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. 93
(da citare in fattura)

Roma, 09/08/2024

Società BITCORP S.r.l.
Via Monte Bianco, 2/A - 20149 Milano
PEC: bitcorp@pec.it

Oggetto: GARA 37 (Quinto Esperimento) - Programma DII - Assistenza tecnico sistemistica finalizzata all'acquisizione di una Capacità offensiva cyber evolutiva su Sistemi di Comando C2 per il reparto Cyber Operations - CIG B2419670BF - CUP D87H24001250001 - Capitolo 1412/3 - E.F. 2024/2025. T.D. 4473488 del 27/06/2024.

Rife: Obbligazione Commerciale nr. 20/2024 del 09/08/2024.

1. Codesta Ditta è risultata essere aggiudicataria della seguente fornitura, comprensiva dei relativi costi alla sicurezza, pari a **euro 0,00** come da T.D. in oggetto:

Descrizione	Capitolo 1412/3 E.F. 2024	Capitolo 1412/3 E.F. 2025
Programma DII - Assistenza tecnico sistemistica finalizzata all'acquisizione di una Capacità offensiva cyber evolutiva su Sistemi di Comando C2 per il reparto Cyber Operations, come da Requisito Tecnico Operativo in allegato.	€. 68.000,00	€. 68.000,00
Totale imponibile	€. 68.000,00	€. 68.000,00
IVA esente ai sensi art. 72 comma 3 punto 2 del DPR 633/72	€. 0,00	€. 0,00
TOTALE	**€. 68.000,00**	**€. 68.000,00**

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. **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**. 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**.
4. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 1412/3 degli Esercizi Finanziari 2024/2025** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).
5. La fornitura/prestazione dovrà essere effettuata a cura di codesta Società secondo le modalità riportate nell'Obbligazione Commerciale in riferimento. La programmazione dei pagamenti impone, pertanto, che la Società emetterà fattura nel rispetto dei seguenti periodi temporali:
   - **1^ fattura** a conclusione della prima parte del servizio entro il **31/12/2024**, e previo riscontro favorevole delle relative prestazioni (IDV SIFAD 1788470);
   - **2^ fattura** a conclusione della restante parte del servizio entro il **31/12/2025**, e previo riscontro favorevole delle relative prestazioni (IDV SIFAD 1788704);
6. **Direttore Esecuzione Contrattuale: C.C. Vincenzo DI MICCO - tel. 06.4691.5048 - e-mail: roc.uto.sac.cs@cor.difesa.it**

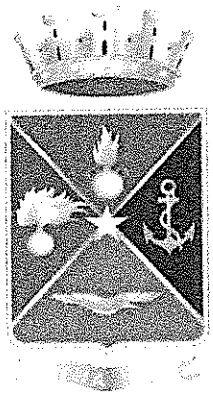
Il CAPO SERVIZIO AMMINISTRATIVO
Col. com. Maurizio LAMBIASE
(documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
MAURIZIO LAMBIASE
RUP AFF
In Data/On Date:
venerdì 9 agosto 2024 14:47:40

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

STATO MAGGIORE DIFESA

VI Reparto – Sistemi C4I e Trasformazione
Ufficio Cyber



REQUISITO TECNICO OPERATIVO

RELATIVO A

Assistenza tecnico sistemistica finalizzata all'acquisizione di una Capacità offensiva cyber evolutiva su Sistemi di Comando e Controllo relativi allo scenario Internet of Things – Protocollo CWMP

Edizione Marzo 2023

PREDISPOSIZIONE DEL DOCUMENTO

Redatto da	Data
SMD – VI Reparto Ufficio Cyber	03.2024

LISTA REVISORI

Ufficio/Sezione/Nominativo

REGISTRO DELLE REVISIONI

Revisione	Data	Capitoli/paragrafi modificati	Osservazioni

INDICE

1. PREMESSA

Le rete *Internet*, originariamente ideata per connettere più dispositivi, di solito collocati in luoghi diversi, anche remoti, consentendo lo scambio dei dati tra loro, si è progressivamente trasformata in una piattaforma in grado di offrire una molteplicità di servizi.

