MASTER

MASTER IN CYBERSECURITY, PREVENZIONE E GESTIONE DEGLI ATTACCHI INFORMATICI

ITMAS101

- DIPLOMA CERTIFICATO DA UN NOTAIO EUROPEO -



DESTINATARI

Questo corso si rivolge a uomini d'affari, manager, imprenditori, lavoratori, studenti e a tutti coloro che desiderano acquisire le conoscenze necessarie in relazione a questo settore professionale.

Permette di conoscere le competenze professionali necessarie per poter garantire la sicurezza dell'accesso e dell'utilizzo delle informazioni registrate sulle apparecchiature informatiche, nonché del sistema stesso, proteggendo da possibili attacchi, identificando le vulnerabilità e applicando sistemi di crittografia alle comunicazioni che vengono effettuate verso l'esterno e l'interno di qualsiasi organizzazione. Inoltre, alla fine di ogni unità didattica, gli studenti troveranno esercizi di autovalutazione che permetteranno loro di seguire il corso in modo indipendente.

Lo studente riceverà l'accesso a un corso iniziale in cui troverà informazioni sulla metodologia di apprendimento, sul titolo di studio che riceverà, sul funzionamento del Campus Virtuale, su cosa fare una volta terminato il corso e su informazioni su Grupo Esneca Formación.

SCHEDA TECNICA

ORE DI STUDIO
600H

MODALITÀ
ONLINE
*La modalità comprende moduli con lezioni dal vivo.

CORSO DI PRESENTAZIONE
ONLINE

TUTOR
PERSONALE

LINGUA
ITALIANO

DURATA
FINO AD UN ANNO
*Prorogabile

IMPORTO

IMPORTO ORIGINALE: ~~2720 €~~
IMPORTO ATTUALE: 680 €

TITOLO OTTENUTO

Un volta terminati gli studi e aver superato la prova di valutazione, l'alunno riceverà diploma che certifica il "**MASTER IN CYBERSECURITY, PREVENZIONE E GESTIONE DEGLI ATTACCHI INFORMATICI**", di ESNECA BUSINESS SCHOOL, avallato , grazie alla nostra condizione di soci, dal CECAP e AEEN, e cioè le massime istituzioni spagnole per la formazione e la qualità.

I nostri titoli, inoltre, posseggono il timbro del Notaio Europe, che garantisce la validità, i contenuti e l'autenticità dei titoli, a livello nazionale e internazionale.

CONTENUTO FORMATIVO

CYBERSECURITY, PREVENZIONE E GESTIONE DEGLI ATTACCHI INFORMATICI

INTRODUZIONE

MODULO 1. INTRODUZIONE ALLA CYBERSECURITY E AGLI ATTACCHI INFORMATICI

UNITÀ DIDATTICA 1. CYBERSECURITY

1. Funzioni
2. Differenziare i concetti relazionati
3. Assicurazione informatica

UNITÀ DIDATTICA 2. CENTRO PER LE OPERAZIONI DI SICUREZZA (SOC)

1. Servizi del SOC
2. Figura del *chief information security officer* (CISO)
   -Funzioni
   -Competenze e abilità
3. Cultura della cybersecurity nelle aziende

UNITÀ DIDATTICA 3. *CYBER THREAT INTELLIGENCE*

1. Campi di applicazione
2. Aspetti differenziali tra cybersecurity e cyber intelligence
3. Tipi di cyber intelligence
   -Cyber intelligence strategica
   -Cyber intelligence tattica
   -Cyber intelligence operativa
4. Il ruolo dell'analista di cyber intelligence
   -Compiti
   -Competenze e abilità

UNITÀ DIDATTICA 4. VANTAGGI DELL'INTELLIGENZA ARTIFICIALE

RIEPILOGO

AUTOVALUTAZIONE

MODULO 2. CRITTOGRAFIA

UNITÀ DIDATTICA 1. CONCETTO DI PRIVACY

UNITÀ DIDATTICA 2. LE BASI DELLA CRITTOGRAFIA E DELLA CIFRATURA

1. Principali utilizzi

UNITÀ DIDATTICA 3 . TIPOLOGIE DI CRITTOGRAFIA

1. Cifrari classici
   -Cifrario di Cesare
   -Cifrario di Vigenère

2. Crittografia simmetrica
   -Algoritmo DES
   -Algoritmo AES
3. Crittografia asimmetrica
   -Algoritmo RSA
   -Algoritmo Diffie Hellman
   -Algoritmo di Rabin
   -Algoritmo DSA
4. Crittografia ibrida

UNITÀ DIDATTICA 4. APPLICAZIONI DELLA CRITTOGRAFIA

1. Firma elettronica
2. Certificato digitale
3. Autenticazione

UNITÀ DIDATTICA 5. METODI DI OCCULTAMENTO DELLE INFORMAZIONI (STEGANOGRAFIA)

UNITÀ DIDATTICA 6. SISTEMI *BLOCKCHAIN*

UNITÀ DIDATTICA 7. CRITTOGRAFIA DI RETE

1. Rete TOR
2. *Deep* web
3. *Dark* web

RIEPILOGO

AUTOVALUTAZIONE

MODULO 3. BIOMETRIA

UNITÀ DIDATTICA 1. COS'È LA BIOMETRIA?

