AI-PACT Tempo Innovation Source

neverbeforeitalia.it

Livello Intermedio (24 ore)

CORSO DI CYBERSECURITY

Premessa

Rivolto a chi ha già una conoscenza di base della **cybersecurity**, questo corso intermedio approfondisce le **tecniche di difesa e le strategie per affrontare minacce più avanzate**. I partecipanti impareranno a gestire e rispondere a incidenti di sicurezza, ad implementare controlli di sicurezza delle reti e a comprendere i requisiti di conformità normativa. Questo corso prepara i professionisti a svolgere ruoli di sicurezza IT più complessi all'interno delle organizzazioni.

A chi è rivolto?

Il corso è destinato a chi possiede già una conoscenza di base della cybersecurity o ha completato il corso di livello base. È adatto a professionisti IT, amministratori di rete e studenti di informatica che desiderano **approfondire le proprie competenze in sicurezza delle reti, gestione degli incidenti e conformità normativa**. Questo corso è ideale per coloro che vogliono svolgere ruoli di sicurezza IT più avanzati all'interno delle organizzazioni.

Obiettivi

- Approfondire la conoscenza delle **minacce avanzate** e delle **metodologie di attacco**.
- Implementare tecniche e strumenti per la **protezione di reti** e **sistemi informatici**.
- Gestire e rispondere in modo efficace a **incidenti di sicurezza informatica**.
- Applicare **principi di sicurezza** alle applicazioni e ai dati, compresa la cifratura e la gestione delle chiavi.
- Comprendere e conformarsi alle **normative e alle linee guida sulla sicurezza informatica** (es. GDPR, ISO 27001).

Programma didattico

Modulo 1: threat landscape e analisi delle minacce (6 ore)

- tipi di minacce avanzate: APT, ransomware, attacchi DDoS;
- analisi di incidenti reali;
- metodi di attacco: tecniche di social engineering, attacchi man-in-the-middle;
- analisi delle vulnerabilità e gestione del rischio.

Modulo 2: sicurezza di rete e gestione degli incidenti (8 ore)

- implementazione di firewall, IDS/IPS, e VPN;
- monitoraggio della rete con strumenti come Wireshark;
- procedure di risposta agli incidenti e gestione delle violazioni;
- logging e analisi dei log per il rilevamento delle intrusioni.

Modulo 3: sicurezza delle applicazioni e dei dati (6 ore)

- introduzione alla sicurezza delle applicazioni web (OWASP Top 10);
- pratiche di coding sicuro;
- protezione dei dati: cifratura, gestione delle chiavi;
- sicurezza dei database e prevenzione delle iniezioni SQL.

Modulo 4: normative e compliance in cybersecurity (4 ore)

- introduzione alle normative sulla sicurezza (GDPR, ISO 27001);
- compliance e best practice;
- creazione di policy di sicurezza e linee guida aziendali;
- implementazione di programmi di sensibilizzazione alla sicurezza.