**Randstad HR Solutions per conto di MBDA Italia, è in cerca di un:**

**Junior Comms & Security Engineer**

MBDA è l'unico gruppo europeo in grado di progettare e produrre missili e sistemi missilistici per rispondere alle più svariate esigenze operative, presenti e future, per le forze armate. MBDA Gruppo conta oltre 11.000 dipendenti, tra Francia, Inghilterra, Italia, Spagna, Germania e Stati Uniti, di cui 60 % nella funzione Engineering. Con più di 90 clienti tra le forze armate di tutto il mondo, MBDA è uno dei leader mondiali nei missili e nei sistemi missilistici. MBDA è controllata con uguali regole di Corporate Governance da Airbus (37,5%), BAE Systems (37,5%) e Leonardo (25%).

MBDA Italia vanta tre siti di eccellenza tecnologica: lo stabilimento di Roma, sede del management, della divisione seeker e del centro di produzione software; il sito di La Spezia, che si occupa prevalentemente dello sviluppo dei prodotti del settore anti-nave e che vanta uno stabilimento dedicato all’integrazione pirica; il sito di Fusaro, dedicato alla produzione meccanica, allo sviluppo dei sistemi a radio frequenza ed al centro di produzione dei radome ceramici.

**Titolo di studio:**

Laurea in Ingegneria Informatica o delle Telecomunicazioni o Elettronica;

Costituiscono titoli preferenziale: Master / corsi su ICT/Information Security e Certificazioni CCNA e CCNP

**Attività previste per il ruolo:**

La Risorsa prescelta si occuperà delle seguenti attività:

Partecipare sotto la guida di un practitioner agli studi relativi all’attività di Cyber Protection and Networking quali:

* Valutazione delle possibili minacce Cyber nei confronti di un sistema d’arma e relativa Risk Analysis;
* Definizione dei requisiti di Cyber funzionali, dimensionali, prestazionali e di hardening di un sistema d’arma;
* Progettazione dell’Architettura di comunicazione fisica e funzionale di Sistema;;
* Progettazione delle contromisure da integrare nell’architettura del sistema d’arma e dei suoi componenti;
* Esecuzione dei trade-off, allocazione dei requisiti ai sottosistemi e supporto alla selezione e test dei componenti COTS e/o sviluppo dei componenti Make;
* Definizione delle giustificazioni e dei piani di test a supporto della fase di verifica del progetto;
* Predisposizione delle informazioni necessarie a supportare il processo di certificazione del sistema d’arma e delle sue parti secondo gli standard richiesti (Common Criteria, NATO, …)

**Competenze professionali:**

* Conoscenza specialistica delle problematiche attinenti il campo della progettazione e implementazione di sistemi di comunicazione complessi (IP based e non), con particolare riferimento alle funzionalità, agli aspetti fisici e di affidabilità, alla modellizzazione e agli studi teorici di dimensionamento;
* Conoscenze legate all’ITC Security, ed in particolare:
  + degli standard per la sicurezza informatica (Common Criteria, ITSEC, ISO 27000/27001/27002/27005) e delle Norme e normative nazionali: L.124/2007, DPCM 22/7/2011, DPCM 11/04/2002 e relative linee guida;
  + dei standard/metodi/processi/tools di threat assessment;
  + dei sistemi e tecnologie di protezione (es. protezione fisica, algoritmi di cifratura, Intrusion detection systems, firewall, crypto, ecc…);
* Conoscenze legate al Networking, ed in particolare:
  + delle reti IP (protocolli di comunicazione, routing, subnetting, QoS, DHCP, spanning tree, ecc.);
  + dei protocolli di comunicazione voce su IP (VoIP);
  + Conoscenza di strumenti di simulazione e di emulazione di reti complesse;
  + Conoscenza di strumenti di valutazione delle performance di reti complesse;
* Conoscenza dei principali linguaggi di programmazione informatica;
* Conoscenze di tecniche di progettazione informatica (es. UML, ecc…);
* Conoscenza delle principali famiglie di sistemi operativi;
* Conoscenza di base di MATLAB/SIMULINK;

Completano il profilo la disponibilità a viaggiare in Italia e all’estero, l’attitudine al lavoro di team in un contesto internazionale, la capacità di analisi e sintesi e di comunicazione scritta e la flessibilità.

**Esperienze Professionale:** Neolaureato

**Costituisce titolo preferenziale:** esperienza pratica, maturata con laboratori e/o approfondimenti personali, nella programmazione e configurazione di apparati di rete e Sistemi Operativi per gli aspetti di networking e di security;

**Conoscenze linguistiche:**

Buona conoscenza della lingua inglese scritta e parlata

**Sede di lavoro:** MBDA Italia Roma

**Indirizzo mail al quale inoltrare le candidature:** [**mbda-selezione@randstad.it**](mailto:mbda-selezione@randstad.it)inserendo in oggetto “Contatto Poliba” entro il **5 Marzo 2021**