COMANDO PER LE OPERAZIONI IN RETE
UFFICIO AMMINISTRAZIONE
Sezione Contratti
C . F . 9 6 4 5 1 0 6 0 5 8 4
Via Stresa 31/B – 00135 ROMA

Posta elettronica: cor@cor.difesa.it
Posta elettronica certificata: cor@postacert.difesa.it

Lettera di Ordinazione n. 187
(da citare in fattura)

Roma, 25/11/2025

NSR SRL
Via Ortigara, 3 – 00195 Roma
(PEC: nsr@pec.nsr.it)

Oggetto: Gara 98 – III ESPERIMENTO - assistenza sistemistica per il supporto sui processi automazione interna del Comando per mezzo dell'infrastruttura Cortex palo alto networks – CIG B8F2119260 - CUP D87H25000960001 – Capitolo 1412/3 – E.F. 2025. RDO 5758281.
IDV: 2021947

Rife: Obbligazione Commerciale nr. 55/2025 del 25/11/2025.

1. Codesta Ditta è risultata essere aggiudicataria della seguente fornitura, comprensiva dei relativi costi alla sicurezza, pari a euro **91,70** come da T.D. in oggetto:

Descrizione	Capitolo 1412/3
assistenza sistemistica per il supporto sui processi automazione interna del Comando per mezzo dell'infrastruttura Cortex palo alto networks.	€. 74.250,00
Totale Imponibile	€. 74.250,00
Iva 22%	**€. 16.335,00**
TOTALE	**€. 90.585,00**

2. La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del Codice dei contratti di cui al decreto legislativo 31 marzo 2023, nr. 36.
3. La Ditta si impegna ad eseguire la fornitura/prestazione a sua cura, rischio e spese **a decorrere dalla data di consegna/accettazione della presente e dovrà essere conclusa entro il giorno il 31/12/2025,** osservando tutte le norme e disposizioni indicate nella presente lettera di ordinazione
4. **la fattura elettronica dovrà essere obbligatoriamente emesse in data successiva all'ultimazione della fornitura/servizio** ovvero successivamente agli esiti positivi delle procedure previste ai fini dell'accertamento della conformità della fornitura/servizio (verbale di verifica conformità ove previsto) e comunque, **previa richiesta di autorizzazione al seguente indirizzo email: uam.sa.sca.cs@cor.difesa.it**; dovrà essere compilata in maniera analitica nelle modalità richieste, come sopra specificato, e dovrà indicare il numero di protocollo del presente ordinativo, il numero di **CIG e CUP, la causale come da oggetto della presente lettera** e l'annotazione "SCISSIONE DEI PAGAMENTI" (qualora in presenza di IVA da versare allo Stato). La stessa dovrà essere intestata ed inviata a: COMANDO PER LE OPERAZIONI IN RETE - Servizio Amministrativo - Via Stresa, n. 31/b – 00135 ROMA Codice Fiscale 96451060584. **Codice Ufficio ai sensi dell'articolo 3, del Decreto MEF n. 55 del 3 aprile 2013 in materia di emissione, trasmissione e ricevimento della fattura elettronica 2SR075**.
5. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 1412/3 dell'E.F. 2025** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).
6. La fornitura/prestazione dovrà essere effettuata a cura di codesta Ditta secondo le modalità riportate nell'Obbligazione Commerciale in riferimento.
7. **Direttore Esecuzione Contrattuale: Magg. Tommaso TROIA tel. 06/469124770 – mail: scd.cert.sthvii.cs@cor.difesa.it**

IL RESPONSABILE UNICO DEL PROGETTO
IN FASE AFFIDAMENTO
Brig. Gen. Maurizio LAMBIASE
(documento firmato digitalmente)

Firmato digitalmente da: MAURIZIO LAMBIASE
RUP AFFIDAM
In Data/On Date:
martedì 25 novembre 2025 09:52:11

FIRMA PER ACCETTAZIONE
IL RAPPRESENTANTE LEGALE DELLA DITTA
(documento firmato digitalmente)

Firmato digitalmente da: SINCERI MARCO
Data: 25/11/2025 14:42:52

ALLEGATO 4

Ai fini della validità dell'offerta, la stessa va presentata seguendo lo schema seguente.
Per informazioni a carattere amministrativo-procedurale:

SCHEMA DI OFFERTA

Alla **COMANDO OPERAZIONI IN RETE**
Ufficio Amministrazione - Sezione Gestione
Finanziaria e Contratti
Via Stresa, 31/B

Oggetto: **Gara 98 – III ESPERIMENTO - assistenza sistemistica per il supporto sui processi automazione interna del Comando per mezzo dell'infrastruttura Cortex palo alto networks – CUP D87H25000960001 – Capitolo 1412/3 – E.F. 2025 – CUP D87H25000960001 – Capitolo 1412/3 – E.F. 2025 - Importo massimo previsto €. 76.342,16 (settantaseimilatrecentoquarantadue/16) IVA esclusa.**

Il sottoscritto Marco Sinceri nella sua qualità di Amministratore Unico e Legale Rappresentante della Ditta NSR S.r.l., pec ufficiogarensr@pec.it residente in Fiumicino Via Ferruccio Tempesti n. 27 Codice fiscale/partita I.V.A. n. 04303141008 presenta la seguente offerta:

