Giorgio Giudice

Certificazioni Professionali in Sicurezza Informatica

002

QUADERNI CLUSIT

CERTIFICAZIONI PROFESSIONALI IN SICUREZZA INFORMATICA

Giorgio Giudice

Comitato Tecnico Scientifico

Associazione italiana per la
Sicurezza Informatica

Quaderni CLUSIT - Gennaio 2005

CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Presentazione

Il settore della sicurezza delle informazioni e delle reti è sicuramente tra i settori che in questi ultimi anni hanno visto crescere a ritmi estremamente elevati il numero dei propri adepti o presunti tali. Considerato l'elevato livello di preparazione che le diverse professioni del settore richiedono non è quindi difficile presagire che nel settore della sicurezza, come in ogni settore delle attività umane, accanto a professionisti con esperienze e background di notevole spessore operano molti incompetenti, che comunque di fatto contribuiscono a sovraffollare un mercato abbastanza esiguo come quello delle sicurezza informatica nazionale, competendo di fatto con professionisti che da diversi anni operano nel settore.

Il problema diventa ancora più serio se si considera il fatto che l'utenza finale è nella stragrande maggioranza dei casi assolutamente impreparata nei confronti della disciplina. Distinguere a "prima vista" un serio professionista della sicurezza da un "fanfarone" non è affatto semplice se non si possiedono esperienza e conoscenze specifiche. Inoltre, contrariamente a quanto succede nella maggior parte dei casi, in cui con l'andar del tempo eventuali carenze di un lavoro consulenziale emergono, nel caso della sicurezza ICT questa evenienza può non verificarsi mai. Ecco perché anche per i professionisti del settore è diventato sempre più difficile riuscire a far riconoscere la propria professionalità, e sovente si trovano spiazzati di fronte all'ultimo arrivato. Per porre fine a questa situazione, un crescente numero di professionisti della sicurezza ha deciso di rifarsi al meccanismo delle certificazioni professionali. Questo fenomeno avviatosi nei paesi anglosassoni già da diversi anni, sta ora assumendo dimensioni di rilievo anche nel nostro paese, dove è in continuo aumento il numero di persone che decidono di ottenere il "bollino blu" nell'ambito della sicurezza informatica.

Il meccanismo delle certificazioni professionali è finalizzato ad attestare il possesso, da parte di una persona, di un certo bagaglio di conoscenze e competenze in uno specifico settore, nonché il rispetto di un codice deontologico; queste competenze sono accertate attraverso esami di vario tipo e natura. Tutto questo ovviamente non basta a qualificare un serio professionista ma costituisce sicuramente un valido biglietto da visita.

Ovviamente anche nell'ambito della sicurezza ICT sono state proposte ed operano sul mercato alcune certificazioni focalizzate sulle diverse professionalità che caratterizzano il settore. A dire il vero, l'universo delle certificazioni di sicurezza è decisamente affollato e l'offerta è talmente abbondante che per un neofita che volesse procedere per questa strada, la scelta del percorso di certificazione da intraprendere richiederebbe uno sforzo non trascurabile, ai fini di individuare quella più adeguata alle proprie aspettative. Diverse sono infatti le opzioni in cui districarsi. Ad esempio è meglio una certificazione neutrale e vendor oriented? Oppure, è più valida una certificazione open source o proprietaria? E poi ancora, scelgo una certificazione general purpose o una specialistica?

Ci è quindi parso estremamente doveroso, in qualità di associazione che tra i suoi scopi statutari annovera la promozione di una cultura della sicurezza, adoperarci affinché l'accesso a questa cultura fosse il più facile possibile. In particolare, abbiamo deciso di condividere con tutti i nostri soci uno studio del settore delle certificazioni professionali, che come CLUSIT abbiamo intrapreso negli anni addietro, ai fini di individuare i principali attori che a livello internazionale si occupavano del tema. A questo proposito, abbiamo incaricato Giorgio Giudice, che del suddetto studio è stato oltre che l'ideatore l'artefice, a predisporre il presente contributo, riassumendo nello stesso le principali risultanze dello studio in quesitone. Ne è risultato un volume molto corposo ma al tempo stesso molto completo. In questo volume sono

descritte le principali certificazioni di sicurezza presenti nel panorama internazionale e di ogni certificazione sono forniti nel dettaglio scopi, contenuti e modalità d'esame. Grazie a questo manuale, chiunque voglia intraprendere un percorso di certificazione, potrà individuare con estrema facilità quello che meglio si addice alle sue aspettative e, non meno importante, valutare tempi e costi dell'intero processo. Nell'ambito di questo processo di decisione non va poi scordato il CLUSIT, che attraverso tutti i suoi soci può fornire ulteriori approfondimenti e testimonianze rispetto alla stragrande maggioranza dei percorsi di certificazione qui descritti.

In conclusione, ci troviamo di fronte ad un testo che credo unico nel panorama internazionale, un testo obbligatorio per chiunque intenda intraprendere un percorso di certificazione nel settore della sicurezza, ed un testo molto utile per chi volesse cogliere le diverse sfaccettature che caratterizzano in termini di contenuti e competenze, le diverse professionalità del pianeta sicurezza delle informazioni e delle reti.

Prof. Danilo Bruschi

Presidente del
Comitato Tecnico-Scientifico Clusit

Abstract

Questa ricerca si propone di presentare un quadro generale delle certificazioni professionali nell'ambito della sicurezza informatica.

Nella prima sezione si cercano di individuare le motivazioni della diffusione in atto di queste certificazioni, e di illustrare quali possono essere i criteri di scelta. Seguono, in due sezioni distinte, le descrizioni delle certificazioni rilasciate da organizzazioni indipendenti e quelle rilasciate dai produttori per certificare il personale qualificato sui propri prodotti.

Per ciascuna certificazione si illustra il percorso formativo, si identificano i prerequisiti necessari sia in termini di conoscenze, che di esperienza già maturata e si precisano le modalità di svolgimento degli esami.

Con questa ricerca si è voluto aiutare le aziende, che hanno necessità di identificare con precisione le qualifiche del proprio personale e dei consulenti esterni.

Si è voluto altresì dare uno strumento al personale ed agli operatori del settore IT, per facilitarli nella scelta di percorsi formativi e di certificazione, che consentano anche di ottenere un adeguato riconoscimento delle proprie competenze.

L'autore

Giorgio Giudice

Socio fondatore del Clusit, partecipa attivamente a tutte le attività dell'associazione, oltre a svolgere attività di consulenza. Segue in prima persona i rapporti tra Clusit e (ISC)², coordinando le attività di formazione; è inoltre attivo nel gruppo di lavoro EUCIP che si occupa del profilo di certificazione IT Administrator. Certificato CISM, socio ISACA/AIEA, socio AICA.

INDICE

SEZIONE I
PREMESSA

Perché le Certificazioni Professionali

Negli Stati Uniti ed in generale nei paesi di cultura statunitense il valore di una laurea dipende fortemente dal nome dell'Università: infatti i programmi e la metrica di valutazione sono lasciati, secondo un principio più liberista, alle scelte di ciascun istituto. Nel nostro sistema, più rigido e quindi omogeneo viene riconosciuto alla laurea un valore più istituzionale e meglio definito. La necessità di certificare competenze professionali è nata quindi in Nordamerica, a garanzia di un riconoscimento di competenze e di esperienza più uniforme e riconducibile a standard di valutazione riconosciuti.

Sta crescendo anche nel nostro continente questa necessità, spinta soprattutto dal mercato del lavoro. La velocità di crescita e la richiesta di aggiornamento continuo, specialmente nel mondo dell'Information Technology ed ancor di più in quello della ICT Security, sono fattori che rafforzano il bisogno di certificare le proprie conoscenze e capacità professionali.

Il sistema Universitario ha il compito di dare e garantire la conoscenza delle basi della materia, lasciando ad altri strumenti il compito di aggiornare e di garantire le competenze.

E' in questo scenario che, andando oltre alla formazione e certificazioni già proposte dalle aziende per i propri prodotti, stanno crescendo organizzazioni per la definizione di specifiche professionalità, curandone la preparazione e definendone programmi di certificazione.

Gli elementi che danno valore ad una certificazione sono essenzialmente:

- l'adeguatezza continua dei contenuti alle reali necessità del mercato
- l'autorevolezza e la serietà nella valutazione e nel rilascio della certificazione
- il riconoscimento internazionale della certificazione

Analizzando il valore di una certificazione professionale è necessario considerare che un percorso di formazione, se finalizzato principalmente all'ottenimento della certificazione, non può essere sostitutivo di esperienza e approfondimento delle conoscenze maturati nella pratica, ma deve essere un complemento ed un ampliamento a tutti gli aspetti della security.

E' inoltre da considerare che la valenza di un riconoscimento internazionale diventa indispensabile nel contesto globale delle attuali realtà operative, che non vedono limiti geografici. Nel contempo devono essere considerate le necessità di integrazione con approfondimenti di conoscenze, in particolare sui temi legali, localizzati nella realtà nazionale. In alcuni programmi di certificazione vengono prese in considerazione le questioni legali: ad esempio chi come $(ISC)^2$ tratta solo i concetti generali validi nella maggior parte dei paesi, chi come EUCIP fa esplicitamente riferimento alle normative europee; altri, di impronta statunitense, se affrontano le questioni legali fanno riferimento esplicitamente alla normativa USA.

Le necessità del mercato del lavoro

E' il mercato a richiedere le Certificazioni Professionali: da parte dell'offerta, rappresentata da personale che deve far riconoscere le proprie qualifiche, e da parte della domanda, rappresentata dalle organizzazioni che devono poter riconoscere il personale qualificato.

Perché una Certificazione in Sicurezza Informatica è vantaggiosa a livello individuale.

Molte Aziende leader richiedono una certificazione in Sicurezza per le posizioni di maggiore responsabilità.

Una certificazione dà una accelerazione alla propria carriera e conferma la credibilità come professionista di Security. Tra i molti benefici di una certificazione soprattutto troviamo:

- Il riconoscimento delle capacità richieste dal mercato
- La prova della conoscenza delle best practices in Security
- Una maggior conoscenza per una maggiore soddisfazione professionale
- Una spinta alla propria carriera, che conduce alle posizioni più elevate in materia di Security
- Una forte credenziale che rende la professionalità individuale più "vendibile"

Perché una Certificazione in Sicurezza Informatica è vantaggiosa a livello aziendale.

Né le tecnologie, né le policies da sole offrono una effettiva protezione contro i furti e la perdita dei dati e delle informazioni. La maggiore difesa da questi pericoli è la conoscenza. Le aziende assumendo o formando personale traggono dalle certificazioni molti benefici:

- Efficienza nel recruiting, nel training e nell'avanzamento di carriera dei dipendenti
- Incremento della produttività posizionando personale al livello appropriato in funzione della esperienza maturata
- Incremento della soddisfazione nello svolgimento dei propri compiti e conseguente diminuzione del turnover
- Fiducia che la Security sia mantenuta da professionisti qualificati
- Creazione di processi di Security conformi alle Best Practices, uniformi e congrui tra loro
- Miglioramenti dell'operatività e maggiore efficienza organizzativa
- Aumento delle vendite grazie alla maggiore fiducia dei clienti ed alla maggiore qualità del servizio.

Queste parole di Ben Smith, Senior Security Strategist di Microsoft, riassumono alcune delle principali motivazioni che portano un numero sempre maggiore di persone a certificarsi in Security.

"Organizations need a metric to prove their own trustworthiness to customers and the general public. If a CIO says we've trained and certified 90 percent of our staff in security, that's a very powerful message for the board and for the customers."

Gli schemi di certificazione

ISO/IEC 17024:2003, Conformity assessment - General requirements for bodies operating certification of persons - è uno standard internazionale che definisce i criteri per i gli organismi di certificazione del personale.

La ISO/IEC 17024 fornisce un insieme organico di linee guida per le organizzazioni che si occupano di qualificazione e certificazione del personale, incluse le procedure per l'elaborazione e il mantenimento di uno schema di certificazione. La norma intende aiutare gli organismi che certificano il personale a condurre valutazioni oggettive ed imparziali, così da ridurre qualsiasi rischio di conflitto di interessi.

La nuova norma internazionale effettua un benchmarking tra i diversi schemi di certificazione, in modo da garantirne un funzionamento coerente e comparabile, agevolando in questo modo il mutuo riconoscimento degli schemi e quindi la mobilità del personale. Va sottolineato che oggi sono migliaia gli schemi di certificazione per il personale, applicabili praticamente a tutte le professioni, sia in ambito industriale che dei servizi.

Uno schema di certificazione altro non è che la valutazione - effettuata dall'Organismo di certificazione competente - della formazione, dell'esperienza, delle competenze e abilità applicabili allo specifico settore in relazione al quale la certificazione viene concessa.

