ISTITUTO FORMATIVO EUROPEO ITALIA - Cyber Security Specialist



CERTIFICATION COMPANY







Istituto Formativo Europeo Italia è un Centro di Formazione Autorizzato **MOS**, **MTA**, **ACA**, **ACU**, **HP** e **IC3**, che ha come obiettivo lo sviluppo di una buona strategia di promozione dei programmi internazionali di certificazione Certiport presenti.

Il nostro Certiport Center soddisfa un alto livello qualitativo di erogazione della formazione in aula finalizzata al trasferimento delle competenze ed al conseguimento delle certificazioni.

L'accreditamento in qualità di Certiport Center assicura un supporto formativo e di certificazione capace di coprire ogni esigenza, dalla prima alfabetizzazione informatica alla certificazione delle competenze di settore avanzato altamente professionalizzante.

Adobe CERTIFIED ASSOCIATE

Adobe

La Certificazione ACA è pensata per coloro che utilizzano frequentemente il software per professione o per passione.

AUTODESK.

Autodesk

Autodesk Certifitied User è una Certificazione che attesta le conoscenze della progettazione digitale.

CompTIA.

CompTia

La Certificazione CompTIA attesta le competenze necessarie per operare in modo professionale nell'ambito del supporto tecnico informatico Hardware Software e di Rete.

EC-COUNCIL | ACADEMIA PARTNER

EC-Council | Academy

Siamo ufficialmente riconosciuti a livello di Academia a garanzia della nostra qualità, EC-Council è noto soprattutto nel settore della sicurezza IT, ed offre certificazioni in settori come disaster recovery, sicurezza del software, analisi forensi digitali e conoscenze generali sulla sicurezza IT.

