

LA TECHNOLOGY TRANSFER PRESENTA

CLEMENT DUPUIS

CISSP®

Corso e Workshop
di preparazione all'esame
di Certificazione

ROMA 19-23 APRILE 2010
VISCONTI PALACE HOTEL - VIA FEDERICO CESI, 37



info@technologytransfer.it
www.technologytransfer.it

DESCRIZIONE

La Technology Transfer, in collaborazione con la Security University, propone un eccellente corso di preparazione all'esame CISSP®, tenuto da Clement Dupuis, il padre di www.cccure.org e che vanta al suo attivo una percentuale di oltre il 95% di suoi studenti che passano l'esame al primo tentativo. Il corso non solo aiuterà i partecipanti a superare l'esame e a conseguire la Certificazione, ma insegnerà i complessi concetti dei dieci domini del CBK (Common Body of Knowledge) e spiegherà come questi aspetti lavorano assieme per la costruzione di una vera e approfondita difesa. Verranno utilizzate tecniche avanzate di apprendimento e molti quiz giornalieri che Vi permetteranno di padroneggiare i 10 domini e di superare con facilità l'esame.

Cosa rende unico questo corso rispetto agli altri:

- L'eccellenza del docente, riconosciuta a livello internazionale, sia per gli aspetti didattici che per i risultati ottenuti
- Materiali didattici costantemente aggiornati
- Quiz giornalieri
- Una sezione di consigli e suggerimenti, una sezione di terminologia e 20 domande in ciascun modulo
- Una pratica dell'esame finale con oltre 100 domande

PARTECIPANTI

Professionisti di Information Security che devono affrontare l'esame di certificazione CISSP.

1. Information Security e Risk Management

Identificare le risorse informative dell'organizzazione e sviluppare, documentare e implementare politiche, standards, procedure e guidelines per identificare il rischio.

- CIA
- Ruoli e Responsabilità: RACI
- Asset Management
- Tassonomia: classificazione dell'informazione
- Risk Management
- Analisi e valutazione del rischio
- Classificazione dell'informazione
- Politiche, Procedure, Standards e Guidelines
- Programmi di consapevolezza della sicurezza
- Certificazione e accreditamento

2. Access Control

I controlli dell'accesso sono una serie di meccanismi che lavorano insieme per creare una architettura di sicurezza per proteggere gli assi del sistema informativo.

- AAA
- Accesso ai sistemi e ai dati
- IPS prevenzione dell'intrusione e IDS detection
- Monitoraggio delle tracce
- Metodi di autenticazione
- Autorizzazione: DAC, RBAC, MAC
- Accounting: Logging, Monitoring, Auditing
- Gestione Centralizzata/Decentralizzata e Ibrida
- Single Sign-on: Kerberos, Radius, Diameter, TACACS
- Minacce
- Vulnerabilità

3. Crittografia

La crittografia indirizza i principi, mezzi e metodi per mascherare l'informazione assicurando l'integrità, la riservatezza e l'autenticità.

- Terminologia
- Cripto sistemi
- Cifrari
- Algoritmi
- Hashing
- Componenti dell'infrastruttura della Chiave Pubblica
- Firme elettroniche
- Simmetrica/Asimmetrica
- PKI
- Sicurezza Internet
- Cripto sistemi. SSL, S/MIME, PGP
- Criptoanalisi

4. Sicurezza Fisica

Il dominio della sicurezza fisica fornisce tecniche di protezione per l'intera struttura, dal perimetro esterno allo spazio interno dell'ufficio, includendo tutte le risorse del sistema informativo.

- Edifici e infrastruttura collegata
- Controllo tecnici
- Facilities: riscaldamento/raffreddamento, pianta elettrica e sistema idraulico
- Facility Design
- Sicurezza dagli incendi
- Sicurezza elettrica
- HVAC
- Sicurezza del perimetro: recinti, cancelli e illuminazione
- Installazione fisica: edifici e strutture che ospitano computers
- Controllo dell'accesso fisico: Transponders, Badges, Swipe Cards
- Furto
- Intrusion Detection: CCTV, Allarmi, Guardie e Cani

5. Architettura di Sicurezza e Design

Contiene i concetti, principi, strutture e standards usati per progettare, monitorare e mettere in sicurezza sistemi operativi, apparecchiature, reti, applicazioni e tutti quei controlli usati per forzare vari livelli di disponibilità, integrità e confidenzialità.

