

Job Description:

“Esperto Cyber Security”

Il profilo Esperto Cyber Security che stiamo ricercando per Olivetti deve avere maturato una solida esperienza pluriennale in ambito ICT, in particolare sugli aspetti architetturali di *cyber security* e nella gestione dei processi test in ambito cyber security di software e firmware, assicurando un approccio basato sul “*Security by Design*” al fine di garantire la riservatezza, integrità e disponibilità dei dati e dei servizi digitali erogati dall’Azienda.

Avrà il compito di verificare la postura di sicurezza di soluzioni, servizi e prodotti ICT, coordinare lo svolgimento delle analisi di sicurezza nell’ambito del processo di testing della fabbrica digitale, operando in stretto raccordo con le funzioni di sviluppo ed esercizio.

Dovrà possedere una conoscenza approfondita del ciclo di vita sicuro del software e competenze sulle metodologie di sviluppo software (waterfall, devops, agile). Dovrà conoscere standard e *best practices* in materia di *cyber security*, applicandole al contesto Olivetti per definire ed implementare i necessari controlli di sicurezza.

Dovrà comprendere obiettivi e linee guida dei progetti, seguirne il disegno architetturale e coordinare le fasi di test per gli aspetti di competenza, assicurando che il prodotto finale soddisfi gli standard di sicurezza richiesti.

Verrà assunto con contratto a tempo indeterminato e farà parte di un team di eccellenza, con sede a Roma.

Requisiti professionali

- Conosce il ciclo di vita del software e le principali metodologie di sviluppo (waterfall, devops, agile)
- Ha svolto *Security Assessment* basati sugli standard ISO27001, NIST 800-53 e NIST 800-82, al fine di valutare il livello di sicurezza di sistemi e servizi digitali, definendo una remediation roadmap per indirizzare le scoperture di sicurezza emerse dalle analisi condotte
- Ha competenze in materia di *Static Application Security Testing (SAST)* per l’analisi statica del codice sorgente (validazione degli input, delle librerie utilizzate e delle API, dei parametri di configurazione, etc.)
- Ha competenze in materia di *Interactive e Dynamic Application Security Testing (IAST/DAST)* per l’analisi dinamica delle applicazioni e dei servizi
- Ha competenze in materia di *Mobile App Security Testing* per le verifiche di sicurezza delle APP Mobile
- Ha competenze in materia di *Vulnerability Assessment e Penetration Test*, condotti sia attraverso l’utilizzo di tool di testing automatici che attraverso analisi e attività manuale
- Conosce l’*Open Web Application Security Project (OWASP)*, i principali rischi evidenziati dalla Fondazione e le modalità per testarne la presenza sugli applicativi aziendali
- Conosce tool e strumenti per l’automazione dei test di sicurezza
- Conosce metodologie di sviluppo *Agile oriented* e relativi strumenti, strumenti di sviluppo DevOps CI/CD, tool di security testing, sistemi di configuration e versioning di programmazione, Content Management System, infrastructure as a code
- Conosce le tecnologie radiomobili (nelle diverse generazioni 2G/3G/4G/5G), i protocolli e le architetture M2M e IoT
- Conosce i principali protocolli industriali ed i più diffusi standard internazionali di Cyber Security di riferimento per tale ambito, quali ad esempio IEC 62443 e IEC 62351, i principali rischi di sicurezza che insistono sull’ambito *Industrial Control System*, le principali misure per la messa in sicurezza e le modalità di testing;

Stiamo cercando candidati con spiccate capacità analitiche e gestionali, orientamento al *problem solving* ed in grado applicare il principio di *Security by Design* e di coordinare l'attività di *Security Testing*, coerentemente con le attività di *quality assurance* svolte dal *Validation Team* di Olivetti.

È richiesta attitudine sistematica alla previsione e modellazione soluzioni efficaci per raggiungere il risultato atteso anche in presenza di imprevisti, visione d'insieme, capacità di razionalizzare ed ottimizzare processi produttivi; apprezziamo l'autonomia organizzativa, l'intraprendenza e la creatività; l'attitudine al lavoro in team, all'inclusività, alla condivisione della conoscenza, le capacità comunicative e relazionali.

Costituiscono titoli preferenziali:

- Ottima conoscenza della lingua inglese
- Certificazioni *Lead Auditor ISO27001*, certificazioni tecniche in materia di cybersecurity

Responsabilità

- Garantisce l'applicazione del principio di *Security by Design*, identificando le misure di sicurezza da applicare a nuove soluzioni/progetti
- Verifica le caratteristiche di *cyber security* di nuovi servizi e prodotti tecnologici, da integrare nell'ecosistema Olivetti
- Definisce i controlli di sicurezza da applicare nel ciclo di vita del software e li implementa, valutando il livello di rischio residuo delle soluzioni, siano esse basate su software standard, IoT o mobile APP
- Certifica la postura di *cyber security* di nuove soluzioni o di nuove release di soluzioni esistenti, indirizzando eventuali azioni correttive
- Supporta la definizione, la progettazione e l'esecuzione dei test di sicurezza su sistemi e applicativi, contribuisce all'analisi dei risultati e garantisce un adeguato reporting verso le funzioni competenti
- Progetta, implementa e monitora i report sugli indici di prestazione (SLA/KPI/KPO), per misurare l'efficacia dei processi di competenza ed apportare le opportune migliorie in ottica di *continuous improvement*
- Identifica i tool a supporto del processo di *security testing* e ne garantisce l'adozione e l'utilizzo nei processi operativi