CORSI PROFESSIONALI

Cybersecurity Architect

I partecipanti intraprenderanno un viaggio immersivo nel complesso mondo della sicurezza informatica. Dall'analisi delle sofisticate minacce fino alla creazione di strategie di difesa robuste, il corso copre una gamma di competenze cruciali per diventare architetti di sicurezza informatica competenti in grado di progettare sistemi resilienti e sicuri. Il corso mira a formare professionisti in grado di concepire, progettare e gestire soluzioni di sicurezza all'avanguardia, contribuendo a difendere le risorse digitali in un mondo sempre più interconnesso.

Durata in ore (sincrone + asincrone): 300 (130 + 170)

Numero di edizioni: 1 (gen – lug)

Composizione del corso: competenze digitali avanzate + competenze trasversali modulo da 15 ore + competenze di specializzazione

Obiettivi: sviluppare competenze nell'utilizzo di strategie di difesa, progettazione di architetture sicura, analisi delle minacce, conformità e governance, risposta agli incidenti, creazione di una cultura di sicurezza

Figure professionali di riferimento: cybersecurity architect, cybersecurity engineer, cybersecurity analyst

Formatori: Piergiorgio Ricci, Roberta Moretti

Attestato: micro certificazioni e badge digitali con verifica delle competenze

PROGRAMMA COMPETENZE DIGITALI AVANZATE

MODULO	MACRO ARGOMENTI
Ricerca di informazioni	• Valutare le informazioni sul Web
IT Security	• Concetti di base • Le principali misure di sicurezza online • Le principali tecniche di violazioni dei dati personali • Misure per la sicurezza dei file • I diversi tipi di malware • Gli strumenti per difendersi dai malware • I diversi tipi di reti informatiche • La sicurezza delle reti informatiche • La sicurezza nelle reti wireless • Gli hotspot

	• Il browser e la sicurezza online • Navigare in sicurezza • Posta elettronica • Reti sociali • Messaggistica istantanea • Dispositivi mobili • Il backup dei dati • Eliminare i dati
Gestione database	• Nozioni preliminari • Creare una tabella • La visualizzazione Struttura • Mettere in relazione le tabelle • Query di comando • Creazione guidata delle query • Le query parametriche • Usare le query per filtrare i record del database • Ultime operazioni sulle query • Creare una maschera • Creare una maschera da zero • Creare un report • Creare un report da zeri

PROGRAMMA COMPETENZE TRASVERSALI

Modulo da 15 ore	• Introduzione al concetto di competenze (hard e soft) e di mindset (dinamico e digitale) • Introduzione al bilancio delle competenze e alla sua importanza • Presentazione di strumenti di autovalutazione per il proprio bilancio: competenze, punti di forza e valori.

PROGRAMMA COMPETENZE DI SPECIALIZZAZIONE

MODULO	MACRO ARGOMENTI
Fondamenti sulla sicurezza delle applicazioni web	• Principali rischi e minacce legate alla sicurezza delle applicazioni web • Esplorazione delle best practice per la protezione delle applicazioni web
Testing di sicurezza delle applicazioni web	• Introduzione ai concetti di testing di sicurezza delle applicazioni web • Utilizzare strumenti per identificare vulnerabilità
Protezione delle applicazioni web dagli attacchi più comuni	• Approfondimenti sugli attacchi più comuni alle applicazioni web • Tecniche di mitigazione e prevenzione
Sicurezza delle API e delle applicazioni mobili	• Comprendere la sicurezza delle API e delle applicazioni mobili • Proteggere API e applicazioni mobili da minacce come la manipolazione dei dati e l'iniezione di codice
Introduzione al concetto di Zero Trust	• Principi e filosofie • Le sfide della sicurezza tradizionale e l'approccio Zero Trust come soluzione
Implementazione dell'Architettura di Sicurezza Zero Trust	• Componenti chiave • Come implementare i principi di Zero Trust all'interno di un'organizzazione
Ruolo dell'Identity and Access Management (IAM) nel modello Zero Trust	• Il ruolo critico della gestione delle identità e degli accessi • Esplorazione di strumenti e tecnologie di IAM
Monitoraggio e rilevamento delle minacce in un'architettura Zero Trust	• Monitorare e rilevare le minacce • Strumenti e tecniche per il monitoraggio e la risposta agli incidenti
Sicurezza del Cloud	• Esplorazione delle best practice • Proteggere le applicazioni e i dati sensibili ospitati in ambienti cloud

Incident Response e Disaster Recovery	• Processi di incident response e disaster recovery • Linee guida per la gestione degli incidenti e il ripristino delle operazioni
Compliance e normative di sicurezza	• Principali normative e standard di sicurezza • Garantire la conformità alle normative di sicurezza e proteggere i dati dei clienti
Comunicazione dei risultati della sicurezza	• Strategie per comunicare i risultati delle attività di sicurezza • Come presentare le informazioni sulla sicurezza in modo chiaro e comprensibile