La nuova norma è frutto dei lavori del CASCO, ossia il Comitato ISO che si occupa della valutazione di conformità, ed in particolare del gruppo di lavoro 17, specificamente competente sulla certificazione del personale; ai lavori ha partecipato anche l'IEC (International Electrotechnical Commission).

Certificazioni "Vendor Neutral" e Certificazioni "Vendor Specific"

Le prime nascono dalla necessità di qualificare le conoscenze, le competenze e/o l'esperienza relativa ad argomenti o domini di conoscenza. Si caratterizzano e si contraddistinguono principalmente per la specificità dei contenuti e per il livello di riconoscimento che riescono a vedersi attribuito. Non si pongono in alternativa alle seconde, ma come complementari, coprendo una area di competenze e conoscenze a più ampio raggio.

Nella maggior parte dei casi richiedono l'adesione ad un Codice Etico. Prevedono un aggiornamento periodico, principalmente attraverso programmi di formazione continua.

Le certificazioni "Vendor Specific" nascono dalla necessità di qualificare personale in grado di operare su prodotti e sistemi hardware e/o software specifici. I programmi di certificazione dei "Vendors" sono complementari ai prodotti a cui si riferiscono e come tali devono seguirne l'evoluzione e l'aggiornamento. Recentemente alcuni percorsi di certificazione "Vendor Specific" richiedono l'affiancamento di una certificazione "Vendor Neutral".

Il codice etico e le certificazioni professionali ICT Security

Non c'è dubbio che siamo in un periodo sociale di cambiamento, ancor più in un contesto dove l'utilizzo delle tecnologie legate al trattamento, alla diffusione e alla disponibilità delle informazioni, può determinare decisioni rapide e cambiamenti di potere.

La società, le aziende e le istituzioni per gestire queste tecnologie necessitano di strutture, di attrezzature ma soprattutto di persone con competenze: è indiscussa la necessità di formazione di persone e si parla di formazione continua, si parla di aggiornamento, si parla di reinventare dei profili professionali adatti ai nuovi scenari.

Riflettendo sulle necessità di formazione, ci accorgiamo che la società, le aziende, le istituzioni cercano non solo persone capaci e competenti ma soprattutto persone responsabili.

I sistemi organizzativi si sono trasformati negli ultimi anni distribuendo responsabilità tra tutti i livelli gerarchici di una organizzazione:

- i sistemi di qualità (ISO9000)
- la sicurezza delle persone (Legge 626/94)
- la protezione dei dati personali (D.L. 196/03)
- la gestione della sicurezza delle informazioni (ISO 17799)

si basano sull'assegnazione di responsabilità.

Le persone sono il centro dei meccanismi organizzativi, sono i nodi di una rete di relazioni e di attività.

Ecco perché oltre alle competenze sono necessarie conoscenze dei principi che devono motivare le scelte, i comportamenti, le decisioni.

Ciò che contraddistingue certe professioni "elette" come il magistrato, il notaio, il medico, per citarne solo alcune, è il loro impegno a seguire principi etici e deontologici che sono stati dichiarati e che sono la base della fiducia che riscuotono.

In ogni schema di certificazione professionale è sempre importante la definizione di uno specifico codice etico e deontologico costituito da regole.

Se vogliamo dare riconoscimento e valore alle certificazioni dobbiamo delineare i contenuti di specifici codici etici e deontologici e definire meccanismi che provvedano alla verifica dell'adeguatezza a questi codici. Le organizzazioni accreditate al rilascio delle certificazioni dovranno garantire oltre le competenze e le capacità anche il mantenimento di quelle "regole" contenute nei codici etici e deontologici.

Valutando il valore di una certificazione, dobbiamo quindi focalizzare la nostra attenzione anche alla attenzione posta alla questione etica.

Per completezza sono riportati nell'**APPENDICE A** i codici etici che fanno riferimento ad alcune certificazioni Vendor Neutral.

Disclaimer

Nelle pagine che seguono, sono presentate solo alcune certificazioni in materia di sicurezza informatica: non si sono volute elencare tutte le certificazioni esistenti, ma sono state prese in considerazione solo quelle che l'autore ha ritenuto più esemplificative; si è cercato di fornire un'informazione aggiornata e precisa, ma non si può garantire che le stesse siano necessariamente esaurienti, complete, precise o aggiornate; il contenuto è talvolta riferito ad informazioni reperite sulla Rete e sia l'autore che Clusit - Associazione Italiana per la Sicurezza Informatica non assumono alcuna responsabilità.

SEZIONE II
CERTIFICAZIONI "VENDORS NEUTRAL"

$(ISC)^2$ = INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATIONS CONSORTIUM, INC.

$(ISC)^2$ è una organizzazione not-for-profit organizzata per offrire i propri seminari ed esami di certificazione a livello internazionale, costituita nel 1989, che ha i seguenti scopi:

- Il mantenimento ed l'aggiornamento del "Common Body of Knowledge" [CBK] che è l'insieme e l'aggregato di tutte le conoscenze e le best practices di sicurezza informatica, raccolte a livello internazionale, di rilevanza per i professionisti dell'Information Security.
- La certificazione di professionisti della sicurezza informatica secondo standard internazionali.
- La gestione del training e degli esami di certificazione.
- La garanzia del mantenimento delle credenziali di certificazione attraverso un aggiornamento continuo.

$(ISC)^2$ ha sedi negli Stati Uniti e uffici locali a Londra e Hong Kong.

L'organizzazione è condotta da un Board of Directors eletto periodicamente dai soggetti certificati.

CLUSIT è dal 2003 **Education Affiliate** $(ISC)^2$ per l'Italia e il Canton Ticino.

Sono migliaia i professionisti certificati in una delle due designazioni amministrate da $(ISC)^2$:

- **Certified Information Systems Security Professional [CISSP]**
- **System Security Certified Practitioner [SSCP]**

A fine dicembre 2004 si contavano oltre 30.000 certificati CISSP in 107 paesi nel mondo, quasi 3000 in Europa di cui 102 in Italia: è rilevante la crescita, soprattutto nel nostro paese, se si considera che in meno di un anno il numero dei certificati è quasi raddoppiato.

	Cerificati CISSP al 31/01/2004	Cerificati CISSP al 31/12/2004	Incremento nell'ultimo anno
Mondo	24.254	30.149	24%
Europa	2.022	2.991	48%
Italia	53	102	92%

Certificazione CISSP

Certified Information Systems Security Professional

Definizione

Questa certificazione è prevista per professionisti esperti che siano responsabili per lo sviluppo di policy di sicurezza, standard e procedure a la gestione e conduzione della loro implementazione nell'ambito di una organizzazione.

$(ISC)^2$, nell'ambito della certificazione CISSP, è stata accreditata conforme allo standard internazionale ISO/IEC 17024 che definisce i criteri per i gli organismi di certificazione del personale

La certificazione CISSP è focalizzata su un Common Body of Knowlege (CBK) basato sui seguenti 10 domini:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security

Percorso di certificazione

Per diventare CISSP si deve innanzitutto sottoscrivere il codice etico $(ISC)^2$, quindi si devono completare due processi: l'**Esame** e la **Certificazione**.

Esame

I prerequisiti richiesti per presentarsi all'esame CISSP (indipendenti da quelli richiesti per essere certificati) sono:

- Aver versato la tassa d'esame.

- Dichiarare di possedere un minimo di quattro anni di esperienza professionale nel campo della Sicurezza Informatica (o tre in caso di Diploma di Laurea) , in almeno uno dei 10 domini previsti nel CBK.
- Completare il Candidate Agreement, attestando le proprie asserzioni relativamente all'esperienza professionale e dichiarando il proprio impegno di adesione al Codice Etico $(ISC)^2$.
- Rispondere conformemente a domande relative alla proprio stato giudiziario ed al relativo background.

L'esame CISSP consiste in 250 domande a scelta multipla in lingua Inglese e i candidati hanno 6 ore per completare l'esame. Per passare l'esame è necessario raggiungere un punteggio di 700/1000.

Certificazione

Una volta superato l'esame il candidato deve:

- Presentare adeguatamente completato e sottoscritto l'Endorsement Form.
- Se al candidato viene richiesto di sottoporsi ad un audit, deve passare la verifica delle dichiarazione effettuate.

Endorsement: Una volta che al candidato sia stato notificato il superamento dell'esame, gli sarà richiesto di produrre l'Endorsement Form sottoscritto a titolo di referenza da persona certificata CISSP. In alternativa l'Endorsement Form potrà essere sottoscritto da persona professionalmente qualificata in Sicurezza Informatica o da un funzionario dell'organizzazione di cui fa parte il candidato, che attesti l'esperienza professionale.

Il sottoscrittore dell'Endorsement Form attesterà che, per quanto di sua conoscenza, le asserzioni del candidato relativamente alla propria esperienza siano vere e che egli goda di una buona reputazione nell'industria della Sicurezza Informatica.

Audit: Una percentuale dei candidati che hanno passato l'esame CISSP e presentato la referenza sarà casualmente sottoposta ad un audit, richiedendo di sottoporre un curriculum per una verifica formale ed indagine riguardo alle esperienze professionali dichiarate.

Mantenimento della certificazione CISSP

La certificazione ha una durata di 3 anni. Per ottenere la conferma per ulteriori 3 anni (recertification) bisogna aver maturato 120 unità CPE (Continuing Professional Education).

E' inoltre richiesta una quota di mantenimento annuale, attualmente fissata in $85.

Seminari di preparazione all'esame CISSP

Sono previsti seminari "CBK REVIEW" di preparazione alla certificazione CISSP erogati direttamente da $(ISC)^2$ della durata di 5 giornate intensive. Sono in lingua Inglese e sviluppano in profondità tutti i 10 domini oggetto della certificazione.

Certificazione SSCP

System Security Certified Practitioner Certification

Definizione

Questa certificazione è prevista per professionisti esperti che siano responsabili dell'amministrazione di reti e di sistemi di sicurezza.

La certificazione SSCP è focalizzata su un Common Body of Knowlege (CBK) basato sui seguenti 7 domini:

- Access Controls
- Administration
- Audit and Monitoring
- Risk, Response and Recovery
- Cryptography
- Data Communications
- Malicious Code/Malware

Percorso di certificazione

Per diventare SSCP è necessario possedere i prerequisiti e superare l'esame.

I prerequisiti richiesti per presentarsi all'esame SSCP sono:

- Aver versato la tassa d'esame.
- Dichiarare di possedere un minimo di un anno di esperienza professionale nel campo della Sicurezza Informatica, in almeno uno dei 7 domini previsti nel CBK.
- Completare il Candidate Agreement, attestando le proprie asserzioni relativamente all'esperienza professionale e dichiarando il proprio impegno di adesione al Codice Etico $(ISC)^2$.
- Rispondere conformemente a domande relative alla proprio stato giudiziario ed al relativo background.

L'esame SSCP consiste in 125 domande a scelta multipla in lingua Inglese e i candidati hanno 3 ore per completare l'esame. Per passare l'esame è necessario raggiungere un punteggio di 700/1000.

Mantenimento della certificazione SSCP

La certificazione ha una durata di 3 anni. Per ottenere la conferma per ulteriori 3 anni (recertification) bisogna aver maturato 60 unità CPE (Continuing Professional Education).

E' inoltre richiesta una quota di mantenimento annuale, attualmente fissata in $65.

ISACA
INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

L' *ISACA* e' stata fondata nel 1969 per incrementare la formazione, la comunicazione, lo sviluppo professionale e le opportunità di ricerca nei campi correlati all'auditing ed ai Sistemi Informativi.

Come contributo nel proseguimento di questi obiettivi, fu costituita nel 1976 l'*Information Systems Audit and Centrol Foundation* (ISACF attualmente denominata ITGI - IT Governance Institute), società senza fini di lucro e dedicata al perfezionamento della formazione, della comunicazione, dello sviluppo professionale, degli standard e delle ricerche nel campo dell'Auditing dei Sistemi Informativi.

Durante la sesta Conferenza Annuale Internazionale della ISACA avvenuta il 21 giugno 1978, la ISACF annunciò ufficialmente un programma per la certificazione.

Gli obiettivi formali del programma erano:

- sviluppare e mantenere una procedura d'esame che potesse essere usata per valutare la competenza di persone nell'effettuare gli Audit di Sistemi Informativi;
- fornire un meccanismo per motivare gli Auditor di sistemi informativi a mantenere la loro competenza e supervisionare i programmi di mantenimento;
- aiutare l'Alta Direzione nello sviluppare una armonica funzione di Audit dei Sistemi Informativi fornendo criteri per la selezione e lo sviluppo del personale.

