MASTER CYBER DEFENSE

Master di Cyber Defense - FORMAZIONE A DISTANZA

INIZIO CORSO: **giovedì 19 settembre 2024**
DURATA: **40 ore**
ORARIO LEZIONI: dalle ore 14.00 alle ore 17.30
PREZZO: **3.220,80 € (2.640,00 € + IVA)**

Panoramica corso:

CYBER DEFENSE È
Un percorso strutturato con l'obiettivo di supportare i corsisti nella gestione della Sicurezza Informatica.

GLI OBIETTIVI
• Conoscenza è difesa: impara a conoscere le minacce che mettono a rischio la tua organizzazione.
• Resilienza: padroneggia le best practice e gli strumenti per difendere il tuo perimetro digitale.
• Il fattore umano: la Cyber non è solo tecnologia, proteggerà i tuoi dipendenti.
• Vai oltre la superfice: approfondisci la Threat Intelligence e conosci il dark web.
• Costruisci la sicurezza: come impostare un framework efficace ed efficiente.
• Worst case scenario: scegli come affrontare un Data Breach.

Sei punti fondamentali, un percorso completo ed esaustivo per comprendere i rischi, riconoscerli e contrastarli in maniera efficace.

Calendario corso: 19-26 settembre e 3 ottobre | 10-17-24 ottobre |7-14-21 novembre | 28 novembre e 5-12 dicembre dalle 14.00 alle 17.30. (Le ultime lezioni di ogni modulo saranno con orario 14.00-17.00).

Argomenti trattati:

PRIMO MODULO (10 ore)

Calendario: **19-26 settembre e 3 ottobre 2024**

“Ingegneria Sociale e OSINT: Strumenti e Strategie di Sicurezza Informatica”

In questo corso, ti immergerai nel mondo della cybercultura e della sicurezza informatica, con un focus particolare su due aspetti cruciali: l’ingegneria sociale e l’OSINT (Open Source Intelligence).

Cosa imparerai?
• Difenditi dagli attacchi di ingegneria sociale
• Sfrutta l’OSINT per raccogliere informazioni
• Impara (facendo) come nascono gli attacchi di ingegneria sociale personalizzati

---

SECONDO MODULO (10 ore)
Calendario: **10-17-24 ottobre 2024**

“Cyber Risk e sicurezza delle informazioni: dalla Teoria alla Pratica”

In questo corso, ti immergerai nelle principali tecniche e nei migliori strumenti per la valutazione e la gestione del Cyber Risk, con un focus particolare sull’Information Security Risk e sul Privacy Risk.

Cosa imparerai?
• Gli standard internazionali di riferimento
• Terminologia, metodologie e tecniche
• Modelli di gestione del rischio
• Policy compliance

TERZO MODULO (10 ore)
Calendario: **7-14-21 novembre 2024**

“Ethical Hacking: Come Proteggerei Sistemi dalle Minacce informatiche”

In questo corso intensivo, ti immergerai completamente nell’Ethical Hacking, acquisendo una solida conoscenza teorica e pratica delle tecniche utilizzate dagli hacker per penetrare i sistemi informatici.

Cosa imparerai?
• I concetti base dell’Ethical Hacking
• Le principali metodologie di attacco informatico
• Strumenti e tecniche di Vulnerability Assessment
• Le fasi del Penetration Test
• Come difendersi dagli attacchi informatici

QUARTO MODULO (10 ore)
Calendario: **28 novembre e 5-12 dicembre2024**

“Risposta agli Incidenti e Continuità Operativa: Strumenti e Best Practice”

In questo corso immersivo, acquisirai le competenze e gli strumenti necessari per gestire efficacemente gli incidenti di sicurezza informatica nella tua azienda.

Destinatari:

ll corso si rivolge a tutti coloro che vogliono acquisire conoscenze, metodologie e strumenti per la gestione e la tutela del perimetro aziendale e dei dati sensibili.

Tra i principali professionisti:
• Personale IT e ICT
• Responsabili Cyber Security
• Auditor
• DPO
• Legal Office
• CEO, CISO, CSO, CIO
• Decision Maker e Impreditori

Le caratteristiche e il taglio formativo particolarmente innovativo ed efficace rendono il percorso adatto anche a Studenti di Ingegneria, Informatica, e Computer Science per integrare il loro curriculum accademico con nozioni, concetti ed esercitazioni pratiche nonché e a tutti coloro che sono appassionati di Cyber Security e vorrebbero arricchire il proprio bagaglio personale.