AI-PACT Tempo Innovation Source

neverbeforeitalia.it

Livello Avanzato (24 ore)

CORSO DI CYBERSECURITY

Premessa

Progettato per **professionisti della sicurezza informatica** con esperienza, questo corso avanzato si concentra su **tecniche sofisticate di sicurezza**, tra cui penetration testing, sicurezza del cloud e risposta agli incidenti di alto livello. I partecipanti impareranno a identificare, analizzare e mitigare minacce avanzate, oltre a sviluppare strategie di sicurezza aziendale. Al termine, saranno in grado di gestire infrastrutture complesse e rispondere efficacemente a una vasta gamma di cyber attacchi.

A chi è rivolto?

Questo corso è rivolto a professionisti della sicurezza informatica con esperienza pregressa, che desiderano **acquisire competenze avanzate** in penetration testing, gestione della sicurezza cloud, e risposta agli incidenti complessi. È adatto a specialisti di sicurezza IT, analisti di sicurezza, amministratori di sistemi e ingegneri di rete che mirano a **ruoli di leadership nel campo della cybersecurity** o che vogliono **affinare le loro competenze** per affrontare minacce sofisticate in ambienti IT complessi.

Obiettivi

- Sviluppare competenze di **penetration testing** e **hacking etico**.
- Implementare e gestire **misure di sicurezza avanzate** per infrastrutture cloud e virtualizzate.
- Rilevare e rispondere a **minacce sofisticate** utilizzando strumenti di analisi e monitoraggio in tempo reale.
- Creare e gestire **piani di sicurezza aziendale**, inclusi i piani di continuità operativa e disaster recovery.
- Applicare tecniche di **valutazione del rischio** e sviluppare **strategie di sicurezza** per ambienti IT complessi.

Programma didattico

Modulo 1: penetration testing e hacking etico (8 ore)

- metodologie di penetration testing;
- utilizzo di strumenti avanzati: Metasploit, Nmap, Burp Suite;
- simulazione di attacchi reali su ambienti di laboratorio;
- tecniche di evasione dei sistemi di sicurezza.

Modulo 2: sicurezza delle infrastrutture e del cloud (6 ore)

- sicurezza delle infrastrutture virtuali e cloud (AWS, Azure);
- implementazione della sicurezza nei container (Docker, Kubernetes);
- monitoraggio e logging nei sistemi cloud;
- best practice per la sicurezza in ambienti ibridi.

Modulo 3: advanced threat detection e incident response (6 ore)

- rilevamento delle minacce avanzate (APT, malware persistente);
- utilizzo di SIEM per l'analisi in tempo reale;
- procedure avanzate di risposta agli incidenti;
- cyber threat intelligence e analisi comportamentale.

Modulo 4: pianificazione della sicurezza e risk management (4 ore)

- valutazione e gestione del rischio avanzata;
- sviluppo di piani di continuità operativa e disaster recovery;
- test di sicurezza: red team/blue team exercises;
- strategie di sicurezza a livello aziendale e sviluppo di policy avanzate.