Con il patrocinio di

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Posteitaliane

GLOBAL CYBER SECURITY CENTER

# Corso Cyber Security 2019

## Executive Summary

*Il corso di livello tecnico-teorico, con esercitazioni pratiche e utilizzo di tool e piattaforme, mira ad approfondire gli aspetti tecnici e tecnologici relativi alle minacce informatiche e prevenire e rispondere correttamente in tempi brevi agli attacchi informatici.*

## Audience

*Il corso è rivolto a laureati in materie scientifiche (ingegneria informatica, informatica, matematica, fisica) o in alternativa con esperienza lavorativa nel settore dell'informatica operativa (programmatore, amministratore di sistema, analista) che vogliono sviluppare capacità e conoscenze per diventare Analista della Sicurezza.*

## Durata

*Il percorso didattico è articolato in 4 moduli, uno per mese.*
*Le attività di ciascun modulo, si svolgeranno in due giornate consecutive, dalle 9:00 alle 18.00, per un totale di 16 ore a settimana.*

## Programma

| | |
|---|---|
| Maggio, 21-22 | Malware Analysis |
| Giugno, 18-19 | Threat Intelligence e MISP |
| Luglio, 9-10 | Incident Response parte I |
| Settembre, 17-18 | Incident Response parte II |

## Partneship

*Le lezioni saranno tenute da docenti qualificati ed esperti in materia provenienti dalle principali organizzazioni di spicco del settore, partner dell'iniziativa.*

KASPERSKY lab

TS WAY

Posteitaliane

Global Cyber Security Center

Con il patrocinio di

Università della Calabria
Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica
DIMES

## Prerequisiti

*Per partecipare al corso è necessario avere già conoscenze base di sicurezza e in particolare di network security e programmazione.*

## Capacità e Competenze Acquisite

*Alla fine del corso i partecipanti avranno acquisito le capacità e le competenze per:*

- *Capacità di analisi di malware ed expolit;*
- *Comprendere le varie minacce (in particolare le APT), le tecniche e tattiche di attacco utilizzate;*
- *Applicare specifici metodi di monitoring e detection in caso di eventi/incidenti informatici;*
- *Seguire un processo di gestione incidenti.*

## Il Corso in breve

*Il numero e la complessità degli attacchi informatici, delle vulnerabilità e delle nuove minacce, va via via aumentando e le organizzazioni devono essere al passo con i tempi e saper rispondere con altrettanta velocità ad uno scenario in continua evoluzione. Per prevenire gli attacchi informatici è necessario un monitoraggio continuo e un'analisi approfondita sia dell'infrastruttura che comportamentale. Risulta dunque indispensabile avere all'interno del proprio staff esperti capaci di testare a fondo reti e sistemi, rilevare, prevenire e risolvere attacchi cyber a reti, sistemi, informazioni. Da tali considerazioni, nasce l'idea di istituire il corso di alta formazione in Cyber Security dedicato agli aspetti tecnici-operativi. Con l'ausilio di ambienti e piattaforme virtuali, i partecipanti, potranno simulare veri e propri attacchi e identificare le migliori misure a protezione del patrimonio informativo aziendale.*