Accademia Informatica s.r.l.
Viale Filippo Tommaso Marinetti 221 – 00143 Roma
Tel. 06 39746618 - Fax 06 97749271
www.accademiainformatica.com – info@accademiainformatica.com
PEC: amministrazione@pec.accademiainformatica.com
Iscrizione CCIAA di Roma n. 07153681007 - REA n. RM-1014676
Codice Fiscale e Partita IVA: 07153681007 - Cap. Soc. € 115.000,00 i.v.

CORSO DI FORMAZIONE
"Cybersecurity - Gestione della Sicurezza delle Informazioni e delle Reti"

DESCRIZIONE

Il **Corso "Cybersecurity - Gestione della Sicurezza delle Informazioni e delle Reti"** intende preparare professionisti in grado di gestire i sistemi informativi digitali con competenze pratiche e conoscenze per affrontare le minacce alla sicurezza informatica. L'esperto di **Cybesecurity** è una figura professionale ampiamente richiesta nell'ambito dei servizi digitali. L'esperto di **Cybesecurity** conosce i principali *framework* e le metodologie fondamentali nell'ambito della ***cybersecurity governance***. Collabora alle attività di identificazione delle fonti di rischio per la **sicurezza delle informazioni** e di applicazione di soluzioni idonee al ripristino del corretto funzionamento dei sistemi e delle reti. Conosce le **tecnologie "disruptive" abilitanti** e ne riconoscere le opportunità e i rischi ad esse correlati.

STRUTTURA DEL CORSO

Durata ore:

- 20 ore

MODALITÀ DIDATTICHE

Lezioni frontali, esercitazioni guidate individuali e di gruppo, simulazioni, analisi di casi e problem solving.

Modalità di valutazione degli apprendimenti

Discussione in aula al termine di ogni unità didattica, Laboratori e simulazione di casi.

Aule Didattiche

Il corso richiede l'uso di aule didattiche allestite con PC e software dedicati, il software utilizzato nel corso delle lezioni è open source.

Attestato di Frequenza

Al termine del corso Accademia Informatica rilascerà un Attestato di Frequenza.

PER INFORMAZIONI

ACCADEMIA INFORMATICA Srl
Viale Filippo Tommaso Marinetti, 221 - 00143 Roma
Tel: 06 39746618 | Fax: 06 97749271 - www.accademiainformatica.com/corsi/
E-mail: info@accademiainformatica.com

MODULO	CONTENUTI
MODULO 1. INTRODUTTIVO Elementi di base di cyber security, IT e sicurezza informatica	**Elementi di base di cybersecurity, IT e sicurezza informatica** ▪ Elementi di base di sicurezza informatica, ICT, cybersecurity ed Operational Technology ▪ Fondamenti di processi ed organizzazione aziendale (produzione, monitoraggio, controllo, rendicontazione) ▪ Elementi di infrastruttura IT (informatica, cloud, networking) ▪ Principali ambienti cloud (MS Azure, AWS, Google Cloud)
MODULO 2. Analisi delle vulnerabilità delle reti e dei rischi per la sicurezza delle informazioni	**Supporto all'analisi delle vulnerabilità e dei rischi per la sicurezza delle informazioni** ▪ Requisiti di sicurezza di un sistema informatico: autenticazione delle parti, riservatezza, integrità dei dati e dei flussi, disponibilità del servizio, robustezza e velocità dei sistemi crittografici ▪ Principali standard di riferimento per lo svolgimento di attività di auditing, assessment, risk assessment e risk management ▪ Metodologie di analisi delle vulnerabilità delle reti e dei dati o Studio delle configurazioni dei sistemi sia client che server rispetto ai parametri di funzionamento e di sicurezza ▪ Strumenti per la verifica tecnica delle vulnerabilità e degli attacchi di rete
MODULO 3. Soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti	**Supporto all'implementazione di soluzioni per la gestione dei fattori di rischio all'interno dei sistemi e delle reti** ▪ Le fasi di un Penetration test e la loro applicazione nei diversi contesti precedentemente definiti (reti, sistemi, architetture IT e OT). ▪ La Kill Chain, le fasi di un attacco informatico e la sua applicazione nei contesti precedentemente definiti: reconnaissance, weaponization, Delivery, Exploitation, Installation, Command and control, Action on objectives/Exfiltration ▪ La "Cyber Kill Chain Control Matrix" sua costruzione nella realizzazione degli attacchi: attacchi man in the middle, arp spoofing, session hyjacking, sql injection, attacchi al TLS e all'https, attacchi basati su tecniche di social engeenering, DOS e DDOS, buffer overflow attacks, attacchi alle reti wifi
MODULO 4. Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie	**Identificazione e segnalazione dei rischi connessi all'utilizzo delle nuove tecnologie** ▪ Principali applicazioni dell'intelligenza artificiale o Anomaly detection systems e intrusion detection system costruiti usando tecniche di machine learning e intelligenza artificiale. ▪ Principali rischi dell'intelligenza artificiale in ambito cyber ▪ Principali applicazioni dell'IoT e rischi correlati
Totale ore Aula	20

CALENDARIO DIDATTICO

DATA	ORARIO	DURATA	DOCENTE
Lezione 1 - giovedì 20 febbraio 2025	14:45 - 17:45	3 ore	Prof. Franco Arcieri
Lezione 2 - giovedì 27 febbraio 2025	14:45 - 17:45	3 ore	Prof. Franco Arcieri
Lezione 3 - giovedì 6 marzo 2025	14:45 - 17:45	3 ore	Prof. Franco Arcieri
Lezione 4 - giovedì 13 marzo 2025	14:45 - 17:45	3 ore	Prof. Franco Arcieri
Lezione 5 - venerdì 14 marzo 2025	14:00 - 16:00	2 ore	Prof. Andrea Dimitri
Lezione 6 - giovedì 8 maggio 2025	14:45 - 17:45	3 ore	Prof. Andrea Dimitri
Lezione 7 - giovedì 15 maggio 2025	14:45 - 17:45	3 ore	Prof. Andrea Dimitri