Tra questi servizi, ve ne sono alcuni che per loro natura richiedono l'esistenza di dispositivi dedicati, progettati esclusivamente per supportare e fornire accesso a tale classe di servizi. In questo novero rientrano anche molte piattaforme per il comando e controllo di assetti militari.

Attualmente stiamo assistendo alla fine della prima rivoluzione dell'*Internet of Things* (IoT), ove la rete svolge la funzione di sistema di controllo su scala globale e gli umani hanno già avviato un proprio processo di ibridazione con le macchine (per es. mediante *smartphone*). In questo nuovo paradigma, qualsiasi cosa può essere considerata come un *host* connesso ad *Internet*, in grado non solo di supportare tradizionali funzioni, ma di sfruttare un numero interessante di possibilità.

Nel prossimo futuro, con la massiccia introduzione della robotica su larga scala, delle applicazioni dall'ambito domestico a quelle operative in contesto militare (es. droidi da combattimento, etc.), lo IoT diventerà uno strato imprescindibile di confronto militare.

L'oramai consolidata affermazione del concetto IoT ha spinto *vendor* ed esperti di *cyber security* ad implementare, di pari passo con la crescita dei servizi svolti grazie ad Internet, sistemi di difesa capaci di mitigare i rischi, i pericoli e le minacce informatiche, con al pari l'ambizione di realizzare ciò che è comunemente noto come Zero-*Touch Provisioning*, ovvero la totale assenza di interazione utente nei processi di "*onboarding*", configurazione e gestione remota di quei dispositivi tramite cui i servizi sottoscritti vengono forniti.

La crescita esponenziale del numero di dispositivi IoT ha aumentato la richiesta di soluzioni del genere, in grado di semplificare enormemente i processi di *delivery* e ridurne notevolmente i costi. In particolare, tali soluzioni sono ancor più necessarie nell'ambito dell'*Internet of Military Things* (IoMT), ove la semplificazione dei processi e un alto grado di standardizzazione dei linguaggi sono essenziali per l'utilizzo adeguato e massivo delle soluzioni adottate.

Si aggiunga, poi, come gli scenari operativi del futuro vedranno sempre più operare le Forze Armate in ambiente urbano e in ambiti multi-dominio, secondo un approccio ibrido che richieda capacità di interazione intrusiva e non intrusiva, *overt* e *covert*, dello IoMT e dell'*Internet of Battle Things* (IoBT) con l'intera galassia dell'IoT, sia per avvalersene in termini di supporto alle operazioni che per poter disporre di un vantaggio militare, da un punto di vista offensivo e difensivo.

2. OBIETTIVI

L'obiettivo del presente RTO è definire i requisiti per la fornitura, al Reparto *Cyber Operations* (ROC) del Comando per le Operazioni in Rete (COR), di una attività di assistenza tecnico sistemistica pratica *on site* in tema di capacità offensiva *cyber* nell'ambito dei sistemi di C2 relativi allo IoT/IoMT/IoBT.

La finalità dell'intervento è far acquisire al personale del ROC competenze e capacità nella materia, al fine di consentire successivi sviluppi riguardanti l'attacco *cyber* a sistemi di Comando e Controllo afferenti a sistemi d'arma, quali droni, batterie missilistiche, aerei, mezzi blindati e corazzati, sistemi radar, natanti, etc.

3. SITUAZIONE "AS IS"

Pur avendo acquisito utile conoscenza tecnologica e capacità offensiva *cyber* su parte dei singoli dispositivi che concorrono a comporre l'IoT/IoMT/IoBT, il ROC non ha ancora maturato la piena conoscenza circa lo sfruttamento dei protocolli relativi ad ambienti infrastrutturali di comunicazione non militari. In particolare, nel citato contesto non militare si fa riferimento ad uno

dei protocolli più utilizzati per implementare il paradigma dello *ZeroTouch* in tali ambienti: il *Customer Premises Equipment* WAN *Management Protocol* (CWMP TR069-ultima versione).

4. **SITUAZIONE "TO BE" - OGGETTO E REQUISITI DELLA FORNITURA**

Per colmare il *gap* capacitivo offensivo *cyber* del personale del ROC in tale ambito, è necessario ampliare le conoscenze e le competenze dello stesso, mediante la fornitura di una assistenza tecnico sistemistica che include uno specifico pacchetto di addestramento pratico rispondente ai requisiti tecnico-operativi di seguito specificati.

R01 – Obiettivo

Far acquisire e trasferire al personale del ROC la piena conoscenza circa lo sfruttamento dei protocolli relativi ad ambienti infrastrutturali di comunicazione impiegati in ambio IoT/IoMT/IoBT, con particolare riferimento alle vulnerabilità sfruttabili delle tecnologie che implementano funzionalità *ZeroTouch* mediante il protocollo CWMP TR069-ultima versione.
Il grado di approfondimento richiesto è commisurato all'obiettivo di consentire alla Difesa di sviluppare un proprio assetto volto alla penetrazione[1] nell'ambito di infrastrutture informatiche strategiche [2] avversarie attraverso lo sfruttamento delle vulnerabilità delle tecnologie IoT/IoMT/IoBT e alla condotta di attività offensive *cyber* quali quelle tese a causarne il *Denial of Service* (DoS).

R02 – Definizione degli interventi

Le modalità di dettaglio di articolazione ed erogazione del percorso addestrativo di assistenza tecnico sistemistica dovranno essere sottoposte all'approvazione preliminare del ROC, mediante il responsabile della Difesa designato per la Direzione di Esecuzione.

R02 – Durata e articolazione

La durata complessiva dell'addestramento *on site* a mezzo di assistenza tecnico sistemistica dovrà essere di almeno 34 (trentaquattro) giornate, da erogare in presenza, articolate in 2 (due) giornate per settimana calendariale.

R03 – Docenti

Il pacchetto addestrativo di assistenza dovrà essere erogato dalla ditta appaltatrice mediante i seguenti formatori:

- n. 1 Ingegnere in presenza presso l'area addestrativa, per la supervisione diretta e la formazione del personale militare del ROC;
- n. 1 Ingegnere in remoto, per supporto e attività tecnica in rete.

R04 – Modalità di erogazione degli interventi

Il percorso addestrativo di assistenza tecnico sistemistica dovrà essere erogato in modo da consentire ai discenti di ottenere un'efficace arricchimento del proprio bagaglio tecnico conoscitivo e consentire loro di:

- riscontrare gradualmente le nozioni fornite dai formatori e maturare esperienze, nell'ambito di attività pratiche a carattere tecnico organizzate dalla ditta fornitrice in attinenza al contesto operativo di riferimento precedentemente delineato nel presente documento;

[1] Al concretizzarsi delle necessarie condizioni giuridiche.
[2] Es: Trasporti, Energia, Telecomunicazioni, altre infrastrutture critiche.

- confrontarsi con continuità con gli addestratori sulle tematiche oggetto dell' assistenza *on site*, al fine di disporre del *feedback* sui progressi conseguiti e ottenere la graduale sedimentazione delle nozioni apprese e delle esperienze maturate nelle prove pratiche.

Il percorso addestrativo di assistenza tecnico sistemistica proposto dalla ditta appaltatrice dovrà, pertanto, includere anche moduli preliminari e propedeutici alle attività tecniche oggetto delle prove pratiche.

R05 – Supporti e Ausili didattici

La ditta appaltatrice dovrà fornire tutti i supporti e gli ausili didattici necessari all'erogazione del percorso addestrativo, incluso il *syllabus* del pacchetto addestrativo redatto in aderenza all'obiettivo di far acquisire al personale del ROC la piena conoscenza del protocollo CWMP TR069-ultima versione, delle sue "debolezze"/vulnerabilità e delle modalità di possibile sfruttamento pratico nei sopracitati ambiti di operazioni *cyber*.