1. Utilizzi
2. Vantaggi

UNITÀ DIDATTICA 2. COMPONENTI DI UN SISTEMA BIOMETRICO

UNITÀ DIDATTICA 3. TIPI DI BIOMETRIA

1. Biometria fisiologica
   -Riconoscimento facciale
   -Riconoscimento oculare
   -Riconoscimento delle impronte digitali
   -Altri metodi fisiologici
2. Biometria comportamentale
   -Riconoscimento vocale
   -Riconoscimento della firma
   -Altri metodi comportamentali

UNITÀ DIDATTICA 4. RISCHI E VULNERABILITÀ NEI SISTEMI BIOMETRICI

UNITÀ DIDATTICA 5. BUONE PRATICHE DI RIDUZIONE DEL RISCHIO IN BIOMETRIA

RIEPILOGO

AUTOVALUTAZIONE

MODULO 4. ATTACCHI INFORMATICI A PASSWORD E RETI

UNITÀ DIDATTICA 1. CRIMINALITÀ INFORMATICA: CYBER ATTACCHI

1. Impatto degli attacchi informatici
2. Fasi di un attacco informatico

UNITÀ DIDATTICA 2. ATTACCHI INFORMATICI A PASSWORD

1. Attacco di forza bruta
2. Attacco a dizionario

UNITÀ DIDATTICA 3. ATTACCHI INFORMATICI ALLE RETI

1. Trappole
2. *Spoofing*
3. Attacco dei *cookie*
4. Attacco DDoS
5. Iniezione SQL
6. Scansione delle porte
7. *Sniffing*

RIEPILOGO

AUTOVALUTAZIONE

MODULO 5. ATTACCHI DI INGEGNERIA SOCIALE E *MALWARE*

UNITÀ DIDATTICA 1. COS'È L'INGEGNERIA SOCIALE?

UNITÀ DIDATTICA 2. ATTACCHI DI INGEGNERIA SOCIALE

1. *Spam*
2. *Phishing*
3. *Vishing*
4. *Smishing*
5. *Baiting*
6. *Shoulder surfing*
7. *Dumpster diving*

UNITÀ DIDATTICA 3. CONCETTO DI *MALWARE*

UNITÀ DIDATTICA 4. ATTACCHI *MALWARE*

1. Virus
2. *Trojan*
3. *Worm*
4. *Spyware*
5. Applicazioni dannose
6. *Adware*
7. *Botnet*
8. *Rogueware*
9. *Cryptojacking*

RIEPILOGO

AUTOVALUTAZIONE

MODULO 6. VULNERABILITÀ

UNITÀ DIDATTICA 1. COSA SONO LE VULNERABILITÀ?

UNITÀ DIDATTICA 2. *COMMON VULNERABILITY SCORING SYSTEM (CVSS)*

1. Metriche di base
   -Accesso vettoriale (AV)
   -Complessità di accesso (AC)
   -Autenticazione (Au)
   -Impatti
2. Metriche temporali
   -*Exploitability* (E)
   -Livello di riparazione (RL)
   -Relazione di fiducia (CR)
3. Metriche ambientali
   -Danno collaterale potenziale
   -Distribuzione degli obiettivi
   -Requisiti di confidenzialità, integrità e disponibilità
4. Calcolo del CVSS dopo la definizione delle metriche

UNITÀ DIDATTICA 3. PRINCIPALI TIPI DI VULNERABILITÀ

1. *Buffer overflow*
2. Situazione di corsa
3. Errore di formattazione delle stringhe
4. *Cross site scripting*
5. Iniezione SQL
   -Controllo debole degli accessi
6. Negazione del servizio

RIEPILOGO

AUTOVALUTAZIONE

MODULO 7. ANALISI E GESTIONE DI VULNERABILITÀ, RISCHI E ATTACCHI

UNITÀ DIDATTICA 1. COSA COMPRENDE LA GESTIONE DEL RISCHIO?

1. Analisi dei rischi
2. Trattamento dei rischi

UNITÀ DIDATTICA 2. MISURAZIONE DEL RISCHIO

1. Livello di pericolosità del cyber incidente
2. Livelli di rendicontazione obbligatori

UNITÀ DIDATTICA 3. FASI DELLA GESTIONE DEI CYBERINCIDENTI

1. Preparazione
2. Identificazione
3. Contenimento
4. Mitigazione
5. Recupero
6. Azione post-incidente

UNITÀ DIDATTICA 4. POLITICA DI GESTIONE DEI RISCHI

1. Politica di protezione dei dati
2. Politica delle password
3. Aggiornamento della politica
4. Politica di archiviazione e *backup*
5. Politica sull'uso di apparecchiature, applicazioni e posta elettronica
6. Politica sull'uso delle reti wireless
7. Politiche di classificazione delle informazioni

RIEPILOGO

AUTOVALUTAZIONE

MODULO 8. ANALISI FORENSE

UNITÀ DIDATTICA 1. IN COSA CONSISTE UN'ANALISI FORENSE?

