o agentless) e gestione delle "scan storm";
- aggiornamento automatico e continuo delle firme, dei modelli e dei componenti, senza interruzione del servizio.

B. Rilevamento e risposta (EDR / XDR)

- raccolta continua di telemetria e registrazione granulare delle attività sugli endpoint (processi, connessioni di rete, modifiche al registro/file system, esecuzioni);
- rilevamento comportamentale di minacce avanzate e mirate (APT), anche prive di firma, mediante analisi e correlazione degli eventi;
- mappatura delle tecniche di attacco rilevate sul framework MITRE ATT&CK;
- funzionalità di indagine e threat hunting, con ricostruzione della catena di attacco (root cause analysis) e timeline degli eventi;
- azioni di risposta: isolamento dell'endpoint dalla rete, terminazione di processi, quarantena dei file, rimozione delle minacce e ripristino (remediation/rollback), eseguibili da remoto dalla console;
- automazione della risposta tramite playbook e regole configurabili;
- integrazione di threat intelligence aggiornata (indicatori di compromissione – IoC, reputazione, feed);
- capacità XDR di correlazione con ulteriori sorgenti (rete, posta elettronica, identità/cloud), ove disponibili, per una visione estesa degli incidenti.

C. Gestione, console e amministrazione

- console di gestione centralizzata, preferibilmente in modalità cloud/SaaS, con accesso via web;
- conservazione ed elaborazione dei dati all'interno dell'Unione Europea (data residency UE), nel pieno rispetto del GDPR;
- autenticazione a più fattori (MFA) per l'accesso alla console e gestione granulare dei ruoli e dei privilegi (RBAC);
- gestione centralizzata delle policy di sicurezza per gruppi di dispositivi, con possibilità di configurazioni differenziate;
- dashboard di sintesi, reportistica periodica e personalizzabile, esportazione dei dati;
- registrazione completa degli eventi e delle azioni amministrative (audit log) e relativa conservazione per finalità di tracciabilità;
- qualora erogata in modalità cloud/SaaS, la soluzione dovrà essere qualificata e iscritta nel Catalogo dei servizi cloud dell'ACN almeno al Livello 2 (QC2), idoneo al trattamento di dati e servizi qualificati come critici, ai sensi del DL 82/2021 e della L. 109/2021.

D. Interoperabilità e supporto agli obblighi NIS2

- integrazione con sistemi SIEM e/o con un eventuale SOC, mediante invio dei log (es. syslog) e/o API documentate;
- supporto alla gestione e alla notifica degli incidenti significativi (raccolta evidenze, esportazione di IoC e report), coerentemente con gli obblighi di notifica all'ACN previsti dalla NIS2;

- eventuali funzionalità integrate di valutazione delle vulnerabilità e di visibilità sullo stato di aggiornamento (patch insight) degli endpoint;
- aderenza ai principi e ai controlli dei framework di riferimento (ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0) con tracciabilità rispetto ai requisiti NIS2/ACN.

E. Servizi a corredo

- servizi di supporto tecnico e manutenzione, con livelli di servizio (SLA) definiti e canali di assistenza in lingua italiana;
- attività di onboarding, configurazione iniziale e migrazione dall'eventuale soluzione preesistente, con piano di dismissione del prodotto attuale;
- formazione/affiancamento del personale tecnico dell'Ente;
- eventuale servizio gestito di rilevamento e risposta (Managed Detection and Response – MDR) con monitoraggio 24/7, da quotare in via opzionale e separata.

Ulteriori elementi di valutazione

Saranno oggetto di particolare interesse:

- i risultati di test e valutazioni indipendenti (es. AV-TEST, AV-Comparatives, MITRE Engenuity ATT&CK Evaluations);
- le certificazioni di prodotto e/o di processo (es. ISO/IEC 27001, Common Criteria);
- l'efficacia di rilevamento, il tasso di falsi positivi e l'impatto sulle prestazioni degli endpoint;
- la semplicità di gestione e la maturità della console;
- eventuali soluzioni tecnologiche innovative o migliorative rispetto allo stato dell'arte.

Conformità normativa

Le soluzioni proposte dovranno essere conformi alla normativa vigente in materia di cybersicurezza e protezione dei dati, con particolare riferimento a: Direttiva (UE) 2022/2555 (NIS2) e D.lgs. 138/2024; specifiche e determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN); Regolamento (UE) 2016/679 (GDPR). Costituiscono riferimento i framework ISO/IEC 27001:2022 e NIST Cybersecurity Framework 2.0. Qualora erogata in modalità cloud/SaaS, la soluzione dovrà inoltre risultare qualificata e iscritta nel Catalogo dei servizi cloud dell'ACN almeno al Livello 2 (QC2), in coerenza con gli obblighi di acquisizione dei servizi cloud da parte delle pubbliche amministrazioni (DL 82/2021 e L. 109/2021).

Clausola di neutralità tecnologica (fondamentale)

Le caratteristiche sopra indicate sono da intendersi come requisiti funzionali minimi. Saranno prese in considerazione soluzioni tecnologiche differenti, anche basate su approcci o architetture diversi, purché idonee a garantire prestazioni equivalenti o migliorative sotto il profilo della sicurezza, operativo e di conformità.

