

hacking & security



EC-COUNCIL | CATALOGO CORSI

Hackers are here Where are you?

OverNet Education è dal 2008 il più importante Centro Autorizzato di Formazione EC-Council, in grado di erogare con docenti certificati formazione in lingua italiana.

Per diversi anni OverNet Education ha vinto il prestigioso premio Circle of Excellence Award EC-Council che premia il partner che offre il miglior servizio ai suoi studenti.

L'INTERNATIONAL COUNCIL OF ELECTRONIC COMMERCE CONSULTANTS EC-COUNCIL

EC-Council è un'organizzazione indipendente, con sede a New York, la cui **missione è definire standard professionali nel settore della sicurezza e dell'e-business**. EC-Council è membro e segue le direttive del NOCA.

Il National Organisation for Competency Assurance (NOCA) è un ente che garantisce che le organizzazioni aderenti siano competenti nel loro settore e che rilascino certificazioni sviluppate nel rispetto dei più elevati standard professionali.

Attraverso il proprio network mondiale EC-Council ha certificato professionisti appartenenti a organizzazioni quali FBI, CIA, US Marine, US Air force, US Army, Singapore Police Force, Maritime & Port Authority of Singapore, Stock Exchange of Singapore, Malaysia's Ministry of Defence, Citibank, Hewlett Packard, IBM, VISA, Sony, American Express, Kodak, Fujitsu, Federal Express and UPS.

In Italia: Vodafone, Telecom e alcune banche italiane di primo livello.



OverNet
EDUCATION

Ma quali sono la metodologia e la filosofia che guidano questa linea formativa che si propone di analizzare ogni aspetto legato alla sicurezza e aumentare la visibilità delle reali problematiche esistenti in questo ambito in ogni realtà aziendale?

ESPERTI IN I-SECURITY: FIGURE PROFESSIONALI EMERGENTI

L'evoluzione, la complessità e la continuità degli attacchi informatici richiedono l'intervento di **figure professionali con una competenza specifica di information security** (i-security), che è diversa da quella del System Admin o Network Manager.

Le figure professionali dell'Ethical Hacker, dell'esperto di Computer Forensic, delle Sicurezza delle Reti Wireless o del Penetration Tester rispondono in maniera adeguata alle esigenze di sicurezza.

Per chi invece è già esperto di sicurezza ed è interessato a una carriera manageriale, l'EC-Council offre anche corsi di management che consentono di acquisire lo skill necessario per diventare Chief Information Security Officer (CISO).

IL VALORE DELLA CERTIFICAZIONE DELL'EC-COUNCIL

Le certificazioni dell'EC-Council sono fra le più importanti nel settore della sicurezza. La certificazione più famosa, quella del Certified Ethical Hacker (CEH) se paragonata ad altre di uguale prestigio, presenta i migliori risultati in termini di R.o.I. (Return of Investment), sviluppo della carriera, domanda nel settore della sicurezza e sviluppo del proprio potenziale



CONTATTI - Per essere sempre aggiornato su disponibilità, prezzi e date dei corsi consulta il sito: www.OverNetEducation.it oppure contattaci: info@overneteducation.it - +39 02 365738

EC001
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE SONO INCLUSI

- | 1 **VOUCHER ESAME** VALIDO 1 ANNO
- | 1 **STUDENT BOOKS**
- | 1 **LAB MANUAL**
- | Accessi alla piattaforma **ASPEN** per usare gli strumenti online di supporto alla formazione

- | CORSO: **EC001**
- | DURATA: **4.5 GIORNI**
- | PREZZO: **3.500,00€**
- | TITOLO ESAME: **CERTIFIED ETHICAL HACKER (ANSI)**
- | TIPO ESAME: **QSM**
- | ESAME: **312-50 (ECC EXAM), 312-50 (VUE)**
- | NUMERO DOMANDE: **125**
- | DURATA ESAME: **4 ORE**
- | DISPONIBILTA': **ECC EXAM/VUE**

Descrizione del corso

Il corso Certified Ethical Hacker (C|EH v11) è un corso riconosciuto a livello internazionale. Si tratta di una certificazione riconosciuta e accreditata in conformità ANSI 17024, che dà credibilità e valore aggiunto ai membri certificati.