Inizialmente la certificazione fu attribuita in base alla clausola dell'esperienza professionale (PEP). Per la qualificazione relativo alla PEP fu richiesto un minimo di 5 anni di esperienza o equivalente nel campo dell'Auditing, dei Sistemi Informativi o dell'Auditing di sistemi informativi. Fu costituito un comitato di Certificazione per valutare le domande.

Le certificazioni in ambito PEP ufficialmente terminarono il 30 giugno 1979. Fu stabilito che tutte le successive certificazioni sarebbero state attribuite solo in base al superamento di un Esame di ampia e sostanziale significatività e di un periodo minimo di qualificante esperienza di lavoro.

La certificazione CISA (Certified Information Systems Auditor) è riconosciuta a livello mondiale e conta quasi 26.000 professionisti, di cui 190 in Italia,.

Nel 2002 è stato definito un altro programma di certificazione: CISM (Certified Information Security Manager), con uno schema di certificazione analogo a quello CISA, ma orientato all'Information Security Management. Ad ora sono 5.150 i professionisti certificati, di cui 75 in Italia.

ISACA è presente a livello mondiale anche grazie ai propri "chapters" in più di 60 paesi, che provvedono alla formazione ed alla organizzazione degli esami di certificazione.

I professionisti certificati CISA e CISM sono presenti in oltre 100 paesi nel mondo.

Certificazione CISA

Certified Information Systems Auditor

Definizione

Questa certificazione è prevista per professionisti nelle aree dell'IS auditing, del controllo e della sicurezza. La certificazione CISA ha per oggetto le seguenti aree:

1. **Management, Planning, and Organization of IS**
   Valutazione della strategia, delle normative, degli standard, delle procedure e delle prassi in relazione alla gestione, alla pianificazione e all'organizzazione dei SI.
2. **Technical Infrastructure and Operational Practices**
   Valutazione dell'efficacia e dell'efficienza nella realizzazione e gestione delle infrastrutture tecniche ed operative del sistema informatico aziendale, per assicurare che esso supporti adeguatamente gli obiettivi commerciali aziendali.
3. **Protection of Information Assets**
   Valutazione della sicurezza logica, ambientale e infrastrutturale IT per assicurarsi che soddisfi i requisiti commerciali dell'azienda per la tutela del patrimonio dati contro utilizzi, divulgazione o modifiche non autorizzati e per evitare rischi di danneggiamento o di perdita degli stessi.
4. **Disaster Recovery and Business Continuity**
   Valutazione del processo volto allo sviluppo e al mantenimento di piani documentati, comunicati e testati, a garanzia della continuità operativa e informatica dell'azienda in caso di calamità o interruzioni straordinarie.
5. **Business Application System Development, Acquisition, Implementation, and Maintenance**
   Valutazione delle metodologie e dei procedimenti applicati per lo sviluppo, l'acquisizione, l'attuazione e l'aggiornamento dei sistemi applicativi aziendali al fine di assicurarne la coerenza con gli obiettivi commerciali dell'azienda.
6. **Business Process Evaluation and Risk Management**
   Valutazione dei sistemi e dei processi commerciali al fine di assicurare che i rischi vengano gestiti in conformità con gli obiettivi commerciali dell'azienda.
7. **The IS Audit Process**
   Svolgere le attività di revisione SI in conformità agli standard e ai principi di verifica SI professionalmente in uso per assicurarsi che i sistemi informatici e amministrativi siano adeguatamente controllati, monitorati e vagliati.

Percorso di certificazione

Il processo di certificazione prevede:

- Il superamento dell'esame costituito da 200 domande chiuse, con uno score di almeno 75/100. E' possibile sostenere l'esame anche in lingua Italiana.
- Comprovare un'esperienza professionale di almeno 5 anni nel campo della revisione, del controllo e della sicurezza dei sistemi informativi.
- Aderire al codice etico professionale ISACA
- Seguire i programmi di sviluppo professionale continuo (CPE - Continuing Professional Education)

Seminari di preparazione all'esame CISA

E' previsto un corso di preparazione all'esame strutturato in 5 incontri di 2 giornate, distribuiti nei mesi precedenti l'esame. E' prevista una sola sessione di esame all'anno in contemporanea a livello mondiale e in contemporanea per entrambe le certificazioni CISA e CISM.

Mantenimento della certificazione CISA

La certificazione ha una durata di 3 anni. Per ottenere la conferma per ulteriori 3 anni (recertification) bisogna aver maturato 60 unità CPE (Continuing Professional Education).

E' inoltre richiesta una quota di mantenimento annuale, attualmente fissata in $40.

Certificazione CISM

Certified Information Security Manager

Definizione

Questa certificazione è prevista per i Security Manager e in particolare quei professionisti senior che gestiscono la sicurezza delle informazioni aziendali e possiedono le conoscenze e le esperienze per definire e implementare strategie, processi e strutture atti a gestire i rischi in stretta relazione alle strategie aziendali.

La certificazione CISM ha per oggetto le seguenti aree:

1. **Information Security Governance**
   Si concentra sul framework che garantisce che le strategie di information security siano in linea con gli obiettivi di business e coerenti con le normative generali e gli standard di settore.
2. **Risk Management**
   Riguarda l'identificazione e la gestione dei rischi dell' information security al fine di garantire gli obiettivi di business.
3. **Information Security Program(me) Management**
   Si occupa del disegno, sviluppo e gestione dei programmi di information security al fine di implementare il framework dell'information security governance.
4. **Information Security Management**
   Riguarda le attività di sicurezza per rendere esecutivo il programma di information security.
5. **Response Management**
   Sviluppo e gestione delle capacità di rispondere ad eventi distruttivi per la sicurezza informatica in termini di ripristino e recovery.

Percorso di certificazione

Il processo di certificazione prevede:

- Il superamento dell'esame costituito da 200 domande chiuse, con uno score di almeno 75/100.
- Comprovare un'esperienza professionale di almeno 5 anni, di cui tre di Management in almeno tre delle aree di competenza. (Fino ad un massimo di due anni possono essere sostituiti da altri titoli come ad es. la certificazione CISA o CISSP)
- Aderire al codice di etica professionale ISACA

- Seguire i programmi di sviluppo professionale continuo (CPE - Continuing Professional Education)

Seminari di preparazione all'esame CISM

E' previsto un corso di preparazione all'esame strutturato in 3 incontri di 2 giornate, distribuiti nei mesi precedenti l'esame. E' prevista una sola sessione di esame all'anno in contemporanea a livello mondiale e in contemporanea per entrambe le certificazioni CISA e CISM.

Mantenimento della certificazione CISM

La certificazione ha una durata di 3 anni. Per ottenere la conferma per ulteriori 3 anni (recertification) bisogna aver maturato 60 unità CPE (Continuing Professional Education).

E' inoltre richiesta una quota di mantenimento annuale, attualmente fissata in $40.

SANS INSTITUTE

Il SANS Institute (System Administration, Networking, and Security) è una organizzazione fondata nel 1989 negli Stati Uniti, con l'obbiettivo di fare formazione ed organizzare programmi di training sulla Sicurezza Informatica. Dal 2000 è stato costituito il programma di certificazioni GIAC Global Information Assurance Certification.

Per quasi tutte le Certificazioni vengono proposti seminari di 6 giorni consecutivi in occasione di conferenze organizzate sia negli USA che in altre città d'Europa, Asia, Australia.

Il costo di ciascun esame da sostenere in seguito a training online o in seguito alla partecipazione al seminario è di $250; è anche possibile sostenere l'esame preparandosi individualmente a un costo di $450.

Per fare un esempio, la certificazione GSEC, il cui seminario di preparazione è disponibile sia online che in occasione delle Conferenze organizzate in Europa, consiste in:

- Dimostrare di avere le conoscenze essenziali e le capacità necessarie per ricoprire un ruolo di responsabilità di sicurezza all'interno di una organizzazione.
- Completare un esercizio pratico scritto e sostenere 2 esami di 3 ore ciascuno.
- Il superamento dell'esercizio permettere di accedere agli esami, che si sostengono online sul sito web GIAC.
- Ogni esame è costituito da 100 domande a cui rispondere in 3 ore; per il superamento ed ottenere la certificazione è necessario rispondere correttamente ad almeno 70 domande.

Di seguito sono riportate le certificazioni GIAC disponibili: alla certificazione GSEC indicata per prima, seguono 5 certificazioni più specifiche GCFW, GCIA, GCIH, GCWN e GCUX che rappresentano il percorso necessario alla certificazione più avanzata GIAC Security Expert (GSE); un cenno particolare sulla certificazione GIAC Information Security Fundamentals (GISF), che parte dai concetti elementari della security ed è orientata a principianti che non hanno ancora avuto a che fare con la security, richiede un seminario di 6 giorni. Le ultime certificazioni riportare sono orientate a ruoli più specifici.

GIAC Security Essentials Certification (GSEC)

Livello: Fondamentale

Validità della certificazione: 2 anni

Target: Professionisti di Security che vogliono completare le proprie conoscenze tecniche di security; Amministratori di reti e di sistemi che vogliono capire come si mettono in pratica i concetti di security; managers che vogliono capire la security approfondendone i concetti con terminologia chiara; chiunque, nuovo nella security ma con un certo background in security e networking.

E' disponibile per questa certificazione il training online.

L'ottenimento della certificazione GIAC Security Essentials Certification dimostra di possedere le conoscenze, le qualifiche e le abilità per mettere in pratica i principi della security in ogni organizzazione. I test d'esame per ottenere la certificazione GSEC verificano la qualificazione di personale a cui affidare responsabilità di security.

GIAC Certified Firewall Analyst (GCFW)

Livello: Intermedio

Validità della certificazione: 4 anni

Target: Responsabili della progettazione, implementazione, configurazione e monitoraggio di sistemi di sicurezza come routers, firewalls, VPNs/remote access nell'ambito di un progetto di reti.

Chi è certificato GIAC Certified Firewall Analysts ha le conoscenze, le qualifiche e le abilità per progettare, implementare e monitorare routers, firewalls.

GIAC Certified Intrusion Analyst (GCIA)

Livello: Intermedio

Validità della certificazione: 4 anni

Target: Responsabili del monitoraggio di reti e host, sistemi di analisi del traffico e intrusion detection.

Chi è certificato GIAC Certified Intrusion Analysts ha le conoscenze, le qualifiche e le abilità per configurare e monitorare sistemi di intrusion detection, leggere, interpretare e analizzare il traffico di rete e i relativi files di log.

GIAC Certified Incident Handler (GCIH)

Livello: Intermedio

Validità della certificazione: 2 anni

Target: Responsabili della gestione e azioni agli incidenti; personale a cui è richiesto la conoscenza approfondita dei meccanismi che possono accadere a sistemi e reti e delle contromisure da attuare.

Chi è certificato GIAC Certified Incident Handlers ha le conoscenze, le qualifiche e le abilità per gestire gli incidenti; conoscere gli strumenti e le tecniche di attacco e sapere come intervenire in difesa e in risposta agli attacchi quando necessario.

GIAC Certified Windows Security Administrator (GCWN)

Livello: Intermedio

Validità della certificazione: 2 anni

Target: Responsabili della installazione, configurazione e monitoraggio di sistemi, servizi e reti Windows 2000/XP/2003.

Chi è certificato GIAC Certified Windows System Administrators ha le conoscenze, le qualifiche e le abilità per mantenere sicuri e verificare i sistemi Windows, inclusi i servizi come Internet Information Server e Certificate Services.

GIAC Certified UNIX Security Administrator (GCUX)

Livello: Intermedio

Validità della certificazione: 2 anni

Target: Responsabili della installazione, configurazione e monitoraggio di sistemi, servizi e reti UNIX e/o Linux.

Chi è certificato GIAC Certified UNIX System Administrators ha le conoscenze, le qualifiche e le abilità per mantenere sicuri e verificare i sistemi UNIX e Linux.

GIAC Security Expert (GSE)

Livello: Avanzato

Prerequisiti: Avere conseguito tutte le 5 certificazioni specifiche GCFW, GCIA, GCIH, GCWN, GCUX, avendo almeno in una raggiunto un punteggio del 90% (honors)

Certificazione: L'esame di certificazione si svolge in 4 giorni durante i quali il candidato deve superare: esami con domande a scelta multipla, esercizi hands-on, esercizi scritti, domande con risposte brevi, dimostrare la propria competenza in una breve presentazione orale.

Validità della certificazione: La certificazione GSE non ha scadenza, ma è legata alla validità delle 5 certificazioni specifiche.

