

MODULO CYBER DEFENSE

Risposta agli Incidenti e Continuità Operativa: Strumenti e Best Practice - FORMAZIONE A DISTANZA

INIZIO CORSO: giovedì 28 novembre 2024

DURATA: 10 ore

ORARIO LEZIONI: dalle ore 14.00 alle ore 17.30

PREZZO: 805,20 € (660,00 € + IVA)



Panoramica corso:

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

Cosa imparerai?

- Progetta, sviluppa e implementa piani di risposta agli incidenti: scoprirai le best practice per creare piani di risposta completi e collaudati che ti aiuteranno a minimizzare l'impatto di un incidente informatico.
- Analizza l'impatto aziendale: imparerai a valutare le potenziali conseguenze di un incidente informatico sulla tua azienda, in termini di perdite finanziarie, danni alla reputazione e interruzione del servizio.
- Attua piani di continuità aziendale e disaster recovery: saprai garantire la continuità operativa della tua azienda in caso di un incidente informatico, grazie a piani di continuità aziendale e disaster recovery ben definiti.
- Scopri i Framework di riferimento: approfondirai i principali Framework di riferimento per la gestione degli incidenti informatici, come il NIST Cybersecurity Framework, per allineare le tue pratiche con gli standard del settore.
- Gestisci Data Breach e Incident Response: imparerai a gestire efficacemente le violazioni dei dati e gli incidenti di sicurezza, minimizzando i danni e conformandoti alle normative vigenti.

Obiettivi del 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 superficie: 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.

Argomenti trattati:

Partner tecnico

[Swascan](#) è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa. È la prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security Testing e Threat Intelligence, oltre ad essere un centro di eccellenza di Cyber Security Research. Swascan è stata premiata con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo. Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo un'azienda, dunque, ma un gruppo italiano e un hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

Destinatari:

Il 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.