È ora disponibile in versione 11. Il corso è stato aggiornato per fornire agli studenti gli strumenti e le tecniche utilizzate da hackers e professionisti della sicurezza, allo scopo di poter entrare in qualsiasi sistema informativo. Il programma farà immedesimare i partecipanti "nella mentalità dell'Hacker", cioè insegnerà a pensare come un Hacker e difendersi meglio.

Gli studenti comprenderanno come scansionare, testare e proteggere un sistema. Il corso copre le 5 fasi dell'Ethical Hacking: "Reconnaissance, Gaining Access, Enumeration, Maintaining Access and Covering your tracks".

Il corso è organizzato in una parte di aula con il docente e una parte in autoapprendimento. Il docente, all'inizio del corso, fornirà i dettagli delle parti da studiare in autoapprendimento.

A chi si rivolge

Information Security Analyst / Administrator - Information Assurance (IA) Security Officer - Information Security Manager / Specialist - Information Systems Security Engineer / Manager - Information Security Professionals / Officers - Information Security / IT Auditors - Risk / Threat / Vulnerability Analyst - System Administrators - Network Administrators and Engineers

Certificazione

Gli studenti dovranno superare l'esame sulla piattaforma ECC Exam per conseguire la certificazione.

Gli studenti che hanno superato l'esame riceveranno il certificato CEH.

EC007
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO

| 1 **VOUCHER ESAME** VALIDO 1 ANNO

| CORSO: **EC007**
| DURATA: **5 GIORNI**
| PREZZO: **3.900,00€**
| TITOLO ESAME: **CCISO**
| ESAME: **250 QCM**
| PUNTEGGIO MINIMO: **70%**
| DURATA ESAME: **4 ORE**
| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Il programma CCISO di EC-Council certifica i manager della sicurezza informatica in tutto il mondo.

È la prima formazione mirata a certificare dei professionisti a livello approfondito sulle competenze nel campo della sicurezza informatica. Il corso CCISO non è solo concentrato sulle conoscenze tecniche, ma si orienta anche sull'impatto della gestione della sicurezza informatica dal punto di vista manageriale.

Il programma CCISO è stato sviluppato da esperti con ruolo di CISO ed è rivolto ai loro pari ma anche agli aspiranti CISO. Ogni modulo di questo programma è stato sviluppato con la volontà di certificare i nuovi CISO e anche con l'obiettivo di trasmettere loro le competenze necessarie per raggiungere la generazione dei futuri manager capace di implementare e gestire una vera politica di sicurezza informatica.

A chi si rivolge

Questa formazione è rivolta a Responsabili di IT Security che desiderano sviluppare e qualificare le loro competenze e adattare le conoscenze tecniche alle problematiche generali di impresa.

Certificazione

Gli studenti dovranno superare l'esame sulla piattaforma ECC Exam per conseguire la certificazione.

Gli studenti che hanno superato l'esame riceveranno il certificato CISO.



| CORSO: **CISSP**
| DURATA: **5 GIORNI**
| PREZZO: **3.250,00€**
| TITOLO ESAME: **CISSP**
| ESAME: **250 QSM**
| PUNTEGGIO MINIMO: **700/1000**
PUNTI
| DURATA ESAME: **6 ORE**

Descrizione del corso

La Certificazione CISSP non è solo un riconoscimento oggettivo di eccellenza, ma uno standard riconosciuto a livello mondiale.

Al completamento del corso lo studente avrà acquisito conoscenze e competenze per lo sviluppo di politiche di sicurezza IT, norme e procedure per metterne in pratica l'attuazione in tutta l'azienda.

Il corso è erogato in lingua italiana da docente certificato CISSP ed esperto in materia.