GIAC Information Security Fundamentals (GISF)

Livello: Principianti

Validità della certificazione: 2 anni

Target: Questo percorso di certificazione contiene una varietà di argomenti ottimizzati per dare a chi si occupa di Security le basi di tutti gli elementi di conoscenza necessari e la capacità di comunicare adeguatamente con le persone addette su tutti gli argomenti.

Una buona comunicazione sugli argomenti tecnici permette di colmare quelle lacune che spesso esistono tra managers e amministratori di sistemi. Argomenti base sono tra l'altro la conoscenza delle risorse disponibili, delle best practices, della gestione dei rischi.

GIAC Systems and Network Auditor (GSNA)

Livello: Intermedio

Validità della certificazione: 2 anni

Target: Responsabili tecnici addetti alla sicurezza ed alla verifica dei sistemi informativi; auditors che vogliono acquisire le conoscenze tecniche dei sistemi di cui possano essere responsabili.

Chi è certificato GIAC Systems and Network Auditors ha le conoscenze, le qualifiche e le abilità per impiegare le tecniche base di analisi di rischio e condurre audit tecnici essenziali per la gestione della security.

GIAC Certified Forensic Analyst (GCFA)

Livello: Intermedio

Validità della certificazione: 4 anni

Target: Responsabili di computer forensic, investigazione, analisi, gestione avanzata degli incidenti.

Chi è certificato GIAC Certified Forensic Analysts (GCFAs) ha le conoscenze, le qualifiche e le abilità per condurre le attività di gestione degli incidenti anche in scenari allargati e per condurre investigazioni forensi a livello di reti e di hosts.

GIAC IT Security Audit Essentials (GSAE)

Livello: Fondamentale

Validità della certificazione: 2 anni

Target: Personale che si approccia alle security che deve essere coinvolta in attività di auditing, policy organizzative, procedure, analisi dei rischi e conformità delle policy.

Il personale che ha completato il percorso formativo GIAC IT Security and Audit ha una buona conoscenza dei principi di security ed è in grado di condurre audit con l'uso corretto di checklists.

GIAC Certified ISO-17799 Specialist (G7799)

Livello: Fondamentale

Validità della certificazione: 2 anni

Target: Personale che deve assistere una organizzazione nel processo di certificazione secondo lo standard ISO-17799, svilupparne la cultura, trasferendo i principi delle best practices nell'organizzazione stessa.

Chi è certificato GIAC Certified ISO-17799 Specialist è in grado di implementare efficientemente un sistema ISO-17799.

GIAC Security Leadership Certification (GSLC)

Livello: Manageriale

Validità della certificazione: 2 anni

Target: Responsabili a livello manageriale o di supervisione dello staff di security che devono imparare i principi essenziali e raggiungere le abilità richieste per supervisionare un progetto di security.

Chi è certificato GIAC Security Leadership Certificate ha fatto propri tutti i principi essenziali di security. le best practices e le tecnologie.

GIAC Certified Security Consultant (GCSC)

Livello: Intermedio

Validità della certificazione: 4 anni

Target: Responsabili che vogliono assumere il ruolo di interfeccia con i clienti in progetti di security sia con competenze tecniche che commerciali.

Chi è certificato GIAC Certified Security Consultants (GCSCs) ha le conoscenze, le qualifiche e le abilità per gestire progetti ed incarichi di consulenza di security. In particolare è in grado di prendere decisioni relative al business, comprendere l'impatto di norme legislative, pianificare progetti, vendere servizi di sicurezza, valutare e/o creare piani di business continuity, valutare e/o creare security policy.

COMPTIA

Da oltre ventidue anni, CompTIA (Computing Technology Industry Association) si dedica allo sviluppo dell'industria dell'Information Technology (IT) e delle figure professionali che vi operano e conta oltre 19.000 membri in 89 paesi.

I programmi di certificazione CompTIA rappresentano gli standard industriali per le competenze base dell'Information Technology, con il vantaggio di essere "vendor-neutral", ovvero indipendenti dalle case e dai loro prodotti. Molte di queste certificazioni sono peraltro riconosciute dai vendor come prerequisiti o opzionali per le certificazioni proprietarie avanzate, e sono spesso consigliate o obbligatorie per i propri dipendenti o per il personale dei partner (ad esempio nei programmi di IBM, Cisco, Microsoft, Novell, Hewlett-Packard e Symantec).

Un esempio rilevante è la presenza della certificazione CompTIA Security+ nel MOC (Microsoft Official Curriculum).

Certificazione CompTIA Security+

Introdotta nel dicembre 2002 conta approssimativamente 10.000 certificati in tutto il mondo. Considerata come una certificazione "entry level" tra quelle di sicurezza, rappresenta una qualifica preferenziale o un prerequisito per certificazioni di livello avanzato

Le aree di conoscenza o domini sono così distribuiti:

- 30% Concetti di sicurezza in generale
- 20% Sicurezza delle comunicazioni
- 20% Sicurezza delle infrastrutture
- 15% Basi di Crittografia
- 15% Sicurezza organizzativa e operativa

Target: professionisti IT con competenza nel networking e nell'amministrazione di reti TCP/IP in ambienti Windows e familiarità con altri sistemi operativi.

Prerequisiti: Competenze di networking, sistemi operativi e hardware informatico.

Esame:

Numero parti dell'esame: 1

Numero domande 100

Durata dell'esame: 90 minuti

Minimo punteggio per passare l'esame: 764 su una scala da 100 a 900

Costo dell'esame: € 249

Lingua: Inglese

Certificazione: viene spedita per posta entro 4/6 settimane dalla data dell'esame.

OSSTM OPEN SOURCE SECURITY TESTING METHODOLOGY

L'Institute for Security and Open Methodologies (ISECOM) è una comunità open-source operante dal gennaio 2001 come organizzazione non-profit in USA e Spagna.

ISECOM offre le certificazioni e il supporto al training.

Le certificazioni OSSTM sono basate sulla applicazione del OSSTMM - Open Source Security Testing Methodology Manual

Lo scopo del manuale OSSTMM è quello di definire uno standard unico per i test di sicurezza su Internet. Trascurando le scuole di pensiero di molti esperti di test di sicurezza e focalizzando l'interesse sulla metodologia, si è voluto proporre una soluzione ad un problema di attualità.
A prescindere dalla dimensione della società, dal capitale di finanziamento e dal supporto dei fornitori, ogni esperto di sicurezza o di rete che rispetta i requisiti definiti da OSSTMM ha correttamente eseguito un'istantanea dell'infrastruttura del cliente, a garanzia della sicurezza. Questo non vuol dire che non sia possibile eseguire un test più velocemente, più dettagliatamente o con altre valenze. L'esperto che ha seguito la metodologia indicata nel manuale ha seguito il modello standard portandolo a termine.

Certificazione OSSTMM PROFESSIONAL SECURITY TESTER (OPST)

Definizione

La certificazione ISECOM OPST è focalizzata sull'esecuzione di Security Testing, diretti sia verso la parte esterna al perimetro aziendale, sia verso la parte interna: questa metodologia è nel contempo adatta anche all'esecuzione di test di sicurezza dalla rete interna all'area DMZ aziendale e viceversa, prendendo in considerazione le sei diverse aree della Corporate Security proprie dell'OSSTMM, denominate Moduli Operativi.

- Communications Security
- Wireless Security
- Information Security
- Physical Security
- Internet Security
- Process Security

Target:

- Amministratori di Sistema
- Amministratori di Rete
- Responsabili Sicurezza Informatica
- Security Staff di NOC e SOC
- Security Tester
- Security Auditor
- ISO/BSI Lead Auditor
- Security Consultant
- Tutti coloro che lavorano professionalmente nel campo della System & Network Security

Corso di preparazione all'esame OPST

E' previsto un corso di preparazione all'esame di 5 giornate di tipo "intensive", che includono le quattro ore per l'esame finale di certificazione.

Le giornate formative affrontano i seguenti moduli:

- **Business Information Security** è il modulo formativo che riguarda le necessità relative all'attività in materia di test di sicurezza ed ingloba argomenti quali la riservatezza delle informazioni, la valutazione dei rischi, le testing legalities, le etiche professionali, il reporting, il processo di test e le regole d'impiego;

- **Practical Security Testing** è il modulo di formazione tecnica per la definizione dei termini e delle necessità per i test di sicurezza, basato sull'ultima versione dell'OSSTMM per l'esecuzione di assessment e di stime;
- **Aggressive Security Testing** è la technical baseline avanzata per la definizione dei termini e delle necessità per l'esecuzione di un test di sicurezza, completo e **certificato** OSSTMM per quanto concerne le sezioni Information Security ed Internet Security.

Prerequisiti

La certificazione ISECOM OPST richiede i seguenti prerequisiti:

- buona conoscenza della suite TCP/IP e dei suoi principali protocolli;
- esperienza nell'amministrazione base dei sistemi *NIX e Microsoft Windows;
- dimestichezza nell'installazione e nella configurazione di software di verifica ed analisi della sicurezza (specificatamente su distribuzioni *NIX); dei sopraccitati software è richiesta, inoltre, un'esperienza di base nell'utilizzo;
- conoscenza e comprensione delle architetture di rete;
- conoscenza base dei principali servizi TCP/IP (HTTP, FTP, TELNET, SSH) nell'ottica dello svolgimento di analisi di sicurezza;
- conoscenza base dei sistemi per la sicurezza in rete: *router, firewall, intrusion detection system*;
- conoscenza delle dinamiche di attacco a sistemi informativi.
- buona conoscenza della lingua inglese e delle terminologie tecniche;
- conoscenza del Manuale OSSTMM 2.0;
- esperienza lavorativa o di ricerca pari ad almeno un anno nel settore della ICT Security.

Esame

L'esame è basato su 50 domande a risposta multipla e consiste nell'applicazione di quanto appreso durante il corso, acquisendo dei risultati e giungendo a conclusioni e valutazioni, utilizzando la metodologia OSSTMM ed il workbook BSTA. L'esame è suddiviso in tre sezioni principali: Data Test e Log Analysis, Security Testing Projects e Professional Consulting.

Per ottenere la certificazione è necessario passare l'esame con uno score almeno del 60%.

Costi:

Corso di 5 gg.: € 3.000,00

Esame: € 450,00

Certificazione OSSTMM PROFESSIONAL SECURITY ANALYST (OPSA)

Definizione

La certificazione ISECOM OPSA è focalizzata sulla comprensione dei risultati dei test, sulle loro procedure di esecuzione, sul loro significato, puntando principalmente al processo che porta un team al raggiungimento dei risultati dei test ed alla loro elaborazione.

Target:

- Responsabili Sicurezza Informatica
- Responsabili Privacy, DLG 196/03, Qualità e Certificazione aziendale
- Consulenti esterni e team interni di Risk Analysis e Gestione del Rischio
- Security Auditor, ISO/BSI Lead Auditor
- Senior Security Tester, Senior Security Consultant
- Security Staff di NOC e SOC
- System, Network & Security Technical Administrator
- Tutti coloro che lavorano professionalmente nel campo della System & Network Security a livello di pianificazione, strategia, rischi

Corso di preparazione all'esame OPSA

E' previsto un corso di preparazione all'esame di 4 giornate di tipo "intensive", alle quali va aggiunta la mattina del quinto giorno, durante la quale i partecipanti avranno a disposizione un'ora di *program review* con il docente e quattro ore per l'esame finale di certificazione.

Le giornate formative affrontano i seguenti moduli:

- Il modulo **Security Analysis** costituisce la linea di riferimento per comprendere i risultati dei test di sicurezza come i file di log, l'output degli strumenti di sicurezza ed i dump di protocollo, nonché l'applicazione dei moduli OSSTMM secondo i risultati attesi e le soluzioni pratiche, applicati dal punto di vista della *business motivation*. Vengono anche applicate strategie per la valutazione dei rischi tecnici, test di sopravvivenza dei sistemi e della rete, soluzioni per l'architettura di sicurezza della rete.
- Il modulo **Red Team Strategies** fornisce una visione approfondita delle regole di approccio alla consulenza in materia di sicurezza, dalla fase di prevendita alla fase di preparazione, sino alla stesura del Security Report finale ed al laboratorio con l'ausilio di gruppi di *professional security tester*.
  Inoltre, i partecipanti analizzeranno anche varie strategie di Red Team e di Blue Team

per puntare ai risultati migliori, compreso lo sviluppo di varie strutture di attacco-rete sia per i test interni che per quelli esterni (Attack Test Lab).

- Il modulo **Security Project Management**, infine, fornisce una panoramica e rappresenta un trasferimento di conoscenza nell'ambito dei progetti di test *OSSTMM compliance* e delle loro applicazioni.
  E' focalizzato sulla gestione del progetto: reporting sulle tempistiche, valutazioni, gestione del team, necessità e specifiche tecniche nei contratti, interazioni con la clientela, efficienza dei test e controllo dei costi, compresa la gestione della redditività degli investimenti (ROI) attraverso le *Risk Assessment Values* dell'OSSTMM.

