INTENSIVE MASTER CYBER SECURITY

PROSSIMA EDIZIONE
Novembre 2022

SEDE
Lezioni sincrone in virtual room

DURATA
92 ore da Novembre a Febbraio

FREQUENZA
Formula weekend

Experis™ Academy
ManpowerGroup

OVERVIEW MASTER CYBER SECURITY

L'Intensive Master Cyber Security si pone l'obiettivo di fornire una preparazione tecnica significativa sulle principali tematiche legate alla sicurezza informatica, al fine di consentire alle aziende di dotarsi delle competenze e degli strumenti utili per prevenire un attacco cyber. Un focus specifico sarà fatto sui diversi aspetti che costituiscono una corretta gestione della sicurezza informatica: comprensione dei sistemi, delle reti, dei sistemi perimetrali e del cloud.

QUALI PERCORSI DI CARRIERA POTRAI INTRAPRENDERE

Al termine del percorso formativo, sarai un professionista esperto sulle tematiche legate alla sicurezza informatica e in grado di gestire correttamente la sicurezza dei sistemi e del cloud, dalla prevenzione alle verifiche tecniche.

- Cyber Security Analyst
- Information Security Analyst
- Cyber Security Engineer
- Information Security Consultant

A CHI SI RIVOLGE

Il Master si rivolge a laureati STEM, o professionisti con esperienza nel mondo informatico, che desiderano specializzarsi e acquisire nuove competenze.

PUNTI DI FORZA

- Experis Academy **porta in aula esperti del settore**: i contenuti formativi sono erogati dai migliori professionisti in grado di condividere e trasmettere ai partecipanti le proprie competenze, expertise ed esperienze. Questo assicura un approccio fortemente pratico e applicativo, capace di abbinare approfondimenti teorici, esercitazioni ed use cases
- **Networking**: contatti con professionisti e aziende facenti parte del circuito partner Experis Academy
- **Consulenza** da parte dei professionisti Experis

PROGRAMMA INTENSIVE MASTER CYBER SECURITY

MODULO 1

GESTIONE DELLA SICUREZZA E DELLA COMPLIANCE

La Sicurezza Informatica e la CyberSecurity - La gestione della sicurezza informatica

- Introduzione generale sul tema cybersecurity
- Principali minacce e tecniche di attacco
- Modelli organizzativi
- La sicurezza integrata nell'ambito dei processi IT
- La gestione degli incidenti informatici
- Monitoraggio e gestione degli eventi di sicurezza: dal SOC al CSIRT
- Principali standard per la sicurezza di soluzioni, processi, tecnologie e competenze

Threat Intelligence

- Perché e cosa è esattamente la threat intelligence?
- Che cosa fa la Threat Intelligence: Situational Awareness
- Threat Intelligence Capability
- OSINT & Altre fonti
- Proliferazione di cyber-weapons

MODULO 2

SICUREZZA DEI SISTEMI

La sicurezza dei sistemi

- Security Architecture & Engineering. Principi e normative di riferimento. Security By Design e By Default: integrazione della sicurezza nel ciclo di vita
- Integrazione della sicurezza nei processi
- Assurance, Trust & Defense in Depth; Modelli di sicurezza
- Componenti dei sistemi e loro vulnerabilità
- Sicurezza dei sistemi esposti su internet
- Richiami alle tecniche crittografiche e al loro utilizzo
- Firma digitale e PKI
- Sicurezza dei database e dei middleware. Valutazione della sicurezza
- Certificazione e accreditamento
- Sicurezza dei protocolli applicativi
- Sicurezza delle infrastrutture virtualizzate
- IoT & Embedded devices Security
- Protezione delle postazioni di lavoro
- Progettazione di siti sicuri
- Sicurezza dei dispositivi mobili (focus su IOS e Android)

Laboratorio sicurezza delle reti

- Classificare gli eventi di compromissione usando i modelli Cyber Kill Chain ed il MITRE ATT&CK framework
- Il database Mitre CVE
- Massimizzare il rilevamento e la risposta ad attacchi avanzati durante un tipica kill chain
- Il ruolo della Threat Intelligence
- Microsoft CyberSecurity reference model. Esempi pratici di attacchi

PROGRAMMA INTENSIVE MASTER CYBER SECURITY

MODULO 3

SICUREZZA DEI SISTEMI CLOUD

Sicurezza del Cloud

- Private cloud, Public cloud, Cloud ibrido, Virtual private cloud, Auto scaling, elastic load balancing e containers.
- I rischi e le opportunità dell'utilizzo del Cloud. Come gestire in modo sicuro i diversi tipi di cloud, ovvero quali sono le responsabilità in carico al cloud customer in relazione alle garanzie offerte contrattualmente dal cloud provider. Come il cloud aiuta la sicurezza mediante servizi di sicurezza gestita (es: CASB), la c.d. "Cloud Intelligence", il machine learning.