Al termine del corso gli studenti avranno acquisito competenze nei seguenti argomenti:

1. Security & Risk Management
2. Asset Security
3. Security Engineering
4. Communications & Network Security
5. Identity and Access Management
6. Security Assessment & Testing
7. Security Operations
8. Software Development Security

A chi si rivolge

Il corso è rivolto a esperti nella sicurezza dei sistemi informativi e a chi deve prepararsi alla certificazione professionale CISSP.

Certificazione

Il corso **non include** il voucher esame

EC002
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO
| 1 VOUCHER ESAME VALIDO 1 ANNO

| CORSO: **EC002**
| DURATA: **4.5 GIORNI**
| PREZZO: **3.500,00€**
| TITOLO ESAME: **CHFI 312-49**
| ESAME: **150 QSM**
| PUNTEGGIO MINIMO: **70%**
| DURATA ESAME: **4 ORE**
| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Il corso CHFI darà ai partecipanti le competenze necessarie ad individuare tracce di un'intrusione e raccogliere correttamente le fonti di prova necessarie a dimostrare l'accaduto. Durante il corso verranno mostrati e utilizzati molti dei migliori strumenti a oggi reperibili sul mercato: software, hardware e tecnologie specializzate.

La necessità per le aziende di diventare più efficienti e integrate tra di loro ha dato vita ad un nuovo tipo di criminalità, il "cyber-criminal".

Non è più una questione di "la tua organizzazione sarà attaccata (hacked)?" ma, piuttosto, "quando accadrà?".

"Oggi le battaglie tra aziende, governi e paesi non sono più combattute solo nelle sale riunioni o nei campi di battaglia usando la forza fisica", ora iniziano nel "regno" della tecnologia, che è sempre più parte della vita moderna.

Se la vostra organizzazione richiede le conoscenze o le competenze per identificare, rintracciare e perseguire i criminali informatici, allora questo è il corso per voi.

A chi si rivolge

Questo corso è rivolto a organi e agenzie di polizia, governative, personale della Difesa e Militare, professionisti della sicurezza in ambito commerciale, bancario, assicurativo e forense, amministratori di Sistema e IT managers.

Certificazione

Gli studenti dovranno superare l'esame sulla piattaforma ECC Exam per conseguire la certificazione.

Gli studenti che hanno superato l'esame riceveranno il certificato CHFI.



NELL'ISCRIZIONE E' INCLUSO
| 1 VOUCHER ESAME VALIDO 1 ANNO

| CORSO: **EC010**
| DURATA: **3 GIORNI**
| PREZZO: **2.100,00€**
| ESAME: **CASE .NET**
| NUMERO DOMANDE: **50 QSM**
| DURATA ESAME: **2 ORE**
| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Il programma CASE è concentrato sui processi di sviluppo di applicazioni .NET in modo sicuro. E' un corso pratico che comprende le misure di sicurezza nell'intero ciclo di vita dello sviluppo di applicazioni (SDLC - Secure Software Development Lifecycle): pianificazione, creazione, test e rilascio dell'applicazione.

Gli studenti, dopo la frequenza di questo corso conosceranno:

1. Understanding Application Security, Threats, and Attacks
2. Security Requirements Gathering
3. Secure Application Design and Architecture
4. Secure Coding Practices for Input Validation
5. Secure Coding Practices for Authentication and Authorization
6. Secure Coding Practices for Cryptography
7. Secure Coding Practices for Session Management
8. Secure Coding Practices for Error Handling
9. Static and Dynamic Application Security Testing (SAST & DAST)
10. Secure Deployment and Maintenance

A chi si rivolge

Il corso CASE è rivolto sviluppatori .NET con un'esperienza minima di 2 anni e tutti coloro che vogliono diventare ingegneri, analisti, testers in sicurezza delle applicazioni. Responsabili per il sviluppo, il test, la gestione e la protezione delle applicazioni.

Certificazione

Gli studenti dovranno accedere l'esame sulla piattaforma ECC exam per ricevere la certificazione.

Gli studenti che hanno superato l'esame riceveranno il certificato CASE.

