

Sole
24 ORE
Formazione

MASTER PART-TIME

Cybersecurity



MASTER PART-TIME

Cybersecurity

Scopri il corso →

Il **Master** in **cyber security** fornisce una **preparazione olistica** ed **orientata alla risoluzione di problemi pratici** per un immediato inserimento in ogni contesto operativo. **Prepariamo la difesa alle minacce informatiche del domani.**

Il **programma formativo** mira a sviluppare **competenze** e **capacità tecniche** e **manageriali** sui diversi assi chiave in **ambito Cybersecurity** attraverso un **approccio pratico** e **professionalizzante** ed il **coinvolgimento** di **professionisti di rilievo**

MASTER PART-TIME

- 8 mesi di lezione concentrate nel weekend
- Ottobre 2023
- Pausa per le festività natalizie
- Lezioni un week end su due
- Milano

DETTAGLI

- Master Part-Time
- Lingua Italiano
- Prezzo: **€ 7.500** + IVA
  Consulta il sito** o **contattaci
  per scoprire le promozioni

CERTIFICATI

- Attestato di partecipazione

CARATTERISTICHE

Caratteristiche del Master

A chi è rivolto il Master

Il corso è rivolto a professionisti interessati ad acquisire nozioni specifiche del settore cybersecurity così come a dipendenti di organizzazioni che intendono aggiornare le proprie competenze. Il corso è a numero chiuso ed è previsto un numero massimo di partecipanti pari a 40.





Figure professionali in uscita

Il Master fornisce ai partecipanti competenze che consentano loro di intraprendere una carriera da security expert all'interno di aziende private e pubbliche amministrazioni.

CARATTERISTICHE

Struttura ed Orientamento Didattico

Struttura

*Il **Master è un corso Part-Time** a **numero chiuso** con **frequenza obbligatoria***



Lezioni:
concentrate nel weekend (Venerdì pomeriggio, Sabato)



Frequenza obbligatoria:
almeno 80% delle ore per ottenere il diploma



Durata complessiva:
8 mesi di lezioni (da ottobre a giugno)



Modalità di erogazione:
blended (sincrono e asincrono)

Didattica

*L'**orientamento didattico** del Master è **fortemente pratico-esperienziale**, finalizzato a fornire tutte **le competenze necessarie** in ambito **Cybersecurity** grazie ad un **mix tra lezioni teoriche, sessioni pratiche** ed **esperienze di valore***

80% **Ore erogate in modalità sincrona**

*Modello flessibile che consente di seguire le **lezioni in live streaming** o **on campus** a seconda delle esigenze*

20% **Ore erogate in modalità asincrona**

Lezioni messe a disposizione** su **piattaforma** dedicata **da poter fruire in ogni momento** e **da qualsiasi dispositivo

LEZIONE
Blended

PRATICA
Sincrona

ESPERIENZA
Sincrona

MODULI (1/3)

Moduli e Contenuti

Modulo	*Obiettivi didattici*	*Principali contenuti*
Aspetti normativi e legali su privacy e sicurezza (Testimonianza circuito Bain)	Il modulo approfondisce gli aspetti normativi in tema di cybersecurity ed analizza il loro impatto su aziende e pubbliche organizzazioni.	• Analisi reati informatici • Elementi di diritto nuove tecnologie
Cybercrime ed information warfare (Testimonianza Dolman Aradori NTT)	Il modulo analizza l'attuale panorama delle minacce informatiche, con un focus specifico sulle attività condotte da criminali informatici ed attori statutari. Sono analizzate per ciascuna categoria di attori malevoli, le tattiche, tecniche e procedure (TTP).	• Analisi attuale panorama delle minacce informatiche • Analisi principali categorie di attori malevoli e relative tattiche, tecniche e procedure • Il crimine informatico • Il modello di Cybercrime-as-a-Service • Concetti base di Information warfare • Legame tra crimine informatico e nation-state hacking
Cyber risk management nell'impresa (Testimonianza Nicola Sotira Poste Italiane CERT)	Il modulo illustra i concetti chiave per la gestione del rischio all'interno delle organizzazioni, introducendo concetti chiave per la definizione di una strategia atta all'incremento della resilienza ad attacchi informatici.	• Il rischio cibernetico e la sua gestione • La valutazione dei rischi (analisi minacce, analisi impatti, modelli per la valutazione dei rischi) • La gestione del rischio informatico all'interno di un'organizzazione • Normative • Governance e risk management aziendale