Prerequisiti

Per la certificazione ISECOM OPSA sono suggeriti i seguenti prerequisiti:

- media conoscenza della suite TCP/IP e dei suoi principali protocolli;
- esperienza nelle problematiche di base nella sicurezza dei sistemi *NIX e Microsoft Windows;
- conoscenza generica dell'installazione e della configurazione di software di verifica ed analisi della sicurezza (specificatamente su distribuzioni *NIX); dei sopraccitati software non è richiesta un'esperienza di base nell'utilizzo pratico;
- conoscenza e comprensione delle architetture di rete;
- conoscenza base dei principali servizi TCP/IP (HTTP, FTP, TELNET, SSH) nell'ottica delle esposizioni al rischio tecnico e di violazione delle politiche di sicurezza;
- conoscenza base dei sistemi per la sicurezza in rete: *router, firewall, intrusion detection system*;
- ottima conoscenza della lingua inglese e delle terminologie tecniche;
- conoscenza del Manuale OSSTMM 2.0;
- esperienza lavorativa o di ricerca pari ad almeno tre anni nel settore della ITC Security.

Esame

L'esame è basato su 50 domande a risposta multipla e consiste nell'applicazione di quanto appreso durante il corso, acquisendo dei risultati e giungendo a conclusioni e valutazioni, utilizzando la metodologia OSSTMM ed il workbook BSTA. L'esame è suddiviso in tre sezioni principali: Data Test e Log Analysis, Security Testing Projects e Professional Consulting.

Per ottenere la certificazione è necessario passare l'esame con uno score almeno del 60%.

Costi:

Corso di 4 gg.: € 2.500,00

Esame: € 450,00

L'esame può essere sostenuto indipendentemente dalla frequenza del corso..

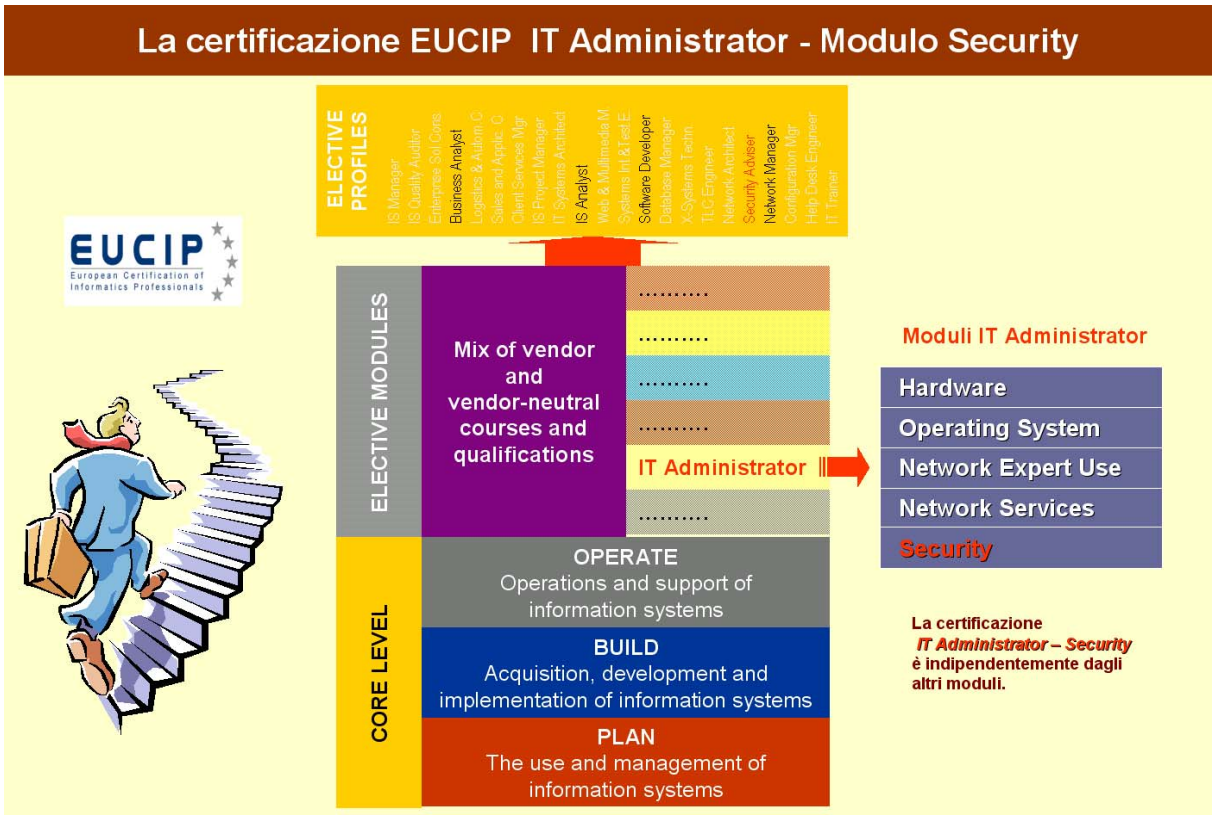
EUCIP - EUROPEAN CERTIFICATION OF INFORMATICS PROFESSIONALS

La certificazione IT Administrator era stata ideata come gradino superiore del programma ECDL Advanced / Specialised e destinata agli specialisti di tecnologie informatiche.

Nell'ambito di un riordino del sistema delle certificazioni promosse dal CEPIS (Council of European Professional Informatics Societis), la Fondazione ECDL e EUCIP Ltd hanno concordato che il programma di certificazione IT Administrator venisse gestito all'interno dello schema di quest'ultima, dove trova una collocazione più idonea come livello intermedio.

Il riferimento in Italia delle certificazioni EUCIP è AICA, Associazione Italiana per l'Informatica ed il Calcolo Automatico, fondata il 4 febbraio 1961. AICA è federata a IFIP, International Federation for Information Processing, ed al CEPIS, Council of European Professional Informatics Societies.

Schema della certificazione EUCIP



Certificazione IT Administrator - 5 SEC

Fermo restando il valore della certificazione IT Administrator a livello globale, i vari moduli che la compongono sono riconosciuti validi a livello internazionale come certificazioni autonome e sono riconosciute come moduli elettivi per alcuni profili EUCIP di livello professionale (es. Network Manager)

In particolare la certificazione IT Administrator - 5 SEC è una qualificazione obbligatoria per poter ottenere la certificazione EUCIP per il profilo NETWORK MANAGER.

E' una certificazione molto aderente alla realtà Europea; essa si basa su un Syllabus realizzato da un gruppo di esperti appartenenti al mondo Accademico, Professionale e con esperienze manageriali.

Il profilo del Certificato IT Administrator - 5 SEC comprende le conoscenze necessarie per garantire una gestione sicura delle strutture informatiche in particolare delle piccole e medie aziende, delle amministrazioni locali di dimensioni relativamente contenute, delle unità periferiche della pubblica amministrazione o della pubblica istruzione come sono le scuole primarie e secondarie.

Questa certificazione definisce il profilo della persona necessaria a molte realtà che attualmente sono ancora impreparate ad una gestione sicura e consapevole dei sistemi informatici.

Aree di competenza:

- Aspetti generali della Sicurezza
- Modelli organizzativi
- Crittografia
- Autenticazione e controllo degli accessi
- Disponibilità dei dati
- Codice maligno
- PKI - Infrastruttura a chiavi pubbliche
- Sicurezza delle reti
- Protezione dei dati
- Aspetti sociali ed etici della sicurezza informatica

Esame:

- 1 sessione teorica rispondendo a questionario a scelte multiple in lingua inglese. (durata del test 4 ore)
- 1 sessione pratica in cui al candidato viene richiesto di affrontare situazioni come configurare, modificare, risolvere una anomalia sia in sistemi Windows che in sistemi Linux. (durata del test 4 ore)

ISMS LEAD AUDITOR

L' Information Security Management Systems (ISMS) Lead Auditor è uno dei profili di certificazione professionale che proviene più dal mondo dell'auditing, ma si intreccia necessariamente con quello della sicurezza informatica in virtù delle Certificazioni di Sistema BS7799.

Non dovrebbe comparire propriamente tra le certificazioni professionali in sicurezza informatica, ma è utile presentarne la classificazione e i percorsi necessari al raggiungimento di questo riconoscimento.

Qualifica	Livello di studi	Esperienza di lavoro richiesta	Training previsto	Esperienza di Audit	
				quantità	giorni
Provisional auditor	Diploma di scuola secondaria	5 anni (4 anni se in possesso di Diploma di laurea o Laurea breve) di cui almeno 2 anni in information security	Corso ISMS lead auditor	---	---
Auditor	Diploma di scuola secondaria	5 anni (4 anni se in possesso di Diploma di laurea o Laurea breve) di cui almeno 2 anni in information security	Corso ISMS lead auditor	4 (come trainee auditor)	20 (10 on-site)
Lead auditor	Diploma di scuola secondaria	5 anni (4 anni se in possesso di Diploma di laurea o Laurea breve) di cui almeno 2 anni in information security	Corso ISMS lead auditor	4 (come trainee auditor) + 3 (come trainee lead auditor)	20 (10 on-site) 15 (10 on-site)
Principal auditor (consultant)	Diploma di laurea o Laurea breve	6 anni in information security	Corso ISMS lead auditor	7 (sole/lead audits)	35 (20 on-site)
Principal auditor (team leader)	Diploma di scuola secondaria	5 anni (4 anni se in possesso di Diploma di laurea o Laurea breve) di cui almeno 2 anni in information security	Corso ISMS lead auditor	certificato lead auditor da 6 anni + 3 sole audits con capacità di audit management in situazioni complesse	

Il percoso di certificazione prevede la frequenza dei cosi di training a cui segue un esame di verifica. Coloro che avranno soddisfatto i requisiti previsti e superato l'esame finale riceveranno la certificazione.

EC-COUNCIL

L'International Council of Electronic Commerce Consultants (EC-Council®) è una organizzazione indipendente, gestita dai propri membri, il cui principale scopo è definire standard professionali e fornire certificazioni professionali ed opportunità per la crescita e lo sviluppo delle professioni orientate al commercio elettronico.

EC-Council. fondata negli USA e con sede principale a New York, comprende tra i propri membri ed affiliati professionisti del mondo accademico, dell'industria e dell'IT.

CEH Certified Ethical Hacker Certification

Corso di preparazione all'esame:

E' previsto un corso intensivo di preparazione all'esame della durata di 5 giornate. Gli argomenti affrontati sono i seguenti:

- Introduction to Ethical Hacking
- Footprinting
- Scanning
- Enumeration
- System Hacking
- Trojans and Backdoors
- Sniffers
- Denial of Service
- Social Engineering
- Session Hijacking
- Hacking Web Servers
- Web Application Vulnerabilities
- Web Based Password Cracking Techniques
- SQL Injection
- Hacking Wireless Networks
- Virus and Worms
- Physical Security
- Linux Hacking
- Evading Firewalls, IDS and Honeypots
- Buffer Overflows
- Cryptography
- Penetration Testing

Target:

- Security officers
- Auditors
- Security professionals
- Site administrators

Prerequisiti: Conoscenza e pratica del TCP/IP, Linux and Windows 2000; sottoscrizione del "Legal Agreement" che prevede l'accettazione dell'uso delle conoscenze acquisite per soli scopi legali, liberando EC-Council da ogni responsabilità in caso di uso fraudolento.

Certificazione: si ottiene, dopo aver partecipato al corso, superando l'esame 312-50 presso un centro Thomson Prometric.

Esame: L'esame "Certified Ethical Hacker (312-50)" consiste in:

- 50 domande
- tempo massimo: 120 min.
- score minimo per il superamento: 70%
- costo: 150$

CHFI Computer Hacking Forensic Investigator

Corso di preparazione all'esame:

E' previsto un corso intensivo di preparazione all'esame della durata di 5 giornate. Gli argomenti affrontati sono i seguenti:

- Computer Forensics and Investigations as a Profession
- Understanding Computer Investigations
- Working with Windows and DOS Systems
- Macintosh and Linux Boot Processes and Disk Structures
- The Investigator's Office and Laboratory
- Current Computer Forensics Tools
- Digital Evidence Controls
- Processing Crime and Incident Scenes
- Data Acquisition
- Computer Forensic Analysis
- E-mail Investigations
- Recovering Image Files
- Writing Investigation Reports
- Becoming an Expert Witness
- Computer Security Incident Response Team
- Logfile Analysis
- Recovering Deleted Files
- Application Password Crackers
- Investigating E-Mail Crimes
- Investigating Web Attacks
- Investigating Network Traffic
- Investigating Router Attacks
- The Computer Forensics Process
- Data Duplication
- Windows Forensics
- Linux Forensics
- Investigating PDA
- Enforcement Law and Prosecution
- Investigating Trademark and Copyright Infringement

Target:

- Personale delle forze dell'Ordine e della Polizia
- Personale della Difesa e Militare
- Professionisti dell'e-Business Security
- Systems administrators

- Legali
- Professionisti del mondo bancario e assicurativo
- Agenzie Governative
- IT managers

Certificazione: si ottiene aderendo al Codice etico e, dopo aver partecipato al corso, superando l'esame 312-49 presso un centro Thomson Prometric.