ECO08
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO
| 1 **VOUCHER ESAME** VALIDO 1
ANNO

| CORSO: **ECO08**
| DURATA: **3 GIORNI**
| PREZZO: **2.500,00€**
| TITOLO ESAME: **EC-COUNCIL
CERTIFIED INCIDENT HANDLER**
| ESAME: **ECIH 212-89**
| NUMERO DOMANDE: **100**
A SCELTA MULTIPLA
| DURATA ESAME: **3 ORE**
| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Il programma ECIHv2 propone un approccio olistico che copre numerosi argomenti intorno alla risposta e gestione della compromissione.

Il corso va dalla preparazione e pianificazione del processo di risposta della compromissione fino al recupero delle risorse importanti dell'organizzazione dopo un incidente di sicurezza. Allo scopo di proteggere le organizzazioni, questi concetti sono fondamentali per poter gestire e rispondere a futuri attacchi e minacce.

Gli studenti, dopo la frequenza di questo corso avranno una profonda conoscenza delle seguenti aree:

1. Introduction to Incident Handling and Response
2. Incident Handling and Response Process
3. Forensic Readiness and First Response
4. Handling and Responding to Malware Incidents
5. Handling and Responding to Email Security Incidents
6. Handling and Responding to Network Security Incidents
7. Handling and Responding to Web Application Security Incidents
8. Handling and Responding to Cloud Security Incidents
9. Handling and Responding to Insider Threats,

A chi si rivolge

Questo corso è particolarmente utile ai tecnici di IT security, amministratori di valutazione dei rischi, per testers, cyber investigatori giudiziari, amministratori sistemi, ingegnere sistemi, amministratori firewall, responsabili delle rete, responsabili e professionisti IT e tutte le persone interessate alla gestione e alla risposta delle compromissioni alla sicurezza informatica.

Certificazione

Gli studenti dovranno accedere l'esame sulla piattaforma ECC exam per ricevere la certificazione.

Gli studenti che hanno superato l'esame riceveranno il certificato CIH

EC014
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO
| 1 VOUCHER ESAME VALIDO 1 ANNO

| CORSO: **EC014**
| DURATA: **5 GIORNI**
| PREZZO: **3.500,00€**
| TITOLO ESAME: **CPENT**
| PUNTEGGIO MINIMO: **70% (CPENT) O 90% (LPT MASTER)**
| DURATA ESAME: **24 ORE**
| DISPONIBILTA': **RPS**

Descrizione del corso

Il programma CPENT insegna come eseguire un pen-test efficace in un ambiente di rete aziendale che deve essere attaccato, bypassato e difeso. Se avete lavorato solo in reti tradizionali, CPENT vi insegnerà a passare al livello successivo mostrandovi come testare i sistemi IoT e OT, come scrivere i vostri exploit, costruire i vostri strumenti, eseguire exploit binari avanzati, double pivot per accedere alle reti nascoste, e anche personalizzare gli script/esplosi per penetrare i segmenti più intimi della rete.

Il cuore del programma CPENT è quello di aiutarvi a padroneggiare le vostre competenze in pen-test, mettendole in pratica sulle nostre range cibernetiche.

Le range CPENT sono state progettate per essere dinamiche per fornirvi un programma di formazione nel mondo reale, così come gli obiettivi e la tecnologia continuano a evolversi nelle reti dal vivo, le range di formazione e test CPENT imiteranno questa realtà mentre il nostro team di ingegneri continua ad aggiungere obiettivi e difese per tutta la durata del corso CPENT.

A chi si rivolge

Questa formazione è rivolta ad amministratori rete, amministratori sicurezza rete, ingegnere sicurezza rete, tecnico difesa rete, analista CND, analista sicurezza, responsabile sicurezza e ogni persona coinvolta nelle operazioni rete.

Certificazione

CPENT è un esame pratico, completamente online e protratto in remoto, che mette alla prova i candidati attraverso un esame pratico, basato sulle prestazioni, della durata di 24 ore. L'esame è suddiviso in 2 esami di 12 ore ciascuno.

I candidati che ottengono un punteggio superiore al 70% otterranno la certificazione CPENT. I candidati che ottengono un punteggio superiore al 90% ottengono la prestigiosa credenziale LPT (Master).