Per ogni modulo, previste **testimonianze** di **professionisti** di rilievo e **simulazioni pratiche** sui diversi temi

MODULI (2/3)

Moduli e Contenuti

Modulo	*Obiettivi didattici*	*Principali contenuti*
Incident response e threat intelligence (Testimonianza Domenico Raguseo Exprivia)	La risposta ad un incidente è essenziale per limitare gli effetti dello stesso e ripristinare in sicurezza le operazioni nel più breve tempo possibile. Il modulo illustra le varie fasi che compongono il processo di gestione degli incidenti, le figure professionali coinvolte e le tecnologie in uso.	Incident Response • SOC Processes Overview • Incidenti informatici • Processo di gestione di un incidente • Incidenti e Intelligence • Analisi Artifatti and Logs • Elementi di Computer Forensics • Cyber Crisis Response Threat Intelligence • Intelligence Process • Attori malevoli • Cyber Attack Frameworks (KillChain, Att&Ck) • Malware Intelligence (IoC, STIX model) • Darkweb Intelligence (Tor, Markets) • Tecnologie TIP e Security Operation Center
Crittografia e cybersecurity (Testimonianza Capo sicurezza Engineering come proposto da Bain)	Il modulo approfondisce i concetti base della crittografia ed illustra la loro implementazione in applicazioni di uso comune nel settore.	• Fondamenti di crittografia e crittoanalisi • Algoritmi di cifratura simmetrica e asimmetrica • Sistemi RSA e infrastrutture a chiavi pubbliche • Certificati digitali e Transport Layer Security • Hashing a password cracking, attacchi ai database • Attacchi MITM e protocollo Diffie-Hellman



Per ogni modulo, previste **testimonianze** di **professionisti** di rilievo e **simulazioni pratiche** sui diversi temi

MODULI (3/3)

Moduli e Contenuti

Modulo	*Obiettivi didattici*	*Principali contenuti*
Analisi malware (Gianni Amato CSIRT Nazionale)	Il modulo analizza le principali famiglie di codici malevoli (malware), le tecniche e tecnologie per la loro analisi, e le soluzioni per la difesa delle aziende da queste minacce.	• Introduzione alla malware analysis • Ambiente di laboratorio per l'analisi del malware • Analisi statica e Dinamica • Tecniche di evasione del malware • Analisi di case study di infection chain • Threat intelligence e threat hunting • Rilevamento e prevenzione malware
IoT e mobile security (Testimonianza Luca Iuliano Telsy)	Il modulo analizza gli aspetti propri di sicurezza per il dispositivo dell'internet delle code e dei dispositivi mobili. Si illustrano le metodiche di attacco e difesa per entrambe le categorie.	• Introduzione a IoT e Mobile Security • Sicurezza delle applicazioni mobile, Principali • Minacce alle applicazioni mobili • Analisi mobile malware • Gestione delle vulnerabilità
Tecniche di hacking (Testimonianza Luca Buongiorno capo cybersecurity lab zte)	Il modulo illustra tecniche e strumenti utilizzati in ciascuna fase di un'attività di penetration testing.	• Introduzione all'hacking etico • Penetration testing e vulnerability assessment • Principali attacchi • Il processo di penetration testing • Social Engineering • Web application hacking • Hardware hacking



Per ogni modulo, previste **testimonianze** di **professionisti** di rilievo e **simulazioni pratiche** sui diversi temi

FACULTY

Faculty

Docenti

*La **docenza** è **affidata** sia a **professori universitari** sia a **professionisti** di rilievo al fine di garantire un'**esperienza didattica completa** e **pratica***



Pierluigi Paganini

Coordinatore Scientifico del corso, CEO e fondatore di CYBHORUS, fondatore di Cybaze, membro dell'ENISA

(Short Bio da abbreviare)

Francesco Marcaldo

Ricercatore presso l'Università degli Studi del Molise di Campobasso

È ricercatore presso l'Università degli Studi del Molise di Campobasso ed è Associato di Ricerca presso l'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche (CNR) di Pisa.