TIPOLOGIA	Qtà richieste	Prezzo unitario	TOTALE COMPRENSIVO COSTI SICUREZZA, come da offerta MEPA (A)
assistenza sistemistica per il supporto sui processi automazione interna del Comando per mezzo dell'infrastruttura Cortex palo alto networks come da Requisito Tecnico Operativo in allegato.	come da RTO in allegato	**€ 74.250,00**	€ 74.250,00
N.B. ALLEGARE DETTAGLIO ANALITICO PREZZI OFFERTI SUDDIVISO PER COSTO UNITARIO DEI MATERIALI E/O ATTIVITA' DA SVOLGERE COME DA RTO IN ALLEGATO		ONERI DELLA SICUREZZA (a cura stazione appaltante qualora previsti non soggetti a ribasso) (B)	€ 0,00
		COSTI SICUREZZA a cura Ditta indicazione obbligatoria (solo da indicare) *	€ 91,70
		IMPORTO IMPONIBILE	**€ 74.250,00**
		IVA 22%	**€ 16.335,00**
		Totale Offerta	**€ 90.585,00**

*** Ai sensi dell'art. 26, comma 6, del D.Lgs. 9 aprile 2008, n.81 e del D.L. n. 70/2011 "Decreto sviluppo", è obbligatoria l'indicazione dei costi per la sicurezza.**

La presente offerta ha validità fino al 31/12/2025.

L'OFFERENTE

timbro e firma

NSR. datasecurity

Dettagliato elenco dei prezzi offerti

TD 5758281	Gara 98 – III ESPERIMENTO - assistenza sistemistica per il supporto sui processi automazione interna del Comando per mezzo dell'infrastruttura Cortex palo alto networks – CUP D87H25000960001 – Capitolo 1412/3 – E.F. 2025.

Descrizione Attività	EFFORT	Valore
Assistenza sistemistica per il supporto sui processi automazione interna del Comando per mezzo dell'infrastruttura Cortex palo alto networks come da Requisito Tecnico Operativo in allegato.	135	74.250,00 €
		74.250,00 €

NSR S.r.l.
Firmato digitalmente dal legale rappresentante
Marco Sinceri

COMANDO PER LE OPERAZIONI IN RETE

Reparto Sicurezza e Cyber Defence

CERT Difesa

REQUISITO TECNICO OPERATIVO

Relativo a

Assistenza sistemistica
finalizzata allo studio, documentazione e automazione di processi interni al Comando per le Operazioni in Rete

Edizione 2025

PREDISPOSIZIONE DEL DOCUMENTO

Redatto da	Data
Comando per le Operazioni in Rete Reparto *Sicurezza e Cyber Defence* Ufficio CERT Difesa Magg. Tommaso TROIA Ten.Col. Alessandro CIMA	29/04/2025

LISTA REVISORI

Ufficio/Sezione/Nominativo

REGISTRO DELLE REVISIONI

Revisione	Data	Capitoli/paragrafi modificati	Osservazioni

QUESTO DOCUMENTO È COSTITUITO DA 8 PAGINE TOTALI

Indice

1. Obiettivi

Il Comando per le Operazioni in Rete (COR), in accordo con le disposizioni discendenti dalle decretazioni emesse nel contesto del "Board Direttivo per il conseguimento degli obiettivi tecnologici funzionali all'evoluzione della nuova Governance di sicurezza della Difesa", ha identificato il CERT quale accentratore, gestore e valutatore di tutte le informazioni tecniche riguardanti le minacce cibernetiche nei confronti dell'intero comparto Difesa; ciò al fine di sviluppare una efficace azione di prevenzione e pronta reazione alle minacce attraverso l'impiego di adeguati strumenti di raccolta ed analisi delle informazioni relative ad attori malevoli e caratteristiche degli strumenti e delle modalità operative impiegate dagli stessi.

Scopo del presente requisito è l'acquisizione di un servizio di assistenza sistemistica finalizzato allo studio, documentazione e automazione di processi interni al Comando per le Operazioni in Rete, da attuarsi per mezzo dell'infrastruttura Cortex - Palo Alto Networks ivi presente.

2. Riferimenti

- SMD-G-137/R - Tabelle Ordinative del Comando COR;
- SMD-I-013 - Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa. Ed. 2008;
- SMD-I-024 - Procedure sulla gestione in sicurezza dei servizi informatici non-classificati dell'amministrazione difesa. Ed.2017 – aggiornata alle varianti 2020.
- Resoconto riunione Board attuativo del 07 marzo 2019;

3. Situazione "AS IS"

Presso il CERT Difesa è disponibile una rete operativa, dedicata alle specifiche esigenze dello stesso, contente gli strumenti necessari alle funzioni di *Real Time Security Monitoring*, *Incident Response*, *Cyber Threat Intelligence* e *Cyber Threat Hunting*.

Tra gli strumenti predisposti ed impiegati su tale rete, figura in particolare una infrastruttura del *software* Cortex, del produttore Palo Alto Networks.

