Cybersecurity Management Lead Implementer

CODICE	**DT0299**
DURATA	**5 gg**
PREZZO	**1.790,00 €**
EXAM	

DESCRIZIONE

Al giorno d'oggi le organizzazioni sono interessate da un panorama digitale in continua evoluzione e devono costantemente affrontare nuove minacce e attacchi informatici complessi e sofisticati.

C'è un bisogno pressante di persone qualificate in grado di gestire e implementare efficacemente solidi programmi di cybersecurity per contrastare queste minacce.

Il nostro corso di formazione Cybersecurity Management, Lead Implementer è stato sviluppato per rispondere a questa esigenza.

I discenti apprenderanno i concetti fondamentali di cybersecurity, le strategie, le metodologie e le tecniche utilizzate per stabilire e gestire efficacemente un programma di cybersecurity basato sulle indicazioni degli standard internazionali e sulle best practice di settore per la cybersecurity.

Inoltre, questo corso di formazione consente ai discenti di migliorare la preparazione e la resilienza della propria organizzazione contro le minacce informatiche.

OBIETTIVI RAGGIUNTI

- Spiegare i concetti fondamentali, le strategie, le metodologie e le tecniche utilizzate per implementare e gestire un programma di cybersecurity.
- Spiegare la relazione tra ISO/IEC 27001, NIST Cybersecurity Framework e altri standard e framework rilevanti.
- Comprendere il funzionamento di un programma di cybersecurity e dei suoi componenti.
- Supportare un'organizzazione nella gestione, nel mantenimento e nel miglioramento continuo del proprio programma di cybersecurity.

TARGET

- Manager e dirigenti coinvolti nella gestione della cybersecurity
- Persone incaricate dell'implementazione pratica di strategie e misure di cybersecurity

- Professionisti dell'IT e della sicurezza che desiderano avanzare di carriera e contribuire in modo più efficace agli sforzi di cybersecurity
- Professionisti responsabili della gestione del rischio di cybersecurity e della conformità all'interno delle organizzazioni

PREREQUISTI

I requisiti principali per partecipare a questo corso di formazione sono la comprensione dei concetti fondamentali della cybersecurity.

CONTENUTI

Giorno 1

Introduzione alla cybersecurity e avvio dell'implementazione di un programma di cybersecurity.

- Obiettivi e struttura del corso di formazione
- Standard e quadri normativi
- Concetti fondamentali di cybersecurity
- Programma di cybersecurity
- L'organizzazione e il suo contesto
- Governance della cybersecurity

Giorno 2

Ruoli e responsabilità nella cybersecurity, gestione del rischio e meccanismi di attacco

- Ruoli e responsabilità nella cybersecurity
- Asset Management
- Risk Management
- Meccanismi di attacco

Giorno 3

Controlli di cybersecurity, comunicazione, sensibilizzazione e formazione

- Controlli di sicurezza informatica
- Comunicazione sulla sicurezza informatica
- Sensibilizzazione e formazione

Giorno 4

Gestione, monitoraggio e miglioramento continuo degli incidenti di sicurezza informatica

- ICT readiness in business continuity
- Incident Management in cybersecurity

Giorno 5 Mattina

Gestione del miglioramento e della comunicazione ICT

- Misurazione e reporting delle prestazioni e delle metriche di cybersecurity
- Miglioramento continuo
- Chiusura del corso di formazione

Giorno 5 Pomeriggio

Esame finale

- Dominio 1 - Concetti fondamentali della cybersecurity
- Dominio 2 - Avvio del programma di cybersecurity e governance della cybersecurity
- Dominio 3 - Definizione dei ruoli e delle responsabilità di cybersecurity e gestione dei rischi
- Dominio 4 - Selezione dei controlli di cybersecurity
- Dominio 5 - Stabilire programmi di comunicazione e formazione in materia di cybersecurity
- Dominio 6 - Integrazione del programma di cybersecurity nella gestione della continuità operativa e degli incidenti.
- Dominio 7 - Misurare le prestazioni del programma di cybersecurity e migliorarlo continuamente.