EC009
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO

| 1 **VOUCHER ESAME** VALIDO 1 ANNO

| CORSO: **EC009**
| DURATA: **3 GIORNI**
| PREZZO: **2.500,00€**
| TITOLO ESAME: **CERTIFIED THREAT INTELLIGENCE ANALYST**
| ESAME: **CTIA 312-85**
| NUMERO DOMANDE: **50**
| **A SCELTA MULTIPLA**
| DURATA ESAME: **2 ORE**
| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Certified Threat Intelligence Analyst (C|TIA) è un corso progettato e sviluppato in collaborazione con esperti in sicurezza informatica ed informazioni. L'obiettivo è di aiutare gli organismi ad identificare e ridurre i rischi presso un'azienda scoprendo le minacce interne ed esterne fin'ora sconosciute. Il corso basato sul Job Task Analysis (JTA), insegna una metodologia dettagliata allo scopo di stabilire una threat intelligence efficace. Copre numerosi argomenti, dalla pianificazione del progetto di threat intelligence fino all'elaborazione del rapporto e della sua diffusione. Gli studenti, dopo la frequenza di questo corso avranno una profonda conoscenza delle seguenti aree:

1. Introduction to Threat Intelligence
2. Cyber Threats and Kill Chain Methodology
3. Requirements, Planning, Direction, and Review
4. Data Collection and Processing
5. Data Analysis
6. Intelligence Reporting and Dissemination

A chi si rivolge

Ogni professionista della sicurezza informatica con almeno 3-5 anni di esperienza.

Certificazione

Gli studenti dovranno accedere l'esame sulla piattaforma ECC exam per ricevere la certificazione.

I candidati che superano l'esame riceveranno il certificato CTIA.

EC011
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO

| 1 VOUCHER ESAME VALIDO 1 ANNO

| CORSO: **EC011**

| DURATA: **5 GIORNI**

| PREZZO: **2.700,00€**

| TITOLO ESAME: **CERTIFIED NETWORK DEFENDER (ANSI)**

| ESAME: **CND 312-38**

| NUMERO DOMANDE: **100 INTERATTIVE A SCELTA MULTIPLE**

| DURATA ESAME: **4 ORE**

| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Il Certified Network Defender CND è un corso pratico, erogato da docenti certificati. Permetterà agli studenti di certificarsi sulla sicurezza delle reti. Con un programma intensivo e labs, la formazione è stata creata su precise competenze, direttamente legate all'analisi delle proprie responsabilità sul posto di lavoro e all'ambito di formazione cybersecurity data dal National Initiative of Cybersecurity Education (NICE). Oltre ai ruoli di system/network administrators del dipartimento di difesa, il corso viene adattato anche ad altre figure.

Allo scopo di ottenere le competenze operative nella sicurezza di difesa delle reti, la formazione prepara gli amministratori rete alle ultime tecnologie e pratiche di sicurezza.

Il programma Certified Network Defender v2 è stato aggiornato per dare agli studenti tutte le risorse e conoscenze necessarie per aiutare il Blue Team a difendere gli assets.

A chi si rivolge

Questa formazione è rivolta ad amministratori rete, amministratori sicurezza rete, ingegnere sicurezza rete, tecnico difesa rete, analista CND, analista sicurezza, responsabile sicurezza e ogni persona coinvolta nelle operazioni rete.

Certificazione

Gli studenti dovranno accedere l'esame sulla piattaforma ECC exam per ricevere la certificazione.

I candidati che superano l'esame riceveranno il certificato CND.

EC012
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO

| 1 **VOUCHER ESAME** VALIDO 1 ANNO

| CORSO: **EC012**
| DURATA: **3 GIORNI**
| PREZZO: **2.100,00€**
| TITOLO ESAME: **CERTIFIED SOC ANALYST**
| ESAME: **CTIA 312-39**
| NUMERO DOMANDE: **100**
A SCELTA MULTIPLA
| DURATA ESAME: **3 ORE**
| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

Il programma Certified SOC Analyst è la prima tappa per collaborare in un SOC Security Operations Center. Il corso è progettato per gli attuali e aspiranti analisti SOC di livello I e di livello II per acquisire competenza nell'esecuzione di operazioni di livello base e intermedio.