ORACLE

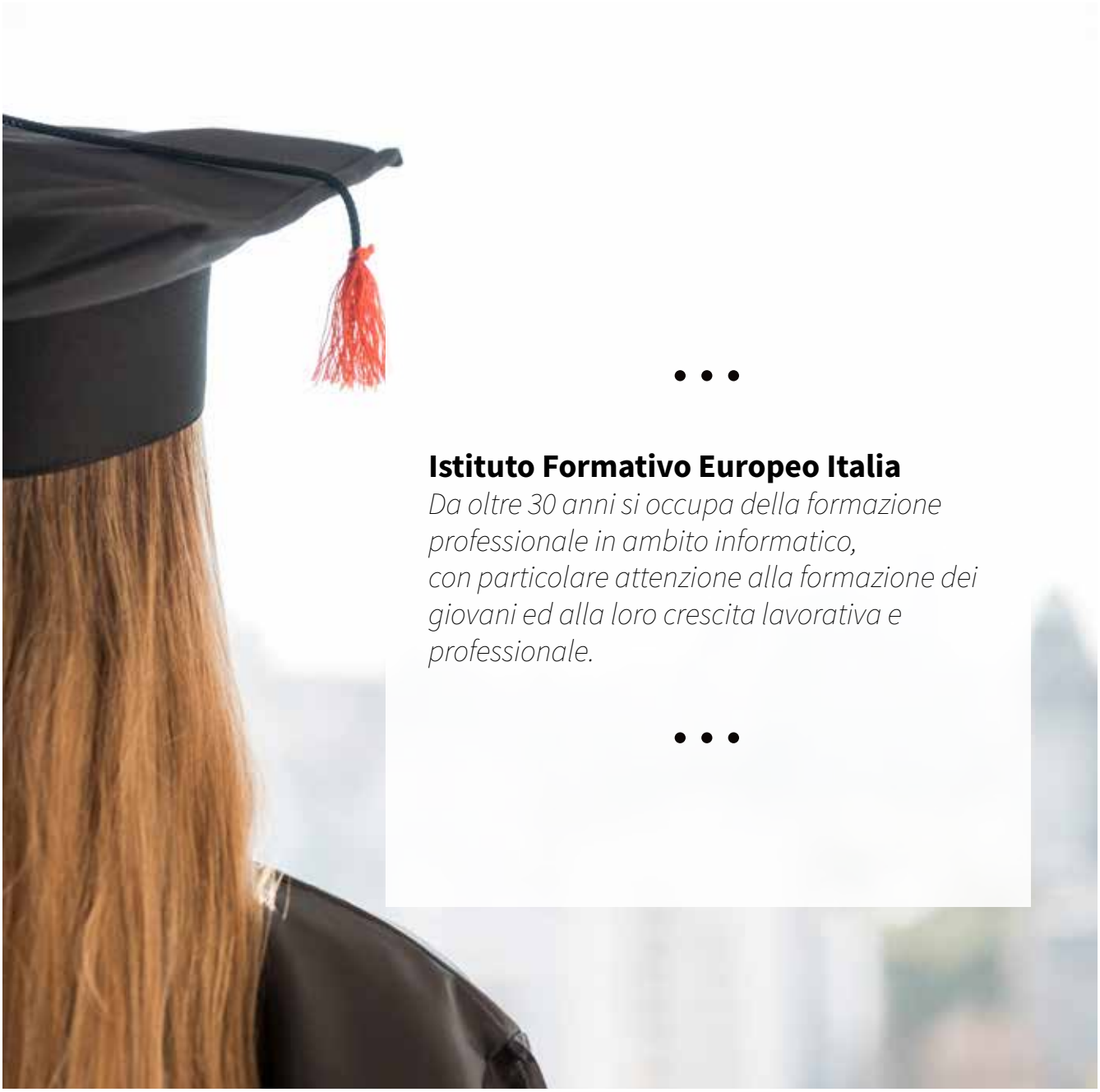
Oracle

La Certificazione Oracle, rappresenta una prova della capacità del programmatore di comprendere la sintassi di base e la struttura del linguaggio di programmazione Java.

Microsoft

Microsoft

La Certificazione Microsoft Office ti permette di distinguerti all'interno del competitivo mercato del lavoro di oggi mostrando le tue competenze di Back Office.



• • •

Istituto Formativo Europeo Italia

Da oltre 30 anni si occupa della formazione professionale in ambito informatico, con particolare attenzione alla formazione dei giovani ed alla loro crescita lavorativa e professionale.

• • •

CONSULENZA DI CARRIERA



“ Imparare ad esaltare e migliorare le tue qualità.

Requisito essenziale per valorizzare il nostro futuro.”

La Consulenza di Carriera è un’attività formativa focalizzata sulla carriera, che attraverso l’analisi della storia professionale e delle caratteristiche personali e motivazionali del cliente, lo aiuta ad aumentare la consapevolezza di se e delle proprie capacità e specificità professionali, al fine di implementare, riposizionare o intraprendere la propria attività lavorativa affrontando il mercato del lavoro in modo più mirato ed efficace.



OBIETTIVO LAVORO

I Colloqui di Lavoro

Assicurarsi un buon posto di lavoro è un obiettivo importante, una svolta decisiva per vita e carriera.

Ma l'intervista del selezionatore spaventa molti candidati, crea stress e agitazione.

Affrontare con successo un colloquio di lavoro richiede perciò equilibrio e preparazione.

I candidati, infatti, ai colloqui di lavoro, vengono scelti non solo sulla base di studi ed esperienze: contano molto il modo di presentarsi e la capacità di entrare in sintonia con gli intervistatori.

Allora, bisogna "allenarsi": raccogliere informazioni, valutare la propria aderenza al profilo ricercato, fare delle prove.

Dopo un'intensa preparazione su questi e altri temi nelle lezioni di consulenza di carriera, i nostri candidati vengono intervistati e valutati da professionisti del settore.

Attraverso la collaborazione con agenzie interinali ed aziende su tutto il territorio nazionale che ricercano profili di alto spessore informatico, i nostri candidati vengono segnalati direttamente agli uffici del personale delle stesse, segnalando l'elevato profilo tecnologico.





CYBER SECURITY

Cisco webex

EC-Council Associate CompTIA P.E.K.I.T.

Un mondo senza gli hacker sarebbe un mondo senza curiosità e innovazione.
"Jon Erickson"

La Cyber Security, anche conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche, è la pratica che consiste nel difendere i computer e i server, i dispositivi mobili, i sistemi elettronici, network e dati da attacchi pericolosi. Il termine abbraccia un ampio raggio di settori e si applica a qualunque cosa: dalla sicurezza dei computer al ripristino di emergenza e all'istruzione degli utenti finali.

Grazie a questo percorso formativo e specializzante i partecipanti acquisiranno competenze tali da poter diventare degli esperti della sicurezza dei sistemi informativi e delle reti informatiche, principalmente dal punto di vista tecnico, ma anche da quello gestionale, organizzativo e normativo. Il corso, infatti, fornisce tutte le conoscenze pratiche e teoriche "anti" HACKER e contro la pirateria informatica, nonché tecniche di Indagini Digitali Forensi.



