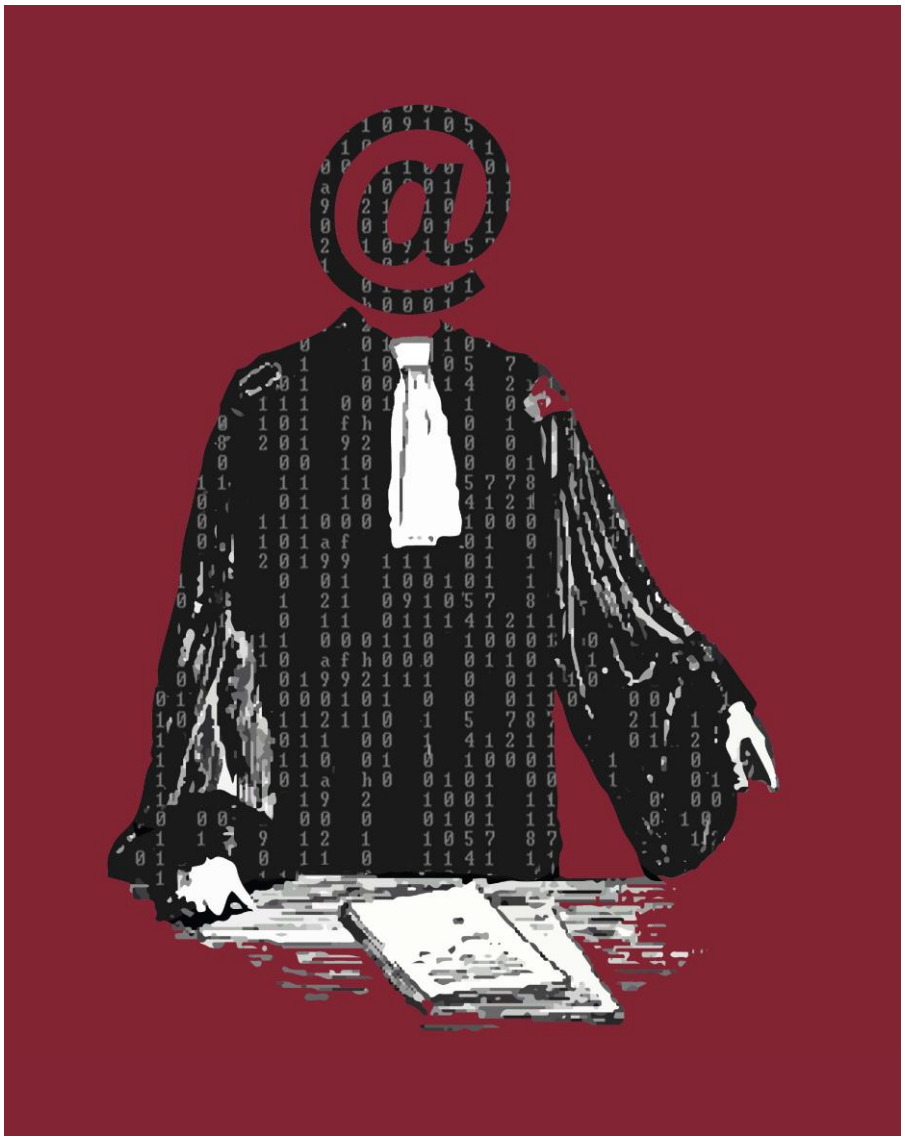
Master Executive in Cyber Security, Digital Forensics and Computer Crimes



#IOHOSCELTO

Contatti

SEDE LEGALE E OPERATIVA **ROMA**

Corso d'Italia 19- 00198 Roma

TEL: 06 90212620

info@masterandskills.com

www.masterandskills.com

CONTESTO ATTUALE

CYBER SECURITY, UN INVESTIMENTO PER IL FUTURO

In un tempo di minacce crescenti, la sicurezza cibernetica rappresenta, per coloro a cui è affidata la tutela degli interessi nazionali, il maggior rischio da gestire per tutti i Paesi del mondo. A livello globale, nel 2015 l'industria della cyber security ha sfiorato un giro di affari di oltre 75 miliardi di dollari e per il 2020 se ne prevede il raddoppio. Una delle più note compagnie di assicurazioni, la londinese Lloyds, ha stimato i danni causati da attacchi informatici in circa 450 miliardi di dollari all'anno, somma che include sia i 'crash di sistema' che i costi di ripristino. La Juniper Networks, azienda leader nel settore dell'internet working, valuta che entro il 2019 il costo mondiale per la perdita di dati sensibili di aziende e cittadini si attesterà su una cifra pari a 1,2 trilioni di dollari. Gli investimenti nella cyber security sono inevitabilmente destinati a crescere, pena il blocco delle attività delle aziende, la sicurezza.

Dietro i crimini informatici si celano frodi e terrorismi globali, la tutela della sicurezza informatica non può essere più in mano soltanto delle autorità o ai servizi di intelligence.

È chiaro che, per conseguire un più elevato livello di sicurezza dei sistemi informatici in una qualsivoglia organizzazione, risulta essenziale la predisposizione di mirate attività di intelligence digitale, ma non bisogna ignorare che le multinazionali della consulenza economica finanziaria stanno ricercando oltre 1000 esperti in digital forencics e computer crimes perchè le grandi frodi sul nuovo petrolio del millennio ovvero i big data preoccupano non solo il mondo delicurezza ma anche il mondo della finanza.

Accanto a questo aspetto c'è tutto l'aspetto legato al Cyber bullismo a reati informatici sui minori, sulle donne e sulle categorie più deboli.

Insomma la rete è diventata croce e delizia del nostro universo

Occorre formare nuovi professionisti giuristi, criminologi, psicologi che abbiano competenze trasversali e multidisciplinari dalla fase normativa e sanzionatoria civile e penale, alla scena del crimine, al reperimento prove, all'investigazione e all'utilizzo delle tecnologie per proteggere o per sanzionare.

Questa risulta quindi essere una professione che è diventata un'opportunità di lavoro crescente per giovani avvocati, psicologi, informatici.

OBIETTIVI

Il Master in Cyber Security, digital Forensics and Computer Crimes risponde al fabbisogno crescente di professionalità tecnologiche nelle scienze forensi in ambiti di diritto penale e diritto processuale penale, per prevenire tutti i rischi da reati informatici, acquisire, gestire, conservare e proteggere dati digitali di utenti pubblici e privati da attacchi informatici, fornendo conoscenze e competenze tecniche per la ricerca della fonte di prova digitale, partendo dal traffico in rete internet, mobile, video e foto, passando per la scena del crimine informatico, fino al criminal data management. L'estremo bisogno dell'esperto in cyber security e digital forensics si evidenzia dalla crescita elevata della domanda di lavoro di specialisti giuridici, informatici, criminologi in tutti i campi pubblici e privati in cui navigano dati sensibili.

Ultimi dati statistici sulle nuove professioni più richieste e ben remunerate sono quelle che lavorano con il petrolio del nostro secolo: i dati e tutto ciò che ruota loro attorno. L'obiettivo ambizioso del corso è quello di fornire strumenti tecnologici, ma anche psicologi per la profilazione del reato.

FUTURO PROFESSIONALE

Il Master executive mira a formare professionisti in grado di fornire il proprio contributo alle investigazioni digitali o consulenza agli organi investigativi o giurisdizionali in materia di Digital Forensics. Inoltre saranno in grado di fornire a singoli utenti, aziende, Enti Pubblici e privati servizi di acquisizione, duplicazione, gestione, conservazione e protezione dei dati, valutare i rischi dei reati informatici, nel rispetto degli standard internazionali ISO.

Figure Professionali in uscita:

- Criminologo Informatico
- Data Security Manager e IT Risk Manager
- Consulente reati informatici in ambito Pubblico e Privato
- Consulente giudiziale e stragiudiziale

Destinatari:

La partecipazione al Master è aperta a laureandi e laureati in:

- Giurisprudenza
- Psicologia clinica
- Criminologia
- Informatica

Durata (TBD)

300 ore di aula

+ 25 ore di laboratori
+ 25 ore di assessment
+16 ore di Testimonianze

Frequenza

Obbligatoria per l'80% delle lezioni

PERCORSO FORMATIVO

Il Master ha tre anime: una giuridica civile e penale, una di natura tecnologica, una terza di natura psicologica-criminologica, al fine di formare il professionista a 360°

INQUADRAMENTO DEL PERCORSO:

L'infrastruttura di rete: la struttura informatica e le infrastrutture critiche
L'infrastruttura di servizi: i social network
L'indicizzazione dei siti
Deep Web e Dark web
Security e nozioni di base di information technology e delle reti
Normativa internazionale e nazionale di riferimento
Gli attori della rete

Area normativa

Recepimento della direttiva NIS
Il nuovo regolamento europeo sulla privacy GDPR 2018
Il nuovo codice sul trattamento dei dati in ambito penale
La riforma della intercettazioni
I crimini di natura informatica
La security in azienda e nella PA
La security e gli attacchi in ambito finanziario
Casistica Civile
La censura su internet
La prova informatica nel processo penale
La digital forensics e la perizia informatica
Osint e Social Media Intelligence

Area tecnologica

Anonimato sulla Rete
Fenomeni di cyber terrorismo in rete e tecniche di contrasto
Il security assessment in azienda e nella Pubblica Amministrazione
La gestione del rischio e la classificazione degli asset e delle informazioni
Esempi pratici di crimini di natura informatica
Strumenti per prevenire i crimini di natura informatica in azienda e nella PA
Aspetti pratici della digital forensics: computer forensics e cellular forensics
Le intercettazioni telefoniche, telematiche ed ambientali
Outsourcing dei servizi di security e strumenti di controllo del servizio Cyber Intelligence
Protezione delle infrastrutture critiche

Area psicologica forense

Criminal profiling in ambito ICT
Nuove tecniche investigative
Nuove tecniche di redazione della consulenza tecnica
Tecniche e strategie di comunicazione in ambito forense

Area operativa

Il Ruolo della Polizia Postale nella lotta al cyber crime e alla pedopornografia online e nella produzione di infrastrutture critiche: le frodi online, hacking, attività forense, collaborazione con forze di polizia internazionale, collaborazione pubblico-privato
Il Ruolo della Guardia di Finanza nel monitoraggio di fonti di finanziamento al terrorismo in rete
La Cyberwar
Il ruolo del CERT Nazionale
Il ruolo dell'Arma dei Carabinieri, nel dettaglio del RACIS, Raggruppamento Carabinieri Investigazioni Scientifiche

Testimonianze di Eccelenza nell'ambito della Cyber Security

Facebook
Ferrovie dello Stato
Vodafone

Laboratori

Ciascun modulo sarà accompagnato da laboratori pratici e casistiche reali

FACULTY

Direttore Tecnico-Scientifico Prefetto Dott. Domenico Vulpiani

Nunzia Ciardi
Dirigente Superiore della Polizia di Stato, Direttore del Servizio Polizia Postale e delle Comunicazioni.
Simone Tacconi
Direttore della Sez. “Informatica Forense” del Servizio Polizia Postale e delle Comunicazioni, presso Dipartimento della Pubblica Sicurezza del Ministero dell’Interno,
Ivano Gabrielli
Dal luglio 2017 è il responsabile della III Divisione del Servizio Polizia Postale e delle Comunicazioni – CNAIPIC, Cyber Terrorismo, Financial Cyber Crime
Elvira D'Amato
Vice Questore Aggiunto responsabile del Centro Nazionale per il contrasto alla pedopornografia on-line presso il Servizio di Polizia postale e delle comunicazioni.
Corrado Giustozzi
Esperto in sicurezza informatica presso Agenzia per l'Italia Digitale per lo sviluppo del CERT governativo per la Pubblica Amministrazione
Giovanni Nazzaro
Ingegnere delle telecomunicazioni, Security Manager & Lawful Interception Advisor, professionista che opera nell’information technology e nelle reti di telecomunicazioni
Stefano Mele
Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza ed Intelligence.
Raoul Chiesa
Founder, President Security Brokers - Global Cyber Defense & Security Services
Isabella Corradini
Psicologa sociale e criminologa, esperta di tematiche di sicurezza, safety e security, con focalizzazione sul fattore umano e metodologie di awareness.
Ernesto Caffo
Professore Ordinario di Psichiatria Infantile e adolescenziale all’Università di Modena e Reggio Emilia (Italia). Presidente e fondatore di S.O.S Il Telefono Azzurro Onlus
Pier Luigi Dal Pino
Direttore Centrale per le Relazioni Istituzionali e Industriali di Microsoft Italia WE
Michele Colajanni
Professore di sicurezza informatica, ha fondato e dirige molteplici attività di ricerca e di formazione, tra cui il Centro di Ricerca Interdipartimentale sulla Sicurezza, il CyberLab con la Tel Aviv University, la prima Cyber Academy nazionale, e master universitari per lo Stato Maggiore Difesa
Stefano Aterno
Avvocato specializzato in: privacy, informatica forense, acquisizione e intercettazione di dati digitali. Docente di Diritto penale dell’informatica e delle nuove tecnologie.
Fulvio Berghella
Consulente di direzione e antiriciclaggio di OASI – Outsourcing Applicativo e Servizi Innovativi SpA (Gruppo ICBPI) di cui è stato Vice Direttore Generale Vicario, responsabile dei Servizi Antiriciclaggio e Formazione, Compliance, Supporto Societario e Sicurezza informatica.
Luisa Franchina
Dirigente Generale, Capo della Segreteria Tecnica del “Tavolo Pic” per il coordinamento interministeriale delle attività riguardanti le infrastrutture critiche alle dipendenze funzionali del Consigliere Militare del Nucleo Politico Militare della Presidenza del Consiglio.
Selene Giupponi
Vice Presidente Security Brokers ScpA
Rita Forsi
Direttore dell’Istituto Superiore delle Comunicazioni e delle Tecnologie dell’Informazione (ISCOM) del Ministero dello Sviluppo Economico. È anche direttore della Scuola Superiore di Specializzazione in Telecomunicazioni e direttore dell’Organismo di Certificazione per la Sicurezza Informatica (OCSI)
Franco Fiumara
Direttore centrale della protezione aziendale delle Ferrovie dello Stato
Riccardo Barrile
Responsabile Sicurezza Informazioni e Sistemi Informativi Ferrovie dello Stato
Stefano Bargellini
Direttore Safety, Security & Facilities, Vodafone Omnitel
Giulio Confortini
General Counsel dell'Ospedale Israelitico
Corradino Corradi
Head of ICT Security, Privacy&Fraud Management, Vodafone
Serena Gullotti
Responsabile Sicurezza di Security Broker
General Directorate for Political Affairs and Security. OSCE Office.
Alessandro Lega
Senior Security Consultant, come libero professionista, con attività di sviluppo di soluzioni e di opportunità di business nell'ambito della Sicurezza Industriale.
Emanuele Gentili
Cyber Threat Intelligence advisor per realtà pubbliche e private.
Cristian Perrella
Responsabile Sicurezza Facebook per le relazioni Law Enforcement per l'area Europa, Africa e Medio Oriente (EMEA)