Si chiede altresì che la ditta fornitrice predisponga e renda disponibili, per tutta la durata dell'attività istruzionale, dimostrazioni pratiche di sfruttamento reale delle debolezze/vulnerabilità del protocollo, in uno o più possibili ambiti di interesse che saranno definiti dal responsabile del ROC designato per la direzione dell'esecuzione contrattuale.

Le dimostrazioni dovranno essere condotte passo-passo, a beneficio del personale del ROC, allo scopo di apprendere i *framework* e le relative tecniche utilizzate, consistendo l'obbiettivo ultimo del progetto non solo nella condivisione dello specifico *know-how*, ma anche in un vero e proprio *transfer of technology* metodologico relativamente a tali capacità.

La Ditta fornitrice predisporrà un *digital twin* dell'ambiente su cui svolgere l'attività di assistenza, corredato dai relativi requisiti di installazione, le procedure installative, le immagini virtuali da utilizzare sull'infrastruttura della Difesa; inoltre, la Ditta predisporrà quanto necessario per realizzare una dimostrazione su una infrastruttura non virtualizzata, attivata in base alle indicazioni concordate dalla Ditta fornitrice con il ROC.

A premessa delle attività tecniche sulle due predette infrastrutture ICT, la Ditta darà evidenza al responsabile designato del ROC circa le tecniche da essa sviluppate nell'ambito della protezione della propria identità in rete e per l'allestimento di perimetri di schermatura, anonimizzazione e mascheramento declinate esplicitamente all'interno dell'ambiente infrastrutturale a banda larga in cui il protocollo CWMP opera, evitando di fornire addestramento sulle tecniche di anonimizzazione già note per altri ambiti di applicazione (TOR, hopping IP, etc.).

Tali attività dovranno essere eseguite da specifico personale tecnico della Ditta, responsabile dello sviluppo e delle esecuzioni delle metodologie proposte ed in grado di divulgarle efficacemente al personale della Difesa designato, nonché a collaborare attivamente in tutte le attività addestrative previste dai moduli specifici.

Il complesso delle attività del corso avrà un indice d'azione da concordare preliminarmente tra il COR e la Ditta appaltatrice per le attività da svolgere sul *digital twin* e per le prove pratiche, fermo restando che la fattibilità sarà valutata in relazione alle responsabilità che ne derivano.

Pertanto, la Ditta fornirà alla Difesa:

- il citato *syllabus* del pacchetto addestrativo;
- la licenza d'uso, intestata al COR, per gli strumenti utilizzati o sviluppati per e nel contesto dell'intervento di assistenza tecnico sistemistica inclusi gli strumenti *open source* eventualmente "customizzati" dalla stessa e utilizzati nel corso del periodo addestrativo (es. emulatore CPE per CWMP "tr69-simulator");
- la licenza d'uso, intestata al COR, dei *datamodel*, dei *template dispositivo* e delle configurazioni specifiche utilizzate durante le attività addestrative e non disponibili in *open source*, replicanti caratteristiche di dispositivi reali da riutilizzare come base per eventuali personalizzazioni e utilizzi pratici futuri;

- un servizio di supporto tecnico, della durata di 24 (ventiquattro) mesi a decorrere dalla data di termine delle attività assistenza tecnico sistemistica, volto a supportare sia la risoluzione di eventuali problematiche tecniche sia l'esecuzione di attività di configurazione e l'impiego, da parte del ROC, dei suddetti elementi licenziati.

7. PROFILO ECONOMICO

Nella tabella seguente si riporta il riepilogo schematico degli oggetti di fornitura e una stima economica di massima (prezzi IVA esclusa).

N.B. Da escludere nella fase di richiesta di offerta.

Elementi di Fornitura	*Costo (IVA esclusa)*
Erogazione dell'assistenza a favore del personale Difesa, comprensiva di realizzazione ed esecuzione delle attività pratiche	*€ 136.000,00*
Fornitura ausili didattici, incl. *Syllabus*	
Rilascio delle Licenze di utilizzo degli strumenti utilizzati/sviluppati durante il corso, dei *datamodel,* dei template dispositivo e delle configurazioni specifiche non disponibili in *open source*	
Fornitura del Servizio di supporto della durata di 24 mesi	