INTRODUZIONE

Gli Obiettivi

Gli obiettivi del percorso sono di formare il partecipante in modo che sarà in grado di identificare le minacce alla protezione, le vulnerabilità dei sistemi informativi e sarà capace di rispondere a qualsiasi incidente informatico secondo schemi prefissati, verrà fornito della preparazione sulle varie tematiche della cyber security, capaci quindi sia di capacità di sicurezza basilari, come il riconoscimento e il primo intervento alle minacce informatiche, ma anche di conoscenze avanzate di prevenzione, le normative, la sicurezza delle reti ecc.,. fino ad arrivare alla preparazione delle Tecniche di Indagini Forensi.

Inoltre, al termine del corso il partecipante acquisirà le competenze specifiche richieste per svolgere la funzione di Responsabile della Sicurezza così come previsto dal Nuovo Codice Privacy – GDPR.

All'ICT Security Manager spetta il compito di definire la politica di sicurezza del sistema informativo e valutare i rischi connessi all'uso di specifici strumenti informatici.

Come è facile pensare assume sempre più un valore di straordinaria importanza il ruolo dell'ICT Security Manager, come quello di altri professionisti della sicurezza informatica e cresce nelle aziende la necessità di figure di questo tipo.

Cosa Imparerai

- La gestione della sicurezza informatica in azienda
- Vulnerability assessment e mitigazione del rischio informatico
- Uso del sistema operativo LINUX in Command Line
- Uso dei principali tools per l'analisi di rete, protocolli e vulnerabilità
- Analizzare il funzionamento di una web application e identificare le sue vulnerabilità

PROGRAMMA DIDATTICO





CONCETTI GENERALI DI SICUREZZA

- Introduzione ai concetti di sicurezza
- Il paradigma CIA
- Concetto di rischio informatico
- La valutazione del rischio
- Cenni di Cyber Kill Chain Methodology
- Information Assurance (IA)
- La gestione delle policy
- Information Security Laws and Standard
- La sicurezza fisici
- I controlli ambientali (corretta illuminazione, barricate, allarmi, sistemi di rilevamento)
- I controlli HVAC
- Il Disaster Recovery Plan, il BIA
- Risk Assessment e Risk Calculation
- Risposta al rischio informatico

MONITORARE LE ATTIVITA' E RILEVARE LE INTRUSIONI

- Secure Network Architecture
- Studio del firewall e implementazione delle regole
- IDS Vs IPS
- Honeynet e Honeypot
- VPN
- SIEM – cenni

BUSINESS CONTINUITY

- Apprendere i fondamenti della ridondanza
- RAID
- Comprendere il significato di cloud computing
- Comprendere il funzionamento di un backup
- Developing backup plan
- Working with virtualization
- VDE vs VDI



GDPR: TRATTAMENTO DEI DATI PERSONALI

- Il regolamento europeo sulla protezione dati 679/2016
- Ambito di applicazione
- Dati personali
- Trattamenti e soggetti
- Diritti degli interessati
- Illeciti e sanzioni

IDENTITY AND ACCESS MANAGEMENT

- Comprendere il significato di Confidenzialità, Integrità e riservatezza
- Studio ed analisi dei processi di Identificazione, Autenticazione ed Autorizzazione
- Autenticazione - Single Factor VS Multi factor
- Sistema LDAP
- Protocolli di autenticazione di rete: Lo standard 802.1x e l'autenticazione RADIUS



NETWORKING FOUNDATION

- Analisi dell'infrastruttura di sicurezza
- Le periferiche di rete: firewall hub, router, switch, access point, modem, VPN
- I protocolli di rete e le dinamiche di interazione client/server
- Modello ISO/OSI
- I protocolli di applicazione, trasporto e rete
- Verifica e funzionamento dei protocolli in ambiente virtuale
- Analisi delle vulnerabilità dei principali protocolli di rete
- Sicurezza wireless

AMBIENTE OPERATIVO LINUX

- Cenni del sistema operativo Linux
- Studio della Command Line Interface
- I principali comandi per la gestione del S.O.
- Bash e bash scripting – Cenni