- Identificare le problematiche di sicurezza con architetture e designs
- Layering, Data Hiding e Astrazione
- Processori
- Memoria
- Sistemi operativi
- Definire e capire modelli di sistema
- Assicurazione. TCSEC, ITSEC, CC
- Problemi di Architettura: canali coperti + TOC/TOU, riuso dell'oggetto

6. Sicurezza dell'Applicazione

Indirizza gli aspetti di sicurezza da applicare allo sviluppo delle applicazioni software e mette in evidenza l'ambiente dove il software è progettato e sviluppato.

- Principi generali di sicurezza
- Database
- Applicazioni
- Modelli di Intelligenza Artificiale
- SDL
- Attacchi al programma e ai dati
- Malware
- Minacce
- Aspetti del mondo reale
- Change Management
- Sicurezza del Database
- Mobil Code

7. Sicurezza per le Telecomunicazioni, Networks e Internet

- Strutture di Network
- Metodologia di trasmissione
- Formati di trasporto
- Modelli OSI/DoD e TCP/IP
- TCP/UDP/ICMP/IP
- Ethernet
- Dispositivi:
 - Routers/Switches/Hubs
- Firewalls
- Wireless
- Tecnologie WAN: X.25/Frame Relay/PPP/ISDN/DSL/Cable
- Voce: PBX/telefoni cellulari/VOIP
- IPSec
- Vulnerabilità del network

8. Aspetti legali, norme, compliance e investigazioni

- Leggi e norme di Computer Crime
- Le misure e le tecnologie impiegate per investigare sui reati di computer crime
- Etica: due care/due diligence
- Proprietà intellettuale
- Incident response
- Forensics
- Prova
- Leggi: HIPAA, GBL, SOX

9. Business Continuity e Disaster Recovery Planning

- Politica
- Ruoli e Teams
- Business Continuity Planning
- Valutazione dell'impatto sul Business
- Strategia di Recovery
- Sviluppo del Piano di Recovery
- Risposta all'emergenza
- Backups di dati, Vaulting, Journaling, Shadowing
- Backups e memoria off-site
- Software Escrow Arrangements

- Comunicazioni esterne
- Utilities
- Logistiche e approvvigionamenti
- Notifiche/Testing richiesti

10. Sicurezza delle Operations

- Change Control/Configuration Management
- Dual Control, separazione delle mansioni, rotazione delle mansioni
- Controlli di Information Security
- Analisi della violazione
- Audit delle tracce/Reporting
- Protezione della risorsa
- Amministratore adatto/operatore privilegiato
- Procedure di Recovery
- Metodi di attacco
- Valutazione della vulnerabilità e Pen-Testing

CERTIFICAZIONE

CISSP® (Certified Information Systems Security Professional) Certifications is based on the CBK (Common Body of Knowledge) which comprises ten subject domains that is compiled and maintained through ongoing peer review by subject matter experts. requires exam candidates to have a minimum of five years of relevant work experience in two or more of the ten domains, 5 years of work experience with an applicable college degree, or a credential from the (ISC) 2 -approved list.

CISSP® is a registered trademark of (ISC)²® SU CISSP® classes are not endorsed, sponsored or delivered by (ISC)²®.

Disclaimer

CISSP® a registered trademark of (ISC)²® Inc (International Information Systems Security Certification Consortium) Inc. The materials for the Security University classes have been developed specifically for SU and is not endorsed, sponsored or delivered by (ISC)²®. The goal of the course is to prepare security professionals for the CISSP® exam by covering the ten domains defined by (ISC)²®