Il programma evidenzia la creazione di nuove possibilità di carriera grazie alle conoscenze approfondite e meticolose imparate che poi permettono di contribuire in modo dinamico ad un team SOC. Si tratta di un corso intensivo di 3 giorni, copre a fondo i principi fondamentali delle operazioni SOC, della gestione e correlazione di logs, dello schieramento SIEM, della rivelazione avanzata di incidenti fino alla risposta.

Inoltre il candidato imparerà come gestire numerosi processi SOC e a collaborare con il CSIRT in caso di necessità.

A chi si rivolge

Analisti SOC (Livello I e Livello II)

Ogni professionista in sicurezza che si occupa di sicurezza di rete

Analisti Cyber Sicurezza

Tutti coloro che vogliono diventare Analista SOC

Certificazione

Gli studenti dovranno accedere l'esame sulla piattaforma ECC exam per ricevere la certificazione.

I candidati che superano l'esame riceveranno il certificato CSA.

EC013
PROGRAMMA
C O M P L E T O



NELL'ISCRIZIONE E' INCLUSO

| 1 VOUCHER ESAME VALIDO 1 ANNO

| CORSO: **EC013**

| DURATA: **5 GIORNI**

| PREZZO: **3.500,00€**

| TITOLO ESAME: **EC-COUNCIL
DISASTER RECOVERY
PROFESSIONAL**

| ESAME: **312-76**

| NUMERO DOMANDE: **150
QSM**

| DURATA ESAME: **4 ORE**

| DISPONIBILTA': **ECC EXAM**

Descrizione del corso

La certificazione EDRP mira a insegnare e convalidare le capacità dello studente di pianificare, sistemare e mantenere un piano di continuità di attività (PCA) e di ripresa di attività (PRA).

Il programma EDRP porta ai professionisti un'analisi profonda dei principi di continuità e di ripresa di attività, includendo lo studio dell'impatto sull'impresa, la valutazione dei rischi, lo sviluppo di politiche e procedure, e la creazione di un PCA/PRA.

Permette ai professionisti di rendere sicuri i loro dati applicando le politiche e procedure in vigore. Il corso EDRP insegnerà come recuperare e ristabilire i dati critici di un'organizzazione di seguito ad un danno subito.

A chi si rivolge

Questo corso si rivolge ai professionisti IT della continuità e ripresa di attività, ai consulenti di continuità e ripresa di attività, ai consulenti e managers del rischio IT, ai CISOs e Direttori IT.

Certificazione

Gli studenti dovranno accedere l'esame sulla piattaforma ECC exam per ricevere la certificazione.

I candidati che superano l'esame riceveranno il certificato DRP.

Descrizione del corso

Il corso **accorpa** i programmi dei corsi ufficiali EC-Council:

- **EC009 - Certified Threat Intelligence Analyst**
- **EC012 - Certified SOC Analyst**
- **EC008 - Certified Incident Handler**

Nella quota del corso sono inclusi i voucher per sostenere i relativi esami di certificazione.

EC08912

PROGRAMMA

C O M P L E T O



NELL'ISCRIZIONE SONO INCLUSI

| 3 VOUCHER ESAME VALIDI 1 ANNO

A chi si rivolge

Il corso è rivolto a chi desidera acquisire solide competenze Security certificate.

| CORSO: **EC08912**
| DURATA: **7 GIORNI**
| PREZZO: **4.300,00€**

OverNet

EDUCATION

OVERNET SOLUTIONS SRL

Direzione e sede Amministrativa
Centro Direzionale Milanofiori
Strada 4 - Palazzo Q5
20089 Rozzano MI

OVERNET EDUCATION

Rozzano - Milano

T +39 02 365738
F +39 02 36573840

Bologna

T +39 051 269911
F +39 051 223010

Roma

T +39 02 365738

info@overneteducation.it
<http://overneteducation.it>



Rispetta l'ambiente ricicla la carta