FOOTPRINTING E RICOGNIZIONE

- Cenni di OSINT
- Le Google dorks
- I principali tools per la raccolta delle informazioni (theHarvester, Maltego)
- Mirroring di un sito web
- Studio del dominio; analisi del DNS
- Cybersquatting vs Typosquatting
- Ricerca dei sottodomini
- Scansione di rete
- Uso del tool Nmap
- Studio del protocollo: Wireshark
- Studio di real case; lavoro in ambiente virtuale
- Il Framework Metasploit



MALWARE THREAT

- Virus vs malware
- Cybercrime
- Il ransomware CryptoLocker
- Rilevamento anti-virus di malware polimorfico e armored virus
- Strategie di attacco e analisi degli attacchi più comuni
- Software Exploitation
- Malicious code
- Social Engineering Concepts and its Phases
- Social Engineering Techniques
- Insider Threats and Identity Theft
- Social Engineering Countermeasures
- Cenni del funzionamento del Database e del DBMS
- Le vulnerabilità di una web application
- Attacchi agli account: il brouteforce
- Attacchi di tipo XSS
- SQL Injection
- Analisi e simulazione di attacchi alle Web Application
- Password Cracking Techniques
- Password Cracking Tools
- Password Cracking Countermeasures

NETWORK LEVEL ATTACKS AND COUNTERMEASURES

- Packet Sniffing Concepts
- Sniffing Techniques
- Sniffing Countermeasures
- DoS and DDoS Attacks
- DoS and DDoS Attack Countermeasures
- Session Hijacking Attacks
- Session Hijacking Attack Countermeasures

WEB APPLICATION ATTACKS AND COUNTERMEASURERS

- Web Server Attacks
- Web Server Attack Countermeasures
- Web Application Architecture and
- Vulnerability Stack
- Web Application Threats and Attacks
- Web Application Attack Countermeasures
- SQL Injection Attacks
- SQL Injection Attack Countermeasures

MOBILE SECURITY

- Periferiche mobili
- Sicurezza del dispositivo
- Sicurezza delle applicazioni
- Preoccupazioni BYOD
- Pulitura remota, blocco e screen serrature
- GPS controlle applicazioni
- Segmentazione, asset tracking e controllo del magazzino



LA CRITTOGRAFIA

- Storia della crittografia
- La crittografia simmetrica
- La crittografia asimmetrica
- La steganografia
- L'hash e la firma digitale
- I certificati e il non ripudio
- La Public Key Infrastructure
- Il certificato digitale: il ciclo di vita

INDAGINI DIGITALI FORENSI: COMPUTER FORENSICS

- Concetti generali della computer forensics
- Gestione delle comunicazioni: gli scenari di impatto
- La normativa GDPR come definisce la fase di gestione di un incidente informatico
- La fase di ripristino: Business Continuity e le misure organizzative
- Analisi post incident
- Analisi forense e la catena di custodia
- Aspetti legali
- La prova digitale e la sua conservazione
- Fasi dell'attività
- Linee guida per il trattamento dei dati da parte dei CTU e CTP
- Il file system



EXAM CERTIFICATION



Istituto Formativo Europeo Italia essendo un centro accreditato EC-Council, PEKIT e Certiport eroga direttamente gli esami previsti per questo percorso didattico.

EC-COUNCIL | ACADEMIA PARTNER

P.E.K.I.T. center

CERTIPORT A PEARSON VUE BUSINESS AUTHORIZED TESTING CENTER

E|HE Ethical Hacking Essentials

CompTIA Security+

P.E.K.I.T. Security

Questo percorso mira a fornire una figura completa e pratica immediatamente spendibile sul mercato del lavoro.

I cyber criminali infatti stanno diventando sempre più abili e i loro attacchi sempre più sofisticati. Allo stesso tempo aumentano i rischi per le imprese che, oltre ai loro perimetri fisici, devono proteggere anche i confini virtuali sempre più estesi, complici anche le tecnologie di tipo cloud, mobility e IoT.

La richiesta di una figura pluricertificata immediatamente spendibile nel mercato del lavoro cresce esponenzialmente e rappresenta un valore aggiunto rispetto agli altri candidati.

CERTIFICAZIONI INTERNAZIONALI







Certificazioni Erogate:
- EC-Council EHE
- CompTIA Security+
- P.E.K.I.T. Security

Enti Certificatori:
EC-Council ® / PEKIT ®
Certiport ® - Person Vue ®

Modalita' di Erogazione:
Online / Presso le Sedi Abilitate