short master in

CYBER SECURITY

COORDINATORI DEL CORSO: Prof. Danilo Caivano - Dip. di Informatica - Università degli Studi di Bari
Dott.ssa Anna Conte - OMNITECH s.r.l.

SCADENZA BANDO: 30 APRILE 2017
SELEZIONI: MAGGIO 2017
AVVIO ATTIVITÀ DIDATTICHE: MAGGIO 2017

FORMULA FULL-TIME: 6 ore di lezione al giorno per 5 giorni alla settimana
SEDE DI SVOLGIMENTO: ITT G.Giorgi, Via Amalfi n.6, Brindisi (BR)
COSTO: €800 iscrizione + €74,13 per contributi e imposta di bollo

INFORMAZIONI, MODALITÀ DI PARTECIPAZIONE E CONTATTI:
www.uniba.it/didattica/master-universitari/short-master/short-master-a.a.-2016-2017/cyber-security

IL CONTESTO

Iniziativa nata dalla collaborazione tra il Dipartimento di Informatica dell'Università di Bari (www.di.uniba.it), l'I.T.T. G. Giorgi di Brindisi (www.ittgiorgi.gov.it) e il gruppo industriale OmnitechIT (http://omnitechit.eu), leader italiano nell'ambito della Cyber Security. L'economia e i servizi di welfare di un paese avanzato, ormai si poggiano su infrastrutture e servizi erogati tramite il cyberspace, quell'insieme di reti, protocolli e applicazioni informatiche eterogenee e interconnesse che ci circonda. Incidenti informatici che impattino tali infrastrutture e servizi possono avere conseguenze economiche molto rilevanti, a livello di nazione, di imprese e di singoli cittadini. Tali incidenti non investono solo il piano cibernetico, possono infatti partire da questo per poi arrivare ad avere impatti sulle infrastrutture fisiche, provocando indisponibilità di servizi anche essenziali e quindi perdite economiche, fino a possibili perdite umane. Gli incidenti possono essere naturali o provocati da terroristi, cyber criminali, attivisti o da nazioni straniere. Negli ultimi tempi l'opinione pubblica è stata esposta a numerosi casi eclatanti di attacchi cyber, alcuni anche con effetti importanti (terrorismo, operazioni di spionaggio, operazioni militari). Anche le piccole e medie imprese cominciano a comprendere che esiste un problema che potrebbe coinvolgerle, non sempre però capendo che le conseguenze potrebbero essere disastrose. Il livello di consapevolezza è aumentato di conseguenza e ci si inizia a domandare quale sia il proprio livello di preparazione sul tema e, soprattutto, è iniziata oramai da tempo la ricerca di figure professionali capaci di affrontare tali problemi con competenza.

OBIETTIVI

L'obiettivo di questo short master è formare professionisti in Cyber Security, quell'insieme di pratiche che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyberspace. L'intervento formativo punta a dare ai corsisti una panoramica a tutto tondo sulla sicurezza spaziando dalla sicurezza di rete a quella applicativa sino a toccare temi come le vulnerabilità, i meccanismi di accesso ed autenticazione e la crittografia.

REQUISITI DI AMMISSIONE

Possesso titolo di Laurea Triennale in una delle seguenti classi:

- L-07 LAUREE IN INGEGNERIA CIVILE E AMBIENTALE
- L-08 INGEGNERIA DELL'INFORMAZIONE
- L-09 INGEGNERIA INDUSTRIALE
- L-14 LAUREE IN SCIENZE DEI SERVIZI GIURIDICI
- L-18 LAUREE IN SCIENZE DELL'ECONOMIA E DELLA GESTIONE AZIENDALE
- L-20 LAUREE IN SCIENZE DELLA COMUNICAZIONE
- L-30 LAUREE IN SCIENZE E TECNOLOGIE FISICHE
- L-31 SCIENZE E TECNOLOGIE INFORMATICHE
- L-33 LAUREE IN SCIENZE ECONOMICHE
- L-35 SCIENZE MATEMATICHE
- L-36 LAUREE IN SCIENZE POLITICHE E DELLE RELAZIONI INTERNAZIONALI
- L/DC LAUREE IN SCIENZE DELLA DIFESA E DELLA SICUREZZA
- L/SC LAUREE IN SCIENZE CRIMINOLOGICHE E DELLA SICUREZZA
- LMG/01 LAUREE MAGISTRALI IN GIURISPRUDENZA

PIANO DIDATTICO

Più in dettaglio il corso è organizzato in sette moduli formativi, di seguito elencati, ognuno dei quali prevede sia lezioni frontali che attività di esercitazione e laboratorio supervisionate:

Modulo 1 - Sicurezza di Rete - Tecniche Offensive
Modulo 2 - Sicurezza di Rete - Tecniche Difensive
Modulo 3 - Sicurezza di Rete - SIEM (Security Information and Event management)
Modulo 4 - Sicurezza Applicativa in ambiente Web
Modulo 5 - Sicurezza Applicativa in ambiente Desktop
Modulo 6 - Sicurezza Applicativa in ambiente Mobile (Android)
Modulo 7 – Vulnerability, Mitigation and Access Control Management

OPPORTUNITA' IN USCITA

Lo Short Master in Cyber Security è solo una parte di un percorso ben più ampio che prevede:

1) short master 100 ore
2) stage aziendale di massimo 300 ore presso il gruppo Omnitech
3) **assunzione all'interno del gruppo Omnitech.**

Resta inteso che:

- allo stage accederanno coloro che durante il master si saranno distinti per capacità e risultati. A tal proposito farà fede la votazione conseguita nella prova di fine master a cui saranno sottoposti i frequentanti;
- saranno assunti coloro che a fine stage avranno ottenuto una valutazione positiva. Si auspica a tal fine di poter assumere almeno la metà dei corsisti.

Alo scopo di iniziare a dare a questo short master una proiezione internazionale, sono stati riservati 3 posti per candidature provenienti dall'Albania, dando seguito alla collaborazione con l'altra sponda del mediterraneo e rinsaldando così i rapporti italo-albanesi già avviati dall'Università di Bari.

OmnitechIT (omnitechit.eu) è un System Integrator di sicurezza informatica leader a livello europeo, alla continua ricerca dell'eccellenza nei servizi professionali e nelle soluzioni integrate di Information Security. OmnitechIT adotta un approccio olistico alla IT Security, che coniuga una profonda specializzazione nei singoli domìni, con la visione trasversale che abbraccia tutte le tematiche, dai Vulnerability Assessment e Penetration Testing alla sicurezza infrastrutturale, dall'Identity ed Access Management al SIEM, dalla protezione dei dati alla GRC, alla sicurezza dell'Enterprise Mobility, ed è quindi in grado di coglierne in maniera sinergica le dipendenze, e di metterne a valore il potenziale di integrazione.
Da oltre 10 anni, OmnitechIT supporta i clienti nella protezione degli asset e delle informazioni attraverso l'intero stack IT, affiancandoli ed aiutandoli nell'assumere una postura di sicurezza adattiva, sensibile al contesto e consapevole dei rischi, per far fronte alle continue e mutanti minacce del cybercrime, utilizzando la sicurezza come fattore abilitante delle nuove opportunità del business digitale, attraverso il cloud, il mobile, il social ed i big data.

Il **Dipartimento di Informatica** dell'Università di Bari (www.di.uniba.it) nasce nel 1992 in continuità con l'Istituto di Scienze dell'Informazione, quest'ultimo attivo dal 1974. L'offerta formativa è articolata in tre corsi di laurea triennale, Informatica, Tecnologie per la Produzione del Software e Comunicazione Digitale, ed una Laurea Specialistica in Informatica.
A completare l'offerta formativa il corso di Dottorato di Ricerca in Informatica e vari corsi di formazione post laurea e master universitari. Al suo interno sono attivi 10 laboratori di ricerca avanzata in cui operano circa 80 ricercatori. Il Dipartimento vanta numerose collaborazioni con enti ed imprese sia a livello regionale che nazionale ed ha nel tempo promosso molteplici iniziative di ricerca e aziende spin off universitarie.

L'**ITT "Giorgi"** di Brindisi (www.ittgiorgi.gov.it) è il punto di riferimento per la formazione tecnica sul territorio sin dai primi anni del 1960. Si propone di formare dei giovani maturi ed equilibrati, competenti e consapevoli, capaci di trovare un proprio ruolo nella società, consapevoli e autonomi, in grado di prendere decisioni, preparati professionalmente e culturalmente. L'obiettivo è continuare ad essere il punto di riferimento per la formazione tecnica per il territorio, mantenendosi sempre a livelli di eccellenza per qualità, completezza e innovazione dell'offerta formativa e far così crescere, nel suo essere comunità educante, passione, responsabilità, etica, ricerca ed innovazione. L'offerta formativa dell' istituto prevede le seguenti ARTICOLAZIONI: INFORMATICA e TELECOMUNICAZIONI; ELETTRONICA e ELETTROTECNICA; MECCANICA, MECCATRONICA e ENERGIA.