Esame: L'esame "Computer Hacking Forensic Investigator (312-49)" consiste in

- 50 domande
- tempo massimo: 120 min.
- score minimo per il superamento: 70%
- costo: 150$

SCP SECURITY CERTIFIED PROGRAM

Security Certified Program (SCP) è un programma di certificazioni disponibile già dal 2001 da Ascendant Learning, una organizzazione con sede negli USA nell'Illinois.

C'è una ampia rete di Training Partners distribuiti a livello mondiale, che propone corsi di preparazione agli esami.

Il programma di certificazione si compone essenzialmente di 2 livelli di certificazione: il primo livello si ottiene con la certificazione SCNP (Security Certified Network Professional) che è propedeutica al successivo livello SCNA (Security Certified Network Architect).

SCNP (Security Certified Network Professional)

Il programma della certificazione Security Certified Network Professional (SCNP) è focalizzato sui seguenti argomenti:

- Firewalls
- Intrusion Detection
- VPNs
- SSL
- Risk Analysis,
- Linux & Windows Security
- Attack Methods
- Internet Security.

Prerequisiti: viene indicato come prerequisito, ma non richiesto per l'ottenimento della certificazione, un livello di conoscenze/esperienze della security analogo a quello di una certificazione Security+.

Certificazione: si ottiene superando i seguenti 2 esami presso un centro Thomson Prometric o Pearson VUE:

- Hardening the Infrastructure (HTI) - Exam SC0-411 - (60 domande, tempo massimo: 90 min. score minimo per il superamento: 75% - costo: 150$)
- Network Defense and Countermeasures (NDC) - Exam SC0-402 - (60 domande - tempo massimo: 90 min. - score minimo per il superamento: 75%)

Validità della certificazione: 2 anni

SCNA (Security Certified Network Architect)

Il programma della certificazione Security Certified Network Architect (SCNA) è focalizzato sui seguenti argomenti:

- Law and Legislation
- Forensics
- Wireless Security
- Securing Email
- Biometrics
- Strong Authentication
- Digital Certificates and Digital Signatures
- PKI Policy and Architecture
- Cryptography.

Prerequisiti: il prerequisito è la precedente certificazione SCNP.

Certificazione: E' necessario essere precedentemente certificati SNCP e si ottiene superando i seguenti 2 esami presso un centro Thomson Prometric o Pearson VUE:

- Enterprise Security Implementation (ESI) SC0-501 - (60 domande, tempo massimo: 90 min. score minimo per il superamento: 75% - costo: 180$)
- The Solution Exam (TSE) SC0-502 - (30 domande, tempo massimo: 120 min. score minimo per il superamento: 80% - costo: 180$)

Validità della certificazione: 2 anni

SEZIONE III
CERTIFICAZIONI "VENDOR SPECIFIC"

CHECK POINT

Il programma di certificazioni professionali sostenuto da Check Point è previsto per garantire le abilità, le competenze e l'aggiornamento in relazione ai propri prodotti.

CCSA - Check Point Certified Security Administrator

Target: Gli utenti finali e rivenditori che necessitano di una buna conoscenza di VPN/FireWall-1 ed di essere in grado effettuare l'installazione e la configurazione di setup.

Training: Sono previsti corsi di 2 giorni hands-on di preparazione all'esame.

Certificazione: si ottiene superando l'esame presso un centro Pearson VUE.

Esame: 156-210.4 Check Point NG with Application Intelligence - Management I

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Validità della certificazione: E' richiesta la ricertificazione per le nuove versioni del software Check Point. La certificazione ottenuta è valida per la release in corso e per quella immediatamente precedente.

CCSE - Check Point Certified Security Expert

Target: Amministratori di reti e di security che necessitano di implementare e mantenere VPN con FireWall-1. Questa certificazione richiede approfondite competenze su crittografia, firewall e VPN.

Training: Sono previsti corsi di 3 giorni hands-on di preparazione all'esame.

Certificazione: si ottiene superando i seguenti 2 esami presso un centro Pearson VUE:

Esame: 156-210.4 Check Point NG with Application Intelligence - Management I

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Esame: 156-310.4 Check Point NG with Application Intelligence - Management II

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Validità della certificazione: E' richiesta la ricertificazione per le nuove versioni del software Check Point. La certificazione ottenuta è valida per la release in corso e per quella immediatamente precedente.

CCSE Plus - Check Point Certified Security Expert Plus

Target: Amministratori di reti e di security che necessitano di implementare e mantenere VPN con FireWall-1, a livello enterprise e metodiche di troubleshooting. Questa certificazione richiede approfondite competenze su crittografia, firewall e VPN.

Training: Sono previsti corsi di 4 giorni hands-on di preparazione all'esame.

Certificazione: si ottiene superando i seguenti 2 esami presso un centro Pearson VUE:

Esame: 156-210.4 Check Point NG with Application Intelligence - Management I

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Esame: 156-310.4 Check Point NG with Application Intelligence - Management II

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Esame: 156-510.4 Check Point NG with Application Intelligence - Management III

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Validità della certificazione: E' richiesta la ricertificazione per le nuove versioni del software Check Point. La certificazione ottenuta è valida per la release in corso e per quella immediatamente precedente.

CCSPA Check Point Certified Security Principles Associate

Target: certificazione "entry level" che assicura la conoscenza dei fundamenti, dei concetti e delle "best practices" della security orientata a figure quali junior IS (Information Security) professionals, junior network security professionals o junior systems security professionals

Training: Sono previsti corsi di 3 giorni hands-on di preparazione all'esame.

Certificazione: si ottiene superando l'esame presso un centro Pearson VUE.

Esame: 156-110.4 Check Point Certified Security Principles Associate

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

CCMSE Check Point Certified Managed Security Expert

Target: certificazione avanzata per professionisti della security che si occupano dell'implementazione di Check Point's VPN-1/FireWall-1 e Provider-1 Internet security solutions.

Training: Sono previsti corsi di 3 giorni hands-on di preparazione all'esame.

Certificazione: si ottiene superando i seguenti 3 esami presso un centro Pearson VUE:

Esame: 156-210.4 Check Point NG with Application Intelligence - Management I

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Esame: 156-310.4 Check Point NG with Application Intelligence - Management II

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Esame: 156-810.4 Managing Multiple Sites with Provider-1 NG with Application Intelligence

- tempo massimo: 120 min. (90 min. madrelingua inglese)
- score minimo per il superamento: 70%

Validità della certificazione: E' richiesta la ricertificazione per le nuove versioni del software Check Point. La certificazione ottenuta è valida per la release in corso e per quella immediatamente precedente.

CISCO

CCSP Cisco Certified Security Professional

CCSP (Cisco Certified Security Professional) è un livello di certificazione avanzato per i professionisti IT attivamente coinvolti a progettare e sviluppare soluzioni dove intervengono questioni di security a tutti i livelli. Questi professionisti sono responsabili della sicurezza delle reti che sono chiamati a progettare e sviluppare; devono essere in grado di rendere e mantenere sicure reti ed infrastrutture garantendone la produttività e contenendone i costi. Essi devono aver maturato le conoscenze e le esperienze di sicurezza perimetrale, VPN, sistemi di intrusion protection come pure devono saper combinare queste tecnologie per realizzare soluzioni in reti semplici o complesse e integrate.

Target: il ruoli specifici di chi ha conseguito la CCSP sono:

- network security professional,
- systems security professional,
- infrastructure security specialist.

Prerequisiti: per ottenere la certificazione CCSP è necessario essere già certificato CCNA (Cisco Certified Network Associate) o CCIP (Cisco Certified Internetwork Specialist).

Certificazione: il candidato alla certificazione CCSP deve superare i seguenti 5 esami:

- 642-501 SECUR Securing Cisco IOS Networks
- 642-521 CSPFA Cisco Secure PIX Firewall Advanced
- 642-531 CSIDS Cisco Secure Intrusion Detection System
- 642-511 CSVPN Cisco Secure VPN
- 642-541 CSI Cisco SAFE Implementation

Validità della certificazione: la certificazione CCSP è valida per 3 anni; per ricertificarsi devono essere sostenuti gli esami indicati al momento per la certificazione.

Certificazione Cisco Firewall Specialist

Certificazione di sicurezza focalizzata sulla securizzazione di reti impiegando tecnologie Cisco IOS Software e Cisco PIX Firewall.

Prerequisito: Certificazione CCNA.

Certificazione: il candidato deve superare i seguenti 2 esami:

- 642-501 SECUR Securing Cisco IOS Networks
- 642-521 CSPFA Cisco Secure PIX Firewall Advanced

Validità della certificazione: la certificazione CCSP è valida per 2 anni; per ricertificarsi devono essere sostenuti gli esami indicati al momento per la certificazione.

Certificazione Cisco IDS Specialist

Certificazione di sicurezza focalizzata sulla securizzazione di reti impiegando tecnologie Cisco IOS Software e IDS atte a rilevare e rispondere ad attività di intrusione..

Prerequisito: Certificazione CCNA.

Certificazione: il candidato deve superare i seguenti 2 esami:

- 642-501 SECUR Securing Cisco IOS Networks
- 642-531 CSIDS Cisco Secure Intrusion Detection System

Validità della certificazione: la certificazione CCSP è valida per 2 anni; per ricertificarsi devono essere sostenuti gli esami indicati al momento per la certificazione.

Certificazione Cisco VPN Specialist

Certificazione di sicurezza focalizzata sulla securizzazione di reti ed in particolare ala configurazione di VPN su reti pubbliche condivise impiegando tecnologie Cisco IOS Software and Cisco VPN 3000 Series Concentrator.

Prerequisito: Certificazione CCNA.

Certificazione: il candidato deve superare i seguenti 2 esami:

- 642-501 SECUR Securing Cisco IOS Networks
- 642-511 CSVPN Cisco Secure VPN

Validità della certificazione: la certificazione CCSP è valida per 2 anni; per ricertificarsi devono essere sostenuti gli esami indicati al momento per la certificazione.

Esami

Gli esami necessari per conseguire queste certificazioni consistono in domande a risposta multipla e sono sostenibili presso i centri Thomson Prometric o Pearson VUE e sono in particolare:

- **Cisco Certified Network Associate (CCNA 640-801)**
  Durata: 90 minuti (55-65 domande)
  Lingua: Inglese

- **Securing Cisco IOS Networks (SECUR 642-501)**
  Durata: 90 minuti (65-75 domande)
  Lingua: Inglese

- **Cisco Secure PIX Firewall Exam (CSPFA 642-521)**
  Durata: 75 minuti (55-65 domande)
  Lingua: Inglese

- **Cisco Security Intrusion Detection Systems Exam (CSIDS 642-531)**
  Durata: 75 minuti (55-65 domande)
  Lingua: Inglese

- **Cisco Secure Virtual Private Networks (CSVPN 642-511)**
  Durata: 75 minuti (55-65 domande)
  Lingua: Inglese

- **Cisco SAFE Implementation Exam (CSI 642-541 CSI)**
  Durata: 75 minuti (55-65 domande)
  Lingua: Inglese

