COESIONE ITALIA 21-27 TOSCANA | Cofinanziato dall'Unione europea | Regione Toscana | GIOVANISÌ

CYBER SECURITY

VOUCHER
Professionisti

FINANZIATI
Regione Toscana

Descrizione del corso

Questo percorso formativo è progettato per coloro che sono pronti a immergersi nel dinamico mondo della Cyber Security, fornendo le fondamenta per una carriera di successo e la consapevolezza necessaria per navigare in un ambiente digitale sempre più complesso.

Nell'era digitale di oggi, le informazioni rappresentano uno dei beni più preziosi. La rapida digitalizzazione dei servizi, l'espansione della connettività e l'introduzione di dispositivi sempre più intelligenti hanno reso il cyber spazio un terreno fertile per opportunità, ma anche per minacce. La Cyber Security non è più un optional, ma una necessità vitale per individui, aziende e nazioni. Di fronte a minacce in costante evoluzione, la formazione in questo campo assume un'importanza cruciale.

Il corso di Cyber Security mira a fornire ai partecipanti una solida comprensione dei concetti chiave che definiscono il panorama della sicurezza informatica. L'obiettivo principale è di dotare gli studenti delle competenze necessarie per identificare, prevenire e rispondere efficacemente alle minacce informatiche, garantendo la protezione delle risorse informative. Attraverso un mix equilibrato di teoria e pratica, gli studenti saranno preparati a affrontare sfide reali, imparando a bilanciare le necessità operative con le esigenze di sicurezza.

L'approccio didattico del corso si fonda su tre pilastri principali:

1. Conoscenza teorica: Una profonda comprensione dei principi, delle tecniche e delle metodologie che formano la base della Cyber Security. Questo permette di comprendere le ragioni sottostanti alle pratiche di sicurezza, rendendo gli studenti non solo capaci di applicare soluzioni esistenti, ma anche di adattarsi alle nuove minacce.
2. Abilità Pratiche: L'importanza di mettere in pratica la teoria attraverso esercitazioni, laboratori e simulazioni, assicurando che gli studenti siano pronti per situazioni reali.
3. Visione Futuristica: Mentre la formazione si concentra sulle minacce e sulle soluzioni attuali, è essenziale avere uno sguardo verso il futuro, comprendendo le tendenze emergenti e preparandosi alle sfide di domani.

Moduli formativi

Modulo 1: Fondamenti di Cybersecurity (20 ore di cui 20 in FAD)

- Introduzione, cenni storici e contesto
- Principi generali
- GDPR, ISO 27001, Privacy by design, Security by design
- Autenticazione, autorizzazione e controllo degli accessi
- Buone pratiche e comportamenti da evitare
- Sfide emergenti e tendenze

Modulo 2: Crittografia e reti
(20 ore di cui 20 in FAD)

- Crittografia, algoritmi simmetrici e asimmetrici, funzioni di hashing
- Firme digitali, certificati e chiavi
- Sicurezza per hardware, software e dati
- Fondamenti delle reti: TCP/IP, protocolli, topologie
- Firewall, IDS/IPS, VPN
- Sicurezza Web, OWASP
- Sicurezza cloud e IoT
- Deep Web, Dark Web

Modulo 3: Risk assessment
(20 ore di cui 20 in FAD)

- Gestione del rischio, probabilità e impatto
- Metodologie di Risk assessment
- NIST Cybersecurity Framework
- Piani di sicurezza e azioni di remediation
- Manutenzione e hardening
- Risposta agli incidenti
- Bollettini di sicurezza CVE

Modulo 4: Vulnerability scanning e penetration testing
(20 ore di cui 20 in FAD)

- Vulnerabilità note e Zero-day
- Vulnerability Scanning
- Open Source Intelligence
- Analisi forense
- Tecniche di penetration testing
- Sistemi e strumenti

Modulo 5: Social engineering, ethical hacking, infrastrutture
(16 ore di cui 20 in FAD)

- Social engineering: esempi, tecniche e strumenti
- Phishing e baiting, furti di identità, truffe
- Ethical hacking e risvolti socio-politici
- Sicurezza delle infrastrutture reali e virtuali

Modulo 6: Principali minacce nel metaverso
(16 ore di cui 20 in FAD)

- Privacy, Data breach, Data loss, Biometrics threats
- Crypto/Token/NFT scams, furti e truffe, frodi finanziarie
- Darkverse: un dark web nel metaverso
- Attacchi Cyber-Physical
- Virtual/Augmented/Mixed/Extended Reality Threats