Si ritiene opportuno acquisire un servizio di assistenza sistemistica finalizzato all'automazione di alcuni processi interni al Comando per le Operazioni in Rete per mezzo dell'infrastruttura in parola.

4. Situazione "TO BE"

Scopo del presente requisito è l'acquisizione di un servizio di assistenza sistemistica:

- erogato da personale interno del fornitore, che deve essere qualificato come *partner* del produttore Palo Alto Networks, o da aziende *system integrator* il cui personale sia certificato dal produttore medesimo (almeno in possesso delle seguenti certificazioni: PSE – Palo Alto Network Systems Engineer e PCSE – Palo Alto Network Security Engineer);
- quantificabile in almeno 90 giornate / uomo.

Il servizio di assistenza sistemistica in parola dovrà essere finalizzato allo studio, documentazione e automazione di processi interni al Comando per le Operazioni in Rete, con particolare focus su quanto operato dal CERT Difesa, attraverso la realizzazione di:

a. almeno n.5 *use case*, c.d. "*playbook*" sulla piattaforma Cortex XSOAR, nelle modalità tecniche indicate per tramite dal DEC;
b. la realizzazione di una monografia per ogni *use case*, che documenti il processo analizzato e le azioni automatizzate per mezzo di codice, sulla quale basare future implementazioni / manutenzioni / migrazioni.

Gli *use case* da realizzare dovranno permettere di automatizzare:

1. la gestione del ciclo di vita degli IoC ricevuti dal Comando per le Operazioni in Rete attraverso flussi di *Cyber Threat Intelligence*;
2. la creazione automatica di documenti di testo, bollettini ovvero eventi MISP (*Malware Information Sharing Platform*) a partire dalle informazioni raccolte sui sistemi di sicurezza in uso presso il Comando per le Operazioni in Rete (es: Sandbox) ovvero da siti Internet individuati quali sorgente (es: siti internet di produttori di *hardware*, siti internet di enti deputati alla sicurezza cibernetica);
3. la ricerca sui sistemi di monitoraggio in uso presso il Comano per le Operazioni in Rete a partire da *observables* (es: indirizzi IP, *hash*, nomi a dominio, ecc...) ottenuti in maniera indipendente, finalizzata alla creazione di *report* e/o all'esportazione di catture di traffico (file .PCAP) qualora disponibili;
4. l'analisi di archivi di dati alla ricerca di:
   - *malware* veicolati all'interno;
   - specifici riferimenti al Ministero della Difesa, alle Forze Armate ovvero ad articolazioni da esse dipendenti, ovvero di specifiche parole chiave o etichette contenuti nei testi;
   - *Personal Identifiable Information*;

   nonché la produzione di *report* dedicati;
5. l'esecuzione di azioni per bloccare la minaccia (es: la creazione ovvero la rimozione di blocchi di *observables* e/o IoC sui sistemi di sicurezza al verificarsi di determinate condizioni);
6. (opzionale) l'analisi di messaggi di posta elettronica ritenuti potenzialmente malevoli / spam / *phishing*;
7. (opzionale) ogni altro *use case* implementabile nel limite delle giornate / uomo eventualmente residue successivamente alla realizzazione dei n.5 *use case*.

Saranno pertanto funzionali ed imprescindibili per il raggiungimento dell'obiettivo le integrazioni con sistemi di terze parti in esercizio sulla rete, al fine poter recepire eventi o *alert* ovvero per creare e gestire *incident* corredati da tutti i necessari attributi e informazioni. I sistemi per cui è almeno richiesta l'integrazione sono i seguenti:

- SIEM Qradar, Qradar EDR;
- piattaforma MISP;
- *sandbox* Fireeye;
- *firewall* CheckPoint;
- RSA Netwitness;
- ecosistema Trellix;

- altri apparati in grado di dialogare tramite lo scambio di informazioni in *standard* STIX (*Standard Threat Intelligence eXchange*) / TAXII (*Trusted Automated Exchange of Intelligence Information*), protocollo *syslog*, API REST.

Il sistema dovrà inoltre essere in grado di connettersi a una o più caselle di posta elettronica per permettergli di interpretare le *e-mail* in ingresso od automatizzare l'invio di *mail* verso terzi.

5. Gap Analysis

Attività	Da realizzare	In realizzazione	Realizzata
studio, documentazione e automazione di processi interni – realizzazione di almeno n.5 *use case*	X		
realizzazione di una monografia per ogni *use case* automatizzato	X		

6. Piano Attuativo

L'impresa dovrà essere conclusa entro il 15 Ottobre 2025.

7. Possibili soluzioni

L'impresa dovrà essere realizzata da erogato da personale interno del fornitore, che deve essere qualificato come *partner* del produttore Palo Alto Networks, o da aziende *system integrator* il cui personale sia certificato dal produttore medesimo (almeno in possesso delle seguenti certificazioni: PSE – Palo Alto Network Systems Engineer e PCSE – Palo Alto Network Security Engineer).

8. Quotazione economica

A fronte delle fornitura di quanto descritto, si stimano oneri finanziari per un impegno complessivo totale pari ad € 95.000.