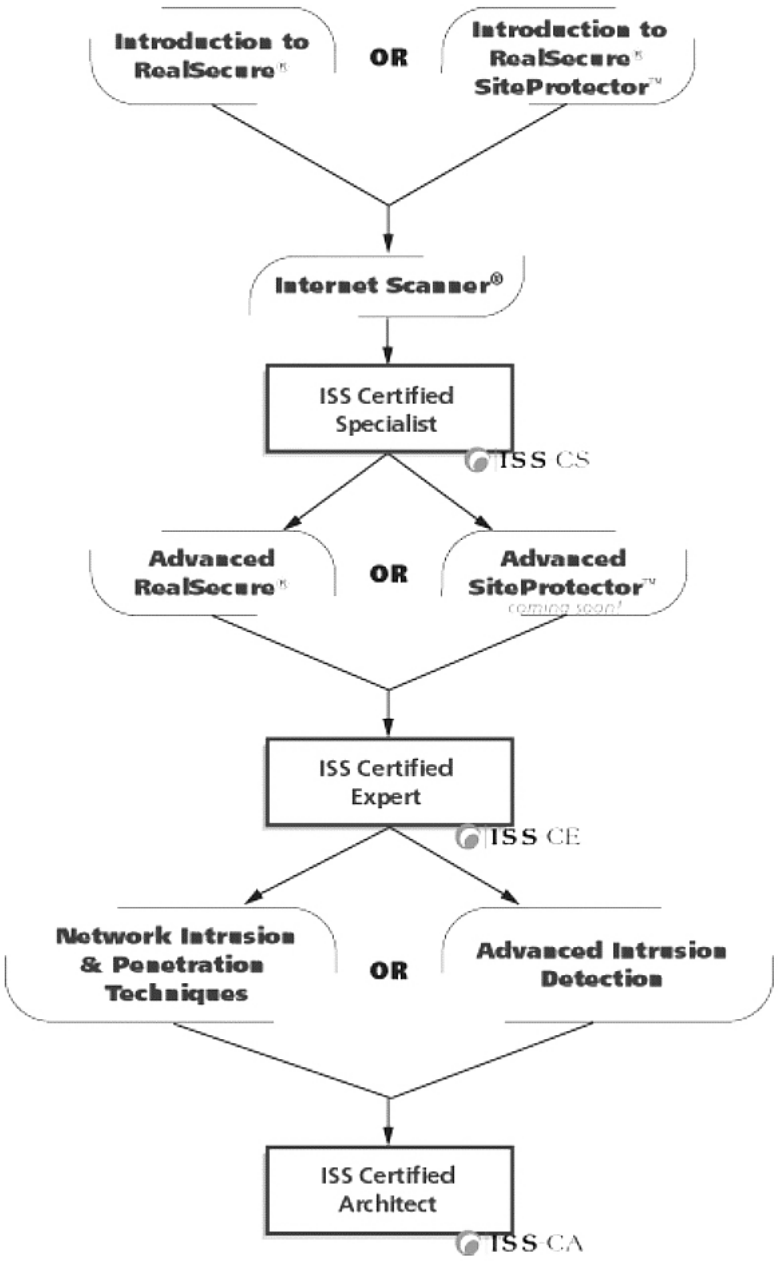
INTERNET SECURITY SYSTEMS

Livelli di certificazione

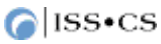
ISS è presente dal 1994 ed offre 3 livelli di certificazione focalizzati sull'impiego dei propri prodotti. Ciascun livello di certificazione comprende e include i precedenti per approfondimento delle conoscenze e delle tecniche di sicurezza. Di conseguenza per ottenere una certificazione di livello superiore è necessario avere in corso di validità quella di livello immediatamente inferiore.

Si possono scegliere percorsi alternativi di certificazione, in funzione di prodotti, secondo il seguente schema dei percorsi di certificazione

:



ISS-Certified Specialist (ISS-CS)



La certificazione ISS-CS attesta la conoscenza e l'esperienza delle tecnologie Internet Security Systems' RealSecure® e la conoscenza dei principi fondamentali di security.

Prerequisiti

- Conoscenza delle tecnologie RealSecure
- Esperienza pratica di 3 mesi sui prodotti RealSecure Protection System
- Conoscenza di base dei principi di networking
- Conoscenza di base dei principi di security

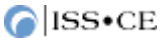
Certificazione: si ottiene superando 2 dei seguenti esami a seconda del percorso scelto, presso un centro Pearson VUE

- CS-RS-001 ISS Introduction to RealSecure
- CS-IS-001 ISS Internet Scanner

oppure

- CS-RSSP-001 ISS Introduction to RealSecure SiteProtector
- CS-IS-001 ISS Internet Scanner

ISS-Certified Expert (ISS-CE)



E' la certificazione ISS a livello intermedio che attesta la conoscenza avanzata della security e la familiarità con l'intera gamma dei prodotti ISS.

Prerequisiti

- Certificazione ISS-Certified Specialist (ISS-CS) valida
- Conoscenza approfondita delle tecnologie RealSecure
- Esperienza pratica di 6 mesi sui prodotti RealSecure Protection System
- Conoscenza a livello intermedio dei principi di networking e del TCP/IP
- Conoscenza a livello intermedio dei sistemi operativi Windows e Unix
- Conoscenza di base dei principi di security

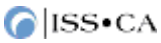
Certificazione: si ottiene superando 1 dei seguenti esami a seconda del percorso scelto, presso un centro Pearson VUE

- CE-ARS-001 ISS Advanced RealSecure

oppure

- CE-ASP-001 ISS Advanced SiteProtector

ISS-Certified Architect (ISS-CA)



E' la certificazione ISS a livello avanzato che attesta la conoscenza approfondita dell'intera gamma dei prodotti ISS e la conoscenza avanzata della security in generale e della sicurezza delle reti.

Prerequisiti

- Certificazione ISS-Certified Expert (ISS-CE) valida
- Conoscenza approfondita delle tecnologie RealSecure
- Esperienza di 9-12 mesi di sicurezza reti
- Conoscenza approfondita dei principi di networking e del TCP/IP
- Conoscenza approfondita dei sistemi operativi Windows e Unix
- Conoscenza operativa dei tools di vulnerability assessment e intrusion detection
- Familiarità con i vari metodi di attacco, inclusi: DDoS, buffer overflows, tecniche di brute force
- Esperienza di network traffic and log analysis

Certificazione: si ottiene superando 1 dei seguenti esami a seconda del percorso scelto, presso un centro Pearson VUE

- ISS Network Intrusion and Penetration Techniques (CA-NIPT-001)

oppure

- ISS Intrusion Detection and Forensics (CA-IDF-001)

Validità della certificazione: le certificazioni ISS sono valide per 18 mesi dalla certificazione. Per mantenere valida una certificazione è necessario ricertificarsi sullo stesso livello o certificarsi su quello più avanzato

E' necessario quindi sostenere nuovamente gli esami previsti al momento della ricertificazione.

Corsi di preparazione agli esami di Certificazione ISS

Sono previsti corsi finalizzati all'uso dei prodotti ISS, articolati in varie modalità, propedeutici al superamento degli esami di certificazione e sono erogati nelle varie sedi dislocate a livello mondiale.

MICROSOFT

Il programma di certificazione individuale Microsoft Certified Professional (MCP) ha l'obiettivo di attestare e valorizzare le competenze tecniche sui prodotti e le tecnologie Microsoft.

Il target delle certificazioni MCP sono Systems Engineer, Systems Administrator, Network Administrator, responsabili del supporto tecnico. Nel programma di certificazioni MCP si evidenziano le certificazioni MCSA e MCSE orientati alla sicurezza sia degli ambienti Windows 2000/XP + Server 2000 che degli ambienti Windows 2000/XP + Windows Server 2003.

MCSA: Security su Windows 2000

La specializzazione Microsoft Certified Systems Administrator (MCSA): Security su Windows 2000 identifica i Systems Administrator specializzati nell'implementare e amministrare la sicurezza in ambienti di medie e grandi dimensioni basati su piattaforma Microsoft.

Certificazione: Per ottenere la certificazione è necessario superare i seguenti 5 esami presso un centro Thomson Prometric o Pearson VUE:

3 esami Core	Esame 70-210: Installing, Configuring, and Administering Microsoft Windows 2000 Professional o Esame 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional
	Esame 70-215: Installing, Configuring, and Administering Microsoft Windows 2000 Server
	Esame 70-218: Managing a Microsoft Windows 2000 Network Environment
2 esami Security	Esame 70-214: Implementing and Administering Security in a Microsoft Windows 2000 Network
	Esame 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition o Esame SY0-101: CompTIA Security+

MCSA: Security su Windows Server 2003

Identifica i Systems Administrator specializzati in attività di gestione, implementazione e supporto della sicurezza su Windows Server 2003. Questi professionisti implementano l'infrastruttura e le procedure di sicurezza, garantiscono la disponibilità dei dati dell'organizzazione ed effettuano il monitoraggio di performance ed eventi sospetti nell'ottica di assicurare quotidianamente l'affidabilità e la sicurezza dell'intero sistema.

Questa certificazione identifica i Systems Administrators specializzati in attività di gestione e amministrazione della sicurezza su piattaforma Windows Server 2003. I candidati alla certificazione devono avere almeno un anno di esperienza in un ruolo focalizzato sulla sicurezza.

Certificazione: Per ottenere la certificazione è necessario superare i seguenti 5 esami presso un centro Thomson Prometric o Pearson VUE:

3 esami Core	Esame 70-210: Installing, Configuring, and Administering Microsoft Windows 2000 Professional o Esame 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional
	Esame 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment
	Esame 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
2 esami Security	Esame 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network
	Esame 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition o Esame SY0-101: CompTIA Security+

MCSE: Security su Windows 2000

La specializzazione MCSE su Windows 2000 relativa alla sicurezza identifica i Systems Engineer specializzati nel progettare, pianificare e implementare la Security in ambienti complessi, tipici in aziende di medie e grandi dimensioni.

Certificazione: Per ottenere la certificazione è necessario superare i seguenti 7 esami presso un centro Thomson Prometric o Pearson VUE:

4 esami Core	Esame 70-210: Installing, Configuring, and Administering Microsoft Windows 2000 Professional o Esame 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional
	Esame 70-215: Installing, Configuring, and Administering Microsoft Windows 2000 Server
	Esame 70-216: Managing a Microsoft Windows 2000 Network Environment
	Esame 70-217: Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure
3 esami Security	Esame 70-220: Designing Security for a Microsoft Windows 2000 Network
	Esame 70-214: Implementing and Administering Security in a Microsoft Windows 2000 Network
	Esame 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition o Esame SY0-101: CompTIA Security+

MCSE: Security su Windows Server 2003

Identifica i Systems Engineer specializzati nelle attività di progettazione, pianificazione e implementazione della sicurezza su Windows Server 2003. Questi professionisti sono responsabili della strategia di sicurezza dell'organizzazione; progettano le politiche di autenticazione e di gestione delle password e degli accessi; si occupano di gestire il sistema di messaggistica e di backup e di definire interfacce di connessione tra i sistemi di back end e quelli di front end.

Questa certificazione identifica i Systems Engineers specializzati nelle attività di progettazione, pianificazione e implementazione della sicurezza sulla piattaforma Windows Server 2003 come parte integrante di un ambiente sicuro. I candidati alla certificazione hanno almeno un anno di esperienza in un ruolo focalizzato sulla sicurezza.

Certificazione: Per ottenere la certificazione è necessario superare i seguenti 8 esami presso un centro Thomson Prometric o Pearson VUE:

5 esami Core	Esame 70-210: Installing, Configuring, and Administering Microsoft Windows 2000 Professional o Esame 70-270: Installing, Configuring, and Administering Microsoft Windows XP Professional
	Esame 70–290: Managing and Maintaining a Microsoft Windows Server 2003 Environment
	Esame 70–291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
	Esame 70-293: Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure
	Esame 70-294: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure
3 esami Security	Esame 70-298: Designing Security for a Microsoft Windows Server 2003 Network
	Esame 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network
	Esame 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition o Esame SY0-101: CompTIA Security+

Esami di Security Microsoft

Esame 70-214

Implementing and Administering Security in a Microsoft Windows 2000 Network

Profilo dei candidati

I candidati all'esame operano in ambienti di elaborazione con dimensioni da medie a molto grandi, nei quali vengono utilizzati Windows 2000 e Active Directory® e computer client dotati di sistemi operativi come Windows NT® Workstation 4.0, Windows 2000 Professional e Windows XP Professional.

I candidati devono possedere almeno un anno di esperienza nell'implementazione e nell'amministrazione di sistemi di protezione e infrastrutture di rete in ambienti con le seguenti caratteristiche:

- Da 200 a oltre 26.000 utenti supportati.
- Da 5 a oltre 150 postazioni fisiche.
- Infrastrutture quali reti LAN, WAN e senza fili.
- Applicazioni e servizi di rete tipici quali stampa, database, messaggistica, firewall e server proxy, infrastruttura a chiave pubblica, accesso remoto, gestione del desktop e hosting Web.
- Scenari di connettività che includono connessione alla rete aziendale dei singoli uffici e utenti situati in sedi remote e connessione delle reti aziendali ad altre reti e a Internet.

Competenze valutate

In questo esame di certificazione viene valutata la capacità di implementare e amministrare sistemi di protezione e infrastrutture di rete che utilizzano Windows 2000 e Active Directory.