4. Modalità di partecipazione

Gli operatori economici interessati possono partecipare trasmettendo:

- una manifestazione di interesse, redatta secondo il modello allegato (Allegato A);

- documentazione tecnica o informativa ritenuta utile (brochure, schede prodotto, white paper, listini indicativi, proposte tecniche non vincolanti, ecc.);
- eventuali certificazioni di prodotto e/o aziendali pertinenti (es. ISO/IEC 27001, risultati di test indipendenti, attestazioni di conformità).

La documentazione dovrà pervenire entro e non oltre il termine perentorio del: **18/06/2026 alle ore 12,00** al seguente indirizzo PEC: provveditorato@pec.irccsneurolesiboninopulejo.it

5. Svolgimento della consultazione

L'Amministrazione potrà, a propria discrezione:

- invitare gli operatori a incontri, tavoli tecnici o audizioni individuali o collettive, anche in modalità telematica;
- richiedere dimostrazioni tecniche (demo/proof of concept) della soluzione proposta;
- formulare richieste di chiarimenti o approfondimenti scritti;
- pubblicare successivi aggiornamenti o esiti della consultazione.

6. Trattamento dei dati

I dati personali saranno trattati nel rispetto del Regolamento (UE) 2016/679 (GDPR) e del D.lgs. 196/2003 e ss.mm.ii., esclusivamente per le finalità connesse alla presente consultazione.

7. Pubblicità

Il presente avviso è pubblicato sul sito istituzionale dell'IRCCS, nella sezione: "Amministrazione trasparente" → "Bandi di gara e contratti".

8. Responsabile del procedimento

Responsabile del procedimento: Dott. Salvatore Alessandro Mingrino

Email: salvatore.mingrino@irccsme.it

Telefono: 090 60128414

9. Chiarimenti

Eventuali richieste di chiarimento potranno essere inoltrate entro il **15/06/2026 alle ore 12,00** esclusivamente via PEC all'indirizzo sopra indicato. Le risposte saranno pubblicate in forma anonima sul sito istituzionale dell'Ente.

Il Direttore dell'U.O.C. Provveditorato
Dott. Salvatore Alessandro Mingrino

ALLEGATO A
Modello di Manifestazione di Interesse

(da compilare su carta intestata dell'operatore economico)

Spett.le IRCCS Centro Neurolesi "Bonino di Pulejo" – Messina –
PEC: provveditorato@pec.irccsneurolesiboninopulejo.it

Oggetto: Partecipazione alla consultazione preliminare di mercato ai sensi dell'art. 77 D.lgs. 36/2023 relativa a: Fornitura di una soluzione di protezione avanzata degli endpoint (Endpoint Protection Platform – EPP) integrata con funzionalità di rilevamento e risposta (Endpoint Detection and Response – EDR/XDR).

Il sottoscritto _____,

in qualità di _____,

della società _____,

con sede legale in _____,

MANIFESTA L'INTERESSE

alla partecipazione alla consultazione preliminare di mercato di cui in oggetto.

A tal fine dichiara:

- di operare nel settore oggetto della consultazione;
- di essere in possesso dei requisiti di ordine generale previsti dalla normativa vigente;
- di non trovarsi in alcuna delle cause di esclusione previste dall'art. 94 del D.lgs. 36/2023;
- di non trovarsi in situazioni di conflitto di interessi ai sensi dell'art. 16 del medesimo decreto;
- di essere consapevole che la presente manifestazione di interesse non costituisce proposta contrattuale né vincolo per l'Amministrazione.

Dichiara inoltre che i prodotti/servizi che la scrivente Ditta commercializza ed è disponibile a offrire, nel contesto di una eventuale procedura che dovesse essere indetta dall'IRCCS, hanno le seguenti caratteristiche (compilare):

- Denominazione della soluzione e versione:
  _____
- Descrizione sintetica e architettura (cloud/SaaS, on-premise, ibrida; ubicazione dei data center):
  _____

- Qualificazione ACN Catalogo Cloud, ove applicabile (indicare livello – almeno QC2 – e riferimento):
  _____
- Caratteristiche di protezione (EPP) e di rilevamento/risposta (EDR/XDR):
  _____
- Sistemi operativi e ambienti virtualizzati supportati:
  _____
- Modalità di integrazione con SIEM/SOC e supporto agli obblighi di notifica NIS2:
  _____
- Certificazioni di prodotto/aziendali e risultati di test indipendenti:
  _____
- Modello di licenza, modalità di erogazione e servizi a corredo (incl. eventuale MDR):
  _____
- Livelli di servizio (SLA) e modalità di assistenza:
  _____
- Indicazione di massima dei costi (perimetro: 500 PdL, 20 server fisici, 200 VM; durata 36 mesi):
  _____

Si allega eventuale documentazione tecnica o informativa ritenuta utile (brochure, schede prodotto, white paper, certificazioni, proposte tecniche non vincolanti, ecc.).

_____ , lì _____

Firma _____