Finanziato dall'Unione europea NextGenerationEU

Regione Lombardia

TIME VISION FORMAZIONE CONSULENZA LAVORO

Informatica

Cybersecurity: privacy e sicurezza dei dati

OBIETTIVI

Il corso "Cyber Security: Privacy e Sicurezza dei Dati" è progettato per formare professionisti capaci di proteggere i sistemi informatici e i dati sensibili da minacce informatiche, nel rispetto delle normative vigenti.

Obiettivi Formativi

- Sviluppare competenze avanzate nell'identificazione di vulnerabilità dei sistemi informatici
- Padroneggiare tecniche di protezione da attacchi informatici comuni e avanzati
- Acquisire conoscenze approfondite sul GDPR e sulle normative sulla privacy
- Implementare soluzioni di sicurezza per reti, cloud e dispositivi mobili
- Apprendere metodologie di penetration testing e valutazione dei rischi
- Sviluppare competenze nella gestione degli incidenti di sicurezza
- Progettare e implementare policy di sicurezza informatica aziendali efficaci
- Acquisire competenze nella crittografia e nei sistemi di autenticazione avanzati

Questo percorso formativo prepara figure professionali in grado di proteggere le infrastrutture IT aziendali, implementare soluzioni di sicurezza conformi alle normative vigenti e rispondere efficacemente agli incidenti informatici in un panorama di minacce in continua evoluzione.

MODULI

Fondamenti di Cyber Security
- Principi di sicurezza informatica
- Panoramica delle minacce cyber attuali
- CIA Triad (Confidenzialità, Integrità, Disponibilità)
- Security by design e approccio proattivo
- Elementi base di risk assessment

Normativa GDPR e Privacy
- Quadro normativo europeo sulla protezione dei dati
- Principi fondamentali del GDPR
- Ruoli e responsabilità (DPO, titolare, responsabile)
- Valutazione d'impatto sulla protezione dei dati (DPIA)
- Gestione delle violazioni dei dati (data breach)

Tecniche di Attacco e Difesa
- Social engineering e phishing
- Malware, ransomware e loro evoluzione
- Attacchi web (SQL injection, XSS, CSRF)
- Tecniche di attacco alle reti
- Strategie difensive e contromisure

Sicurezza delle Reti
- Architetture di rete sicure
- Configurazione e gestione di firewall
- Implementazione di VPN
- IDS/IPS (Sistemi di rilevamento e prevenzione delle intrusioni)
- Segmentazione della rete e zero trust

Penetration Testing
- Metodologie di penetration testing
- Ethical hacking: approcci e strumenti
- Vulnerability assessment
- Reporting e documentazione dei test
- Remediation delle vulnerabilità

Crittografia e Autenticazione
- Principi di crittografia moderna
- Gestione delle chiavi e certificati
- Autenticazione a più fattori (MFA)
- Single Sign-On e gestione delle identità
- Secure coding e implementazione della crittografia

Cloud e Mobile Security
- Modelli di sicurezza nel cloud
- Protezione dei dati in ambienti cloud
- Sicurezza delle applicazioni mobili
- BYOD e gestione dei dispositivi mobili
- Container e virtualizzazione sicura

Incident Response
- Framework per la gestione degli incidenti
- Creazione di un piano di incident response
- Digital forensics e analisi post-incidente
- Threat hunting e monitoraggio proattivo
- Disaster recovery e business continuity

Livello di accesso Diploma

Durata 40 h

Modalità di svolgimento Aula

Visita la pagina sul nostro sito dedicata alla misura **GOL Lombardia**

Il programma è finanziato dal Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 5 "Inclusione e coesione", Componente 1 "Politiche per il lavoro" Riforma 1.1 "Politiche attive del Lavoro e Formazione", finanziato dall'Unione Europea – Next Generation EU

GOL Garanzia Occupabilità Lavoratori