Esame 70-220

Designing Security for a Microsoft® Windows® 2000 Network

Profilo dei candidati

I candidati a questo esame operano in ambienti di elaborazione di medie o grandi dimensioni basati sul sistema operativo di rete Windows 2000. Per partecipare a questo corso è necessario aver maturato almeno un anno di esperienza nell'implementazione e gestione di sistemi operativi di rete in ambienti che soddisfano i seguenti requisiti:

- Numero di utenti supportati compreso tra 200 e oltre 26.000.
- Numero di postazioni compreso tra 5 e oltre 150.
- I servizi di rete e le applicazioni più comuni comprendono: gestione di file e stampa, database, messaggistica, server proxy o firewall, server di accesso remoto, gestione desktop e hosting Web.

- Le esigenze di connettività comprendono la necessità per gli uffici distaccati e gli utenti remoti di collegarsi alla rete aziendale e di connettere la rete aziendale a Internet.

Competenze valutate

Questo esame di certificazione consente di valutare l'abilità dell'utente nell'analizzare i requisiti aziendali di protezione e nel progettare una soluzione in grado di soddisfare tali requisiti. La protezione include:

- Controllo dell'accesso alle risorse.
- Analisi dell'accesso alle risorse.
- Autenticazione.
- Crittografia.

Esame 70-227

Installing, Configuring, and Administering Microsoft® Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition

Profilo dei candidati

I candidati a questo esame operano in ambienti di elaborazione di medie o grandi dimensioni basati sul sistema operativo Windows 2000 Server. Per partecipare a questo corso è necessario aver maturato almeno un anno di esperienza nell'implementazione e gestione di sistemi operativi di rete in ambienti che soddisfano i seguenti requisiti:

- Numero di utenti supportati compreso tra 200 e oltre 26.000
- Più postazioni
- Accesso verso l'esterno per i servizi e le applicazioni client più comuni, quali accesso Web, posta elettronica, Telnet, FTP, reti private virtuali (VPN), gestione dei desktop e criteri di protezione del controllo di accesso
- Hosting di servizi di rete, ad esempio hosting Web interno ed esterno, messaggistica e firewall
- Le esigenze di connettività comprendono la necessità per gli uffici distaccati e gli utenti remoti di collegarsi alla rete aziendale e di connettere la rete aziendale a Internet.

Competenze valutate

Questo esame di certificazione consente di valutare le abilità dell'utente nell'implementazione, amministrazione e risoluzione dei problemi relativi ai sistemi informatici che utilizzano Microsoft ISA (Internet Security and Acceleration) Server 2000 Enterprise Edition.

Esame 70-298

Designing Security for a Microsoft Windows Server 2003 Network

Profilo dei candidati

La certificazione Microsoft Certified Systems Engineer (MCSE) on Windows Server™ 2003 rilascia credenziali ai professionisti IT che operano in un ambiente informatico con il livello di complessità tipico delle medie e grandi aziende. I candidati MCSE avranno almeno un anno di esperienza nell'implementazione e amministrazione di un sistema operativo di rete in ambienti con le seguenti caratteristiche:

- Da 250 a 5000 o più utenti
- Tre o più postazioni fisiche
- Tre o più controller di dominio
- Servizi e risorse di rete quali messaggistica, database, file e stampa, server proxy, firewall, Internet, Intranet, accesso remoto e gestione di computer client
- Requisiti di connettività quali la connessione di filiali e singoli utenti in postazioni remote alla rete aziendale e la connessione di reti aziendali a Internet.

I candidati MCSE, inoltre, dovranno avere almeno un anno di esperienza nei seguenti settori:

- Progettazione di un'infrastruttura di rete
- Implementazione e amministrazione di un sistema operativo desktop

Competenze valutate

Questo esame di certificazione consente di valutare la capacità dei candidati nel raccogliere e analizzare i requisiti aziendali per un'infrastruttura di rete protetta e nel progettare una soluzione di protezione che soddisfi tali requisiti.

Esame 70-299

Implementing and Administering Security in a Microsoft Windows Server 2003 Network

Profilo dei candidati

La certificazione Microsoft Certified Systems Administrator (MCSA) on Windows Server™ 2003 rilascia credenziali ai professionisti IT che operano in un ambiente informatico con il livello di complessità tipico delle medie e grandi aziende. I candidati MCSA avranno da 6 a 12 mesi di esperienza nell'amministrazione di client e sistemi operativi di rete in ambienti con le seguenti caratteristiche:

- Da 250 a 5000 o più utenti
- Tre o più postazioni fisiche
- Tre o più controller di dominio

- Servizi e risorse di rete quali messaggistica, database, file e stampa, server proxy, firewall, infrastruttura a chiave pubblica (PKI), Internet, Intranet, accesso remoto e gestione di computer client
- Requisiti di connettività quali la connessione di filiali e singoli utenti in postazioni remote alla rete aziendale e la connessione di reti aziendali a Internet.

Competenze valutate

In questo esame di certificazione viene valutata la capacità di implementare, gestire, mantenere un'infrastruttura di rete Windows Server 2003 e risolvere i relativi problemi di protezione, nonché di pianificare e configurare una PKI di Windows Server 2003.

RSA SECURITY

Il programma di certificazioni professionali RSA garantisce ai professionisti della security il riconoscimento delle conoscenze, abilità e le credenziali per l'implementazione e il mantenimento affidabile dei sistemi di security RSA.

RSA/CA - RSA Certified Administrator

Certificazione prevista per i professionisti della security che gestiscono e mantengono un sistema di sicurezza basato sui prodotti RSA SecureID. Essi possono amministrare i componenti RSA SecureID entro il contesto degli ambienti in cui operano, le problematiche di security, i problemi di implementazione oltre alla gestione degli aggiornamenti e delle patches e fixes.

RSA/CSE - RSA Certified Systems Engineer

Certificazione prevista per i professionisti della security che installano e configurano soluzioni di security realizzate con prodotti RSA SecureID. I candidati devono essere in grado di progettare soluzioni per i clienti basate sulle necessità aziendali; essere in grado di adeguare l'implementazione all'ambiente operativo ed alle infrastrutture dei clienti; condurre il progetto attraverso le fasi di prototipizzazione, modelli pilota e l'implementazione su larga scala.

Per ciascuna certificazione è richiesto un esame.

Costo dell'esame: $150.

Validità delle certificazione: E' richiesta la ricertificazione ad ogni nuova release dei prodotti. Una volta certificati, RSA avvisa quando è necessaria la ricertificazione.

SYMANTEC

Il programma di Certificazioni Symantec consiste nella combinazione di una Certificazione "vendor neutral" e nel superamento degli Esami "Symantec Solutions"

SCSE - Symantec Certified Security Engineer

Per ottenere la certificazione è necessario superare almeno 1 dei quattro esami Symantec ed essere in possesso di una delle seguenti Certificazioni:

GIAC Firewall Analyst (SANS)

GIAC Incident Handler (SANS)

GIAC Intrusion Analyst (SANS)

GIAC Windows Security Adminstrator (SANS)

SCTA - Symantec Certified Technology Architect

Per ottenere la certificazione è necessario superare almeno 1 dei quattro esami Symantec ed essere in possesso di una delle seguenti Certificazioni:

Security+ (CompTIA)

CISSP - Certified Information Systems Security Professional (ISC)2

CIPP - Certified Protection Professional (ASIS)

CISA - Certified Information Systems Auditor (ISACA)

CISM - Certified Information Security Manager (ISACA)

TICSA - Certified Security Associate (TruSecure)

Security Analyst (CIW)

GSEC - GIAC Security Essentials (SANS)

SCSP - Symantec Certified Security Practitioner

Per ottenere la certificazione è necessario superare almeno 2 dei quattro esami Symantec ed essere in possesso di una delle seguenti Certificazioni:

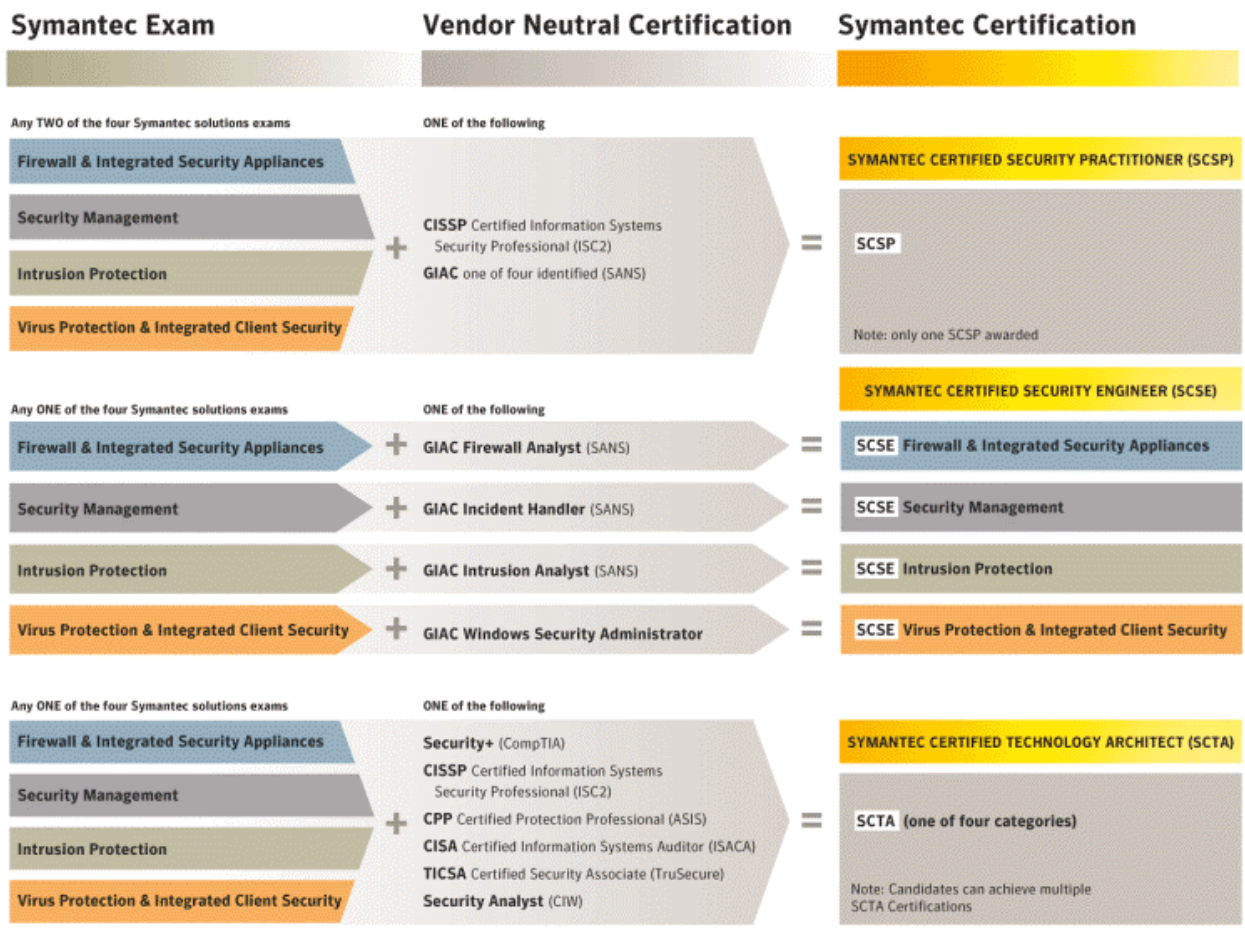
CISSP - Certified Information Systems Security Professional (ISC)2

GIAC Firewall Analyst (SANS)

GIAC Incident Handler (SANS)

GIAC Intrusion Analyst (SANS)

GIAC Windows Security Administrator (SANS)



Esami Symantec Solution:

- 501 Intrusion Protection Solution Exam
  Durata dell'esame: 90 minuti
- 502 Firewall and Integrated Security Appliances Solution Exam
  Durata dell'esame: 90 minuti
- 503 Security Management Solution Exam
  Durata dell'esame: 75 minuti
- 504 Virus Protection & Integrated Client Security Solution Exam
  Durata dell'esame: 90 minuti

Costo dell'esame: € 151 (Thomson Prometric)

Validità delle certificazioni: 2 anni

APPENDICE A – CODICI ETICI

(ISC)^2 CODE OF ETHICS

Code

All information systems security professionals who are certified by (ISC)^2 recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all Certified Information Systems Security Professionals (CISSPs) commit to fully support this Code of Ethics. CISSPs who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification.

There are only four mandatory canons in the code. By necessity such high-level guidance is not intended to substitute for the ethical judgment of the professional.

Additional guidance is provided for each of the canons. While this guidance may be considered by the Board in judging behavior, it is advisory rather than mandatory. It is intended to help the professional in identifying and resolving the inevitable ethical dilemmas that will confront him/her.

Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is a condition of certