COMANDO PER LE OPERAZIONI IN RETE
UFFICIO AMMINISTRAZIONE
Sezione Gestione Finanziaria e 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. 174
(da citare in fattura)

Roma, 25/11/2024

Società DEAS – DIFESA E ANALISI SISTEMI S.p.a.
Piazza degli Affari, 3 – 20123 Milano
PEC: deas-spa@legalmail.it

Oggetto: GARA 158 PROGRAMMA DII – Acquisizione supporto tecnico onsite ai servizi di sicurezza dell'infrastruttura della Difesa. Cap. 1412/3 – CIG B4218BF2A6 - CUP D87H24003180001 – T.D. 4780333 - E.F. 2024. IDV 1851883.

Rife: Obbligazione Commerciale nr. 44/2024 del 25/11/2024.
Codesta Ditta è risultata essere aggiudicataria della seguente fornitura, comprensiva dei relativi costi alla sicurezza, pari a euro 1.665,39 come da T.D. in oggetto:

Descrizione	Capitolo 1412/3 E.F. 2024
Acquisizione supporto tecnico onsite ai servizi di sicurezza dell'infrastruttura della Difesa , come da requisito tecnico operativo in allegato.	€. **132.480,00**
Totale imponibile	€. **132.480,00**
IVA esente ai sensi art. 72 comma 3 punto 2 del DPR 633/72	€. 0,00
TOTALE	**€. 132.480,00**

1. 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.
2. **Si precisa che la fattura elettronica dovrà essere obbligatoriamente emessa 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**.
3. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 7115/1 dell'E.F. 2024** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).
4. La fornitura/prestazione dovrà essere effettuata a cura di codesta Ditta secondo le modalità riportate nell'Obbligazione Commerciale in riferimento e dovrà essere conclusa **come nei termini stabiliti nel R.T.O. in allegato**.
5. **Direttore Esecuzione Contrattuale: Cap. Vincenzo ZERBO tel. 06-46914814 – mail: scd.uis.sas.nps.cn@cor.difesa.it.**

Il CAPO SERVIZIO AMMINISTRATIVO
Col. com. Maurizio LAMBIASE
(documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
MAURIZIO LAMBIASE
RUP AFF
In Data/On Date:
lunedì 25 novembre 2024 16:34:07

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

COMANDO PER LE OPERAZIONI IN RETE

REQUISITO TECNICO OPERATIVO

RELATIVO A

Supporto tecnico on-site ai servizi di sicurezza dell'infrastruttura della Difesa

Ottobre 2024

Digitally signed by SERGIO ANTONIO SCALESE
Date: 2024.10.10 15:49:56 CEST

PREDISPOSIZIONE DEL DOCUMENTO

Redatto da	Data
Comando per le Operazioni in Rete	07/10/2024

LISTA REVISORI

Ufficio/Sezione/Nominativo
RSCD - Ufficio Infrastrutture di Sicurezza

REGISTRO DELLE REVISIONI

Revisione	Data	Capitoli/paragrafi modificati	Osservazioni

QUESTO DOCUMENTO È COSTITUITO DA 4 PAGINE TOTALI

1. PREMESSA

Nell'attuale scenario evolutivo delle Reti e dei servizi telematici assicurati dalla Difesa a beneficio dell'Area di Vertice Interforze, degli Uffici di diretta collaborazione e delle Forze Armate, si rende necessario provvedere:

- a costanti aggiornamenti architetturali e reingegnerizzazioni dei sistemi informatici atti ad assicurare una postura di sicurezza omogenea e a contenere il rischio cibernetico compatibilmente con le *policy* di sicurezza interne, ovvero dettate dall'AgID con le Misure Minime di cui alla Circ. 18 aprile 2017, n. 2/2017 (applicazione dell'art. 14-bis del D.lgs. 7 marzo 2005, n. 82) e da ACN nell'ambito della Strategia Nazionale di Sicurezza e discendente Piano di Implementazione (2022-2026);
- alla conduzione di servizi critici che richiedono le citate misure di protezione;
- a contrastare le crescenti iniziative di attori ostili, governativi e non, presenti nel cyberspazio.

Inoltre, i seguenti fattori:

- evoluzione di prodotti e strumenti di lavoro disponibili al commercio in ottica *Cloud*;
- programmi di sviluppo di nuovi applicativi finanziati con fondi PNRR, basati su soluzioni *container* e micro-servizi;
- necessità di applicare misure di *Governance, Compliancy e Risk* (GDPR, ISO/IEC 27001, PSNC) caratterizzate da specifici controlli di sicurezza e che spesso condizionano in via sostanziale talune scelte tecniche,

ampliano notevolmente la quantità e complessità degli *asset* su cui applicare le misure di protezione.

In tale contesto si rende necessario sul piano strategico-operativo un approccio olistico alla *cyber security* che includa:

- la valutazione continua dell'esposizione *cyber* tecnologica al fine di comprendere le potenziali minacce e vulnerabilità specifiche dell'organizzazione attraverso analisi periodiche e aggiornate;
- la valutazione continua dell'esposizione *cyber* umana al fine di comprendere le potenziali minacce e vulnerabilità derivanti da comportamenti inappropriati e/o superficiali del personale, nell'utilizzo di qualsivoglia *asset* aziendale;
- la valutazione continua delle informazioni circolanti *sul web (*sia *clear i dark)* e sui *social network* afferenti all'organizzazione al fine di comprendere ciò che un attaccante può conoscere sull'organizzazione in seguito ad attività di *information gathering* è importante per poterne prevedere le mosse. Inoltre, è importante avere immediata contezza di eventuali data *leakage* che possano abilitare attacchi *cyber* (es. furto di credenziali) o rappresentare un problema di *business* (ad es. informazioni sensibili su amministrazione, progetti, etc.);
- la valutazione continua delle capacità di reazione al fine di avere contezza della reale capacità di identificazione e risposta ad un incidente informatico.

Conseguentemente lo sviluppo professionale e la verticalità di competenze del personale dell'A.D. **non sono sufficienti a far fronte in autonomia alle necessità in costante crescita** sia per volumi sia per competenze ed esperienze necessarie.

Peraltro, il Comando per le Operazioni in Rete (COR) sta perseguendo un complesso e articolato processo di potenziamento dell'infrastruttura proprietaria telematica, tra cui la realizzazione della nuova Mono Foresta Mono Dominio (MFMD) e l'evoluzione del *Data Center* mediante l'estensione alle infrastruttura del Polo Strategico Nazionale (PSN). **In tale quadro, si rende necessario disporre di un supporto tecnico *on-site* da parte di una società *leader* nelle capacità operative legate al dominio cibernetico e rivolte alla tutela della Sicurezza Nazionale e delle Istituzioni, per perseguire il citato pro-**

cesso evolutivo e condurre una valutazione approfondita in merito a potenziali minacce al fine di evitare che si presentino nuovamente vulnerabilità già riscontrate in passato.

2. OBIETTIVO

L'obiettivo del presente requisito è di poter disporre di un servizio di consulenza e supporto tecnico *on-site* da parte di una società nazionale *leader* nelle capacità operative legate al dominio cibernetico e rivolte alla tutela della Sicurezza Nazionale e delle Istituzioni. Il supporto dovrà essere assicurato da n. 4 figure[1] professionali, dotati di NOS per alta classifica, che operino, insieme alle altre figure professionali **già impiegate presso il COR,** per perseguire il citato processo evolutivo e concorrere alla valutazione complessiva dell'esposizione dell'organizzazione alle minacce *cyber*. In particolare, tali figure potranno essere impiegate in base alle esigenze nei tre Reparti del COR per effettuare le seguenti attività:

1. supporto tecnico nelle simulazioni di attacco e reverse *engineering* delle minacce osservate, pratiche, tecnologie di VA/PT ed attività varie di *hacking* e *cyber offensive*;
2. supporto per la valutazione delle attività di evoluzione del *Data Center* ed estensione alle infrastrutture del Polo Strategico Nazionale;
3. supporto al carico di lavoro in costante crescita per le attività di monitoraggio, investigazione e risposta agli incidenti;
4. analisi di Log;
5. monitoraggio costante della rete e dei sistemi aziendali per rilevare e prevenire attività sospette o tentativi di intrusione;
6. in caso di eventi di sicurezza, contribuire all'analisi dell'attacco nonché garantire una risposta tempestiva, con attuazione di misure di contenimento e procedure di ripristino, al fine di minimizzare i tempi di fermo e preservare l'integrità dei dati;
7. ulteriori esigenze che dovessero emergere nel corso del supporto e ad oggi non preventivabili.

3. TERMINI E PIANIFICAZIONE ATTIVITA'

Il luogo di effettuazione della prestazione per le n. 4 figure professionali per le attività di cui al para. 2 (da 1 a 7) è il COR Difesa (nelle sedi di Via Stresa 31/B – 00135 Roma e occasionalmente, qualora necessario, presso l'Aeroporto Militare F. Baracca, sito in via di Centocelle 301, 00175 - Roma).

Le figure professionali individuate relazioneranno ai Responsabili Tecnici ed al Direttore di Esecuzione circa le attività condotte nonché le **prestazioni orarie effettivamente svolte** da remunerare.

4. STIMA ECONOMICA

Sedi di svolgimento della prestazione lavorativa	**Attività ordinaria** Comando le operazioni in Rete nella sede di via Stresa 31/B – 00135 Roma.
Durata	(**60** giorni lavorativi)
Numero risorse	**4**, come descritto al paragrafo 2.

[1] Esperti multidisciplinari (dotati di certificazione CEH, Red Hat, OSCE, OSCP, OWP, EWPT) che concorrono alla valutazione complessiva dell'esposizione dell'organizzazione alle minacce *cyber*.