INFORMAZIONI

QUOTA DI PARTECIPAZIONE	MODALITÀ D'ISCRIZIONE	CONDIZIONI GENERALI	TUTELA DATI PERSONALI
<p>€ 2000 (+iva)</p> <p>La quota di partecipazione comprende documentazione, colazioni di lavoro e coffee breaks.</p> <p>LUOGO Roma, Visconti Palace Hotel Via Federico Cesi, 37</p> <p>DURATA ED ORARIO 5 giorni: 9.30-13.00 14.00-17.00</p> <p>È previsto il servizio di traduzione simultanea</p>	<p>Il pagamento della quota, IVA inclusa, dovrà essere effettuato tramite bonifico, codice Iban: IT 34 Y 03069 05039 048890270110 Banca Intesa Sanpaolo S.p.A. Ag. 6787 di Roma intestato alla Technology Transfer S.r.l. e la ricevuta di versamento inviata insieme alla scheda di iscrizione a:</p> <p>TECHNOLOGY TRANSFER S.r.l. Piazza Cavour, 3 00193 ROMA (Tel. 06-6832227 Fax 06-6871102)</p> <p>entro il 6 Aprile 2010</p> <p>Vi consigliamo di far precedere la scheda d'iscrizione da una prenotazione telefonica.</p>	<p>In caso di rinuncia con preavviso inferiore a 15 giorni verrà addebitato il 50% della quota di partecipazione, in caso di rinuncia con preavviso inferiore ad una settimana verrà addebitata l'intera quota. In caso di cancellazione del seminario, per qualsiasi causa, la responsabilità della Technology Transfer si intende limitata al rimborso delle quote di iscrizione già pervenute.</p> <p>SCONTI DI GRUPPO</p> <p>Se un'azienda iscrive allo stesso evento 5 partecipanti, pagherà solo 4 partecipazioni. Chi usufruisce di questa agevolazione non ha diritto ad altri sconti per lo stesso evento.</p> <p>ISCRIZIONI IN ANTICIPO</p> <p>I partecipanti che si iscriveranno al seminario 30 giorni prima avranno uno sconto del 5%.</p>	<p>Ai sensi dell'art. 13 della legge n. 196/2003, il partecipante è informato che i suoi dati personali acquisiti tramite la scheda di partecipazione al seminario saranno trattati da Technology Transfer anche con l'ausilio di mezzi elettronici, con finalità riguardanti l'esecuzione degli obblighi derivati dalla Sua partecipazione al seminario, per finalità statistiche e per l'invio di materiale promozionale dell'attività di Technology Transfer. Il conferimento dei dati è facoltativo ma necessario per la partecipazione al seminario. Il titolare del trattamento dei dati è Technology Transfer, Piazza Cavour, 3 - 00193 Roma, nei cui confronti il partecipante può esercitare i diritti di cui all'art. 13 della legge n. 196/2003.</p>

CLEMENT DUPUIS CISSP® Corso e Workshop di preparazione all'esame di Certificazione

Roma 19-23 Aprile 2010
Visconti Palace Hotel
Via Federico Cesi, 37

Quota di iscrizione:
€ 2000 (+iva)

In caso di rinuncia o di cancellazione dei seminari valgono le condizioni generali riportate sopra.

È previsto il servizio di traduzione simultanea

nome

cognome

funzione aziendale

azienda

partita iva

codice fiscale

indirizzo

città

cap

provincia

telefono

fax

e-mail



Timbro e firma

Da restituire compilato a:
Technology Transfer S.r.l.
Piazza Cavour, 3 - 00193 Roma
Tel. 06-6832227 - Fax 06-6871102
info@technologytransfer.it
www.technologytransfer.it

DOCENTE

Clement Dupuis è Senior Security Evangelist e Security Curriculum Manager alla Security University e Creatore del sito di CISSP Open Study Guides: www.cccure.org. Per 20 anni è stato Communication e IT Security specialist nel DND (Department of National Defense) canadese. Agli inizi degli anni '90 ha supportato le operazioni NATO in Somalia e Ruanda costruendo e supportando complessi sistemi di comunicazione computer/satellite. Ha partecipato attivamente allo sviluppo della prima versione del materiale dei corsi CISSP e GSEC per il SANS Institute. È uno degli istruttori più popolari e più richiesti che ottiene sempre alle Conferenze il più alto gradimento da parte dei partecipanti. Costruisce un bel rapporto con i suoi studenti ed è sempre disposto a consigliarli prima, durante e anche dopo il superamento degli esami.