Laboratorio sicurezza cloud

- Obiettivi: consentire di svolgere e verificare gli effetti della configurazione sicura di utenze, sistemi e infrastrutture cloud, se possibile mostrando configurazioni di servizi CASB.
- Illustrare e far utilizzare soluzioni e configurazioni avanzate di sicurezza dei servizi di almeno un grande cloud provider.

MODULO 4

VERIFICHE TECNICHE DI SICUREZZA

Tecniche di verirfica della sicurezza dei sistemi e delle reti - Teoria e pratica

- Enumerazione di porte e servizi di un sistema (port-scanning con nmap, masscan, ecc.)
- Identificazione di potenziali vulnerabilità (check risultati e ricerche online)
- Verifica e exploitation di potenziali vulnerabilità (valutazione di possibili exploit e utilizzo degli stessi)
- Enumerazione di un'applicazione web (directory e file enumeration con tool come gobuster, ffuf, ecc.)
- Analisi e verifica di un'applicazione web (utilizzo di proxy web come Burpsuite)

CALENDARIO

NOVEMBRE
Ven. 11 | 9.00 -18.00
Sab. 12 | 9.00 -18.00
Dom. 13 | 9.00 - 13.00

Sab. 19 | 9.00 - 18.00

Sab. 26 | 9.00 - 18.00

DICEMBRE
Ven. 16 | 9.00 - 18.00
Sab. 17 | 9.00 - 18.00
Dom. 18 | 9.00 - 13.00

GENNAIO
Sab. 14 | 9.00 - 18.00

Ven. 20 | 9.00 - 18.00
Sab. 21 | 9.00 -13.00

FEBBARIO
Ven. 3 | 9.00 - 18.00
Sab. 4 | 9.00 -18.00

AZIENDE E RELATORI IN AULA

CLAUDIO CILLI

WORLD LEADING AUTHORITY IN NATIONAL SECURITY AND INTELLIGENCE, COMPANY PROTECTION, CYBER-SECURITY AND CRITICAL INFRASTRUCTURES

Laureato con lode in Ingegneria Elettronica, autorità riconosciuta a livello mondiale nelle aree della Sicurezza Nazionale e dell'Intelligence, sicurezza dei sistemi informativi e compliance normativa con oltre 25 anni di esperienza, è attualmente advisor di Governi e grandi aziende per la Cyber Security e protezione delle infrastrutture critiche. Ha progettato sistemi di elaborazione "sicuri" per le Forze Armate. È autore di libri tecnici e articoli pubblicati su riviste del settore in Italia e all'estero, ed è relatore in conferenze internazionali.

LUCA BECHELLI

@P41
PARTNER - INFORMATION & CYBER SECURITY

FABIO CARRETTO

@SOTER IT SECURITY
CEO E PENETRATION TESTER

DANIELE SCANU

@SOTER IT SECURITY
CEO E PENETRATION TESTER

OPEN BADGE DI CERTIFICAZIONE

Al termine del percorso, e al raggiungimento del 70% di frequenza, ogni partecipante al Master riceverà un Open Badge nominale. L'Open Badge è una certificazione internazionale, fruibile in formato digitale, che certifica le competenze raggiunte nei percorsi di Alta Formazione Experis Academy.
I Badge digitali permettono di tracciare in modo efficace i risultati conseguiti nel percorso formativo e di condividere tali risultati in modo semplice, sicuro e verificabile.

EXPERIS ACADEMY

Experis Academy nasce, nel 2014, con l'obiettivo di rispondere allo skills shortage delle aziende grazie alla possibilità di formare ed inserire le migliori figure professionali sul mercato del lavoro IT & Technology in rapida crescita.
Grazie alla profonda conoscenza dei mercati di riferimento e delle specificità delle realtà aziendali, uniti a expertise tecnica interna e a una rete capillare di professionisti qualificati, Experis Academy offre soluzioni uniche e innovative nell'ambito del Talento e della Tecnologia, accompagnando i clienti in un processo di trasformazione tecnologica e digitale che nasce dalla perfetta simbiosi tra persone e innovazione.

MODALITA' DI PAGAMENTO

Il Master è a numero chiuso ed è richiesta una valutazione dei requisiti di ingresso che verrà effettuata da un nostro referente Academy attraverso un incontro conoscitivo.

Pagamento in un'unica soluzione **€2.500 + IVA**

Pagamento dilazionato in 2 tranche da **€1.375+ IVA**

- 1° tranche al momento dell'iscrizione
- 2° tranche entro il 30 Novembre 2022

Al fine di perfezionare l'iscrizione sarà necessario compilare, sottoscrivere ed inviare l'apposito modulo di registrazione al percorso di formazione.

Per maggiori informazioni
contattaci compilando l'apposito form, **CLICCA QUI**.