1. Principi
2. Fasi
   -Raccolta di informazioni
   -Analisi
   -Stesura del rapporto

UNITÀ DIDATTICA 2. PROVE DIGITALI

1. Catena di custodia
2. Prove *online* e *offline*
3. Dati volatili e dati statici
4. Linee guida generali per la raccolta delle prove

UNITÀ DIDATTICA 3. ANALISI FORENSE IN BASE AL SISTEMA OPERATIVO

1. Windows
2. MacOS
3. Linux

UNITÀ DIDATTICA 4. ANALISI FORENSE DEL TRAFFICO DI RETE

UNITÀ DIDATTICA 5. ANALISI FORENSE DI STRUMENTI WEB

UNITÀ DIDATTICA 6. ALTRE APPLICAZIONI DI ANALISI FORENSE

1. Analisi dei dispositivi mobili
2. Analisi del *database*
3. Scansione della posta elettronica
4. Analisi del *cloud*

UNITÀ DIDATTICA 7. RECUPERO FILE

RIEPILOGO

AUTOVALUTAZIONE

MODULO 9. *ETHICAL HACKING*

UNITÀ DIDATTICA 1. COS'È L'*ETHICAL HACKING*?

1. Profilo dell'*hacker* etico
2. Benefici

UNITÀ DIDATTICA 2. FASI DELL'*ETHICAL HACKING*

1. Pianificazione
2. Riconoscimento
3. Accesso e analisi
4. Documentazione del processo
5. Analisi post-implementazione delle vulnerabilità segnalate

RIEPILOGO

AUTOVALUTAZIONE

MODULO 10. SICUREZZA DELLE INFORMAZIONI

UNITÀ DIDATTICA 1. CONCETTO DI SICUREZZA DELLE INFORMAZIONI

UNITÀ DIDATTICA 2. PRINCIPI ALLA BASE DELLA SICUREZZA DELLE INFORMAZIONI

1. Confidenzialità
2. Integrità
3. Disponibilità
4. Autenticità e non ripudio
5. Tracciabilità

UNITÀ DIDATTICA 3. GESTIONE INTERNA O ESTERNA DELLA SICUREZZA

UNITÀ DIDATTICA 4. CONTROLLI DI SICUREZZA

1. Controlli preventivi
2. Controlli di rilevamento
3. Controlli correttivi
4. Controlli di monitoraggio

RIEPILOGO

AUTOVALUTAZIONE

MODULO 11. SICUREZZA DEL WEB E DEI SISTEMI

UNITÀ DIDATTICA 1. PROTOCOLLO HTTP/HTTPS

UNITÀ DIDATTICA 2. INIEZIONI

1. HTML
2. *iFrame*
3. SQL

UNITÀ DIDATTICA 3. CONTROLLO DEGLI ACCESSI E AUTENTICAZIONE

UNITÀ DIDATTICA 4. CICLO DI VITA DELLO SVILUPPO DEI SISTEMI

UNITÀ DIDATTICA 5. SICUREZZA DEL *CLOUD*

UNITÀ DIDATTICA 6. SICUREZZA DEI *BIG DATA*

RIEPILOGO

AUTOVALUTAZIONE

MODULO 12. SICUREZZA IoT

UNITÀ DIDATTICA 1. INTERNET DELLE COSE (IoT)

1. Architettura IoT

UNITÀ DIDATTICA 2. CYBERSECURITY NEI DISPOSITIVI IoT

1. Minacce ai dispositivi IoT
   -Lacune nella trasmissione dei dati
   -Difetti nell'*hardware*
   -Difetti nel *software*
   -Errori di configurazione
2. Valutazione della sicurezza IoT

UNITÀ DIDATTICA 3. GESTIONE DELLA SICUREZZA IoT

RIEPILOGO

AUTOVALUTAZIONE

MODULO 13. SICUREZZA DELLA RETE

UNITÀ DIDATTICA 1. PROTOCOLLI TCP/IP

UNITÀ DIDATTICA 2. *FIREWALL*

UNITÀ DIDATTICA 3. SISTEMI E STRUMENTI DI PROTEZIONE DELLA RETE

1. SIEM
2. IDS
3. IPS
4. DLP
5. VPN

UNITÀ DIDATTICA 4. SICUREZZA DELLA RETE WIRELESS

1. *Wired equivalent privacy* (WEP)
2. *Wifi protected access* (WPA)
   -WPA
   -WPA2
   -WPA3

RIEPILOGO

AUTOVALUTAZIONE

SOLUZIONI

BIBLIOGRAFIA COMPLEMENTARE