(Manca Foto)

Luigi Martire

Esperto internazionale di Incident Response e Threat Intelligence, malware analysts

Manca Short Bio + Foto

Francesco Corona

Esperto di Sicurezza Informatica, docente con esperienza ventennale

(Manca Short Bio + Foto)

Andrea Marini

Esperto di Vulnerability Management & Prevention Gruppo Generali

(Short Bio da abbreviare + Foto)

Antonio Farina

Head of Cyber Threat Intelligence Research at Cluster25

Manca Short Bio + Foto

Antonio Colombo

DFIR Specialist and Cyber Threat Intelligence Enthusiastic, membro ISC2 Chapter Italy

Manca Short Bio + Foto

Luca Mella

Esperto di Sicurezza Informatica, Incident Response e Threat Intelligence

È esperto di Sicurezza Informatica, Incident Response e Threat Intelligence. Menzionato come Influential Malware Research Professionals.

(Manca Foto)

Carmine Di Biase

Technical director ed esperto di sicurezza infromatica per Namirial s.p.a.

Manca Short Bio + Foto

Marco Mariscoli

Avvocato (Manca Job Title)

Avvocato specializzato in diritto penale con particolare attenzione ai reati informatici e diritto nuove tecnologie.

(Manca Foto)

Davide Lo Prete

Esperto di Cyber Security Strategy & Governance

Manca Short Bio + Foto

PANELISTS

Testimonianze e Laboratori

*Di seguito solo alcuni dei tanti **panelist** che parteciperanno con **testimonianze** e **laboratori** al corso.*
*Essi sono **professori universitari** e **professionisti** di rilievo.*
*Tale tipologia approccio formativo è concepito con il fine di garantire un'**esperienza didattica completa** e **pratica***

Dolman Aradori

Head of Security di NTT Data

(Manca Short Bio + Foto)

Luca Iuliano

Engineering director di Telsy, Gruppo TIM

(Manca Short Bio + Foto)

Nicola Sotira

Head of Post Italiane CERT

(Manca Short Bio + Foto)

Luca Bongiorni

Direttore del Cybersecurity Lab e CSO di ZTE

(Manca Short Bio + Foto)

Gianni Amato

Senior Cybersecurity Consultant CERT-AgID

(Manca Short Bio + Foto)

Domenico Raguseo

Responsabile della Unit di CyberSecurity del gruppo Exprivia

(Manca Short Bio + Foto)

PARTNER

Network dei Partner

*Di seguito le **Aziende Partner** dei **Master Sole 24 Ore Formazione***

TERMINI E CONDIZIONI

Modalità di Iscrizione e Pagamento

Iscrizione



Il **Master** è a **numero chiuso** e prevede un **processo di selezione** ai fini di **valutare competenze tecniche, attitudini** e **motivazioni dei candidati**



Per la **candidatura** è necessario completare la **domanda di ammissione** con:

- **Curriculum Vitae**



Il **processo di selezione** prevede:

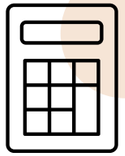
- **Analisi** della **domanda** di ammissione e **Curriculum Vitae**
- **Colloquio** orale

Pagamento



Quota di partecipazione:

- Prezzo: **€ 7.500** + IVA
  ***Consulta il sito** o **contattaci** per scoprire le promozioni*



Modalità di partecipazione:

- Il **pagamento** della quota **può avvenire tramite carta di credito** e **bonifico bancario**
- La quota può essere rateizzata in **quattro rate** da € ____ *+ IVA l'una*
- Possibilità di **finanziamento** con **Sella Personal Credit** previa approvazione della finanziaria*

** Messaggio pubblicitario con finalità promozionale. Operazione soggetta ad approvazione di Sella Personal Credit SpA. Per maggiori informazioni è possibile richiedere il modulo "Informazioni europee di base sul credito ai consumatori" (SECCI) e la copia del testo contrattuale.*



sole24oreformazione.it