KEN TERRANOVA

FORMATORE PRESSO
"IANUA - ISTITUTO DI CONOSCENZE SOCIOLOGICHE E CRIMINOLOGICHE"

Dott. in Scienze Criminologiche per l'Investigazione e la Sicurezza
Security Analyst & Cybersecurity Specialist

PRESENTAZIONE

La forza di una catena si misura dalla resistenza dell'anello più debole. Tramite servizio, ricerca e formazione in ambito Sicurezza, dedico la mia vita a fortificare gli anelli deboli, siano essi anelli interiori e personali o esterni della società. In quest'ottica, credo nell'unione delle persone, dei saperi e delle scienze per lo sviluppo di una società più sicura.

ISTRUZIONE E FORMAZIONE UNIVERSITARIA

LAUREA MAGISTRALE IN SCIENZE CRIMINOLOGICHE PER L'INVESTIGAZIONE E LA SICUREZZA

Alma Mater Studiorum - Università di Bologna | 2021
Tesi e specializzazione: Infiltrazione Mafiosa nelle Emergenze
Votazione: 106/110

LAUREA TRIENNALE IN SCIENZE SOCIALI PER LA COOPERAZIONE, LO SVILUPPO E LA PACE

Università di Pisa | 2017
Tesi e specializzazione: Logistica Umanitaria e Medio Oriente (con permanenza di 3 mesi in Giordania)
Votazione: 105/110

DIPLOMA DI DIRIGENTE DI COMUNITA'

Istituto Tecnico Economico e tecnologico "I.T.E.T. - F.lli Fontana" di Rovereto | 2011

MASTER E CORSI DI FORMAZIONE

MASTER IN CYBERSECURITY, DIGITAL FORENSIC E DATA PROTECTION

Università degli Studi "Niccolò Cusano", Roma | 2022

Master di II livello (1500 ore)
Modulo 1 (300 ore) - Cyber crimes: quadro normativo internazionale, europeo ed italiano: i cyber crimes: la digitalizzazione della criminalità, anche organizzativa; la normativa internazionale: analisi delle convenzioni internazionali rilevanti in materia di cybersicurezza, contrasto al terrorismo e alla criminalità informatica, la protezione dei dati; la direttiva e-privacy e le prospettive di riforma; Unione Europea: normativa generale ed interventi nell'area EU; analisi dei criteri, principi e adempimenti previsti dalle normative europee; il diritto italiano: analisi delle normative di recepimento nazionale, analisi di disposizioni rilevanti del codice penale, di procedura penale e della normativa speciale di settore; Perimetro Sicurezza, CSIRT e CERT: l'importanza dell'iteroperabilità tra Stato Regioni e azienda nella gestione degli alert di sicurezza.
Modulo 2 (600 ore) - Cyber crimes: imprese ed aziende private: analisi del quadro normativo applicabile al settore privato; il livello di sicurezza adeguato al rischio e la sicurezza degli strumenti di pagamento; analisi della giurisprudenza in tema di risarcimento dei danni da furto di identità e dati personali; analisi della distribuzione dei ruoli e delle responsabilità nelle organizzazioni complesse; evoluzione della criminalità informatica in Italia; evoluzione della criminalità informatica nel settore bancario; criminalità informatica e protezione degli asset informativi nel settore sanitario; il data breach (violazione dei dati) nelle imprese; procedure di indagine e gestione dei data breach; IoT overview (protocolli, standard e campi di applicazione); cybersecurity nel mondo industriale (ICS e SCADA) e nelle auto a guida autonoma; modelli di IoT Risk Assessment; delitti informatici e trattamenti illeciti di dati; il monitoraggio e la prevenzione: le armi delle aziende contro gli attacchi Cyber; l'importanza del SOC (Security Operation Center); l'analisi del "movimento laterale"; l'utilizzo di Honeypot Vulnerability Assessment e Test Penetration; la gestione dell'incidente: i log fondamentali da mantenere ed analizzare; le simulazioni e le procedure interne per il data breach.
Modulo 3 (300 ore) - Parte prima - Cyber crimes: la Pubblica Amministrazione: analisi del quadro normativo applicabile nelle PA; brevi cenni storici sulla criminalità informatica in Italia; il caso Noi PA; la sicurezza delle APP nella PA; analisi delle APP nella sanità pubblica: il caso di APP Immuni; il caso relativo alla truffa al CEO; analisi dell'APP Immuni: analisi del quadro normativo e le app di contact tracing nel contesto internazionale; furti d'identità in ambito sanitario pubblico e sanitario accreditato: come, quando e perchè.

ESPERIENZE ACCADEMICHE

CULTORE DELLA MATERIA SPS/12
Alma Mater Studiorum - Università di Bologna | dal 2022

TUTOR DIDATTICO LM SCIENZE CRIMINOLOGICHE
Alma Mater Studiorum - Università di Bologna | dal 2019

CONTRATTO CO.CO.CO. PER CORSI DI ALTA FORMAZIONE
Università di Pisa | 2017

MEMBERSHIP

SOCIO ORDINARIO
Società Italiana di Intelligence "SOCINT" | 2022

CONTATTI

Email: terranova.ken@gmail.com
LinkedIn: Ken Terranova

TRATTAMENTO DEI DATI PERSONALI

Parte seconda - Trattamento dei dati personali in ambito lavorativo: la disciplina privacy nei rapporti di lavoro pubblici e la nuova disciplina prevista dal Reg. UE 2016/679; i controlli a distanza sull'attività del lavoratore e riforma dell'art. 4 dopo il Jobs act: videosorveglianza, geolocalizzazione, dispositivi di riconoscimento biometrico; le soluzioni biometriche per il controllo, l'accesso e per la rilevazione presenza nella PA; gestione della posta elettronica e dei dati di navigazione su internet nell'ambito del rapporto di lavoro; ambito di utilizzabilità delle prove per fini disciplinari; lo smart working e la tutela della protezione dei dati; lo smart working e gli illeciti penali; analisi dei principali reati informatici e illeciti realizzati nelle imprese. Le garanzie costituzionali; reati posti a tutela dell'inviolabilità del domicilio; reati posti a tutela dell'inviolabilità dei segreti; delitti contro il patrimonio mediante violenza alle cose o persone; delitto contro il patrimonio mediante frode; illeciti penali in ambito protezione dei dati personali; illeciti penali in ambito legge sul diritto d'autore; illeciti presenti in diverse normative applicabili all'ambiente digitale; le indagini a tutela della persona offesa del reato: analisi dei casi di studio.
Modulo 4 (300 ore) - Cybersecurity e informatica forense: panoramica sulle Best Practices Computer Forensics; l'immodificabilità della fonte di prova ed il metodo scientifico; il sopralluogo informatico; analisi live e post mortem (i perchè, pro e contro); identicità della prova; hash, cosa sono ed il problema della collisione; catena custodia; ripetibilità delle operazioni; digital profiling e sociali engineering; gli strumenti della C.F. - open source vs commerciale; Write blocker ed hardware forense; le quattro fasi (identificazione, acquisizione, analisi, reporting) in pratica; GNU/Linux per la C.F.; cenni su casi reali di cronaca; panoramica sulla mobile forensics: tecniche di acquisizione ed analisi sui cellulari/tablet; live analysis ed acquisizione su un sistema acceso; il futuro della D.F.; i miti e le leggende; elementi di OSINT; indagini sulle criptovalute; introduzione all'Intelligenza Artificiale applicata al digital forensics; set-up di un Laboratorio di Digital Forensics; panoramica sui crimini informatici e la loro evoluzione e diffusione; malware e cracking; anatomia di un attacco informatico; le vulnerabilità; i rischi e le minacce (ransomware, phishing, social engineering, MITM, ecc.); la difesa (contromisure informatiche ed umane); la prevenzione e le regole; esempio di un protocollo SGSI; il Dark Web e sistemi di anonimizzazione; i vettori di malware; i nuovi cybercriminali; semplici regole di protezione domestica; la profilassi informatica; contromisure tecniche; incident response; la sicurezza come processo.

ALTRI CORSI, SEMINARI E CONVEGNI

CYBERSECURITY SPECIALIST MASTERY PROGRAM - ETHICAL HACKER
Geeks Academy | 2022

CORSO DI PERFEZIONAMENTO IN INTELLIGENCE E SICUREZZA NAZIONALE
Università degli Studi di Firenze - Scuola di Scienze politiche "Cesare Alfieri" | 2021
Tesi e specializzazione: Vulnerabilità formative nella trasformazione digitale

CORSO DI PERFEZIONAMENTO IN SCENARI INTERNAZIONALI DELLA CRIMINALITA' ORGANIZZATA
Università degli Studi di Milano Statale - 2021

AUTORIZZAZIONE
AUTORIZZO IL TRATTAMENTO DEI DATI PERSONALI CONTENUTI NEL MIO CURRICULUM VITAE IN BASE ALL'ART. 13DEL D. LGS. 196/2003 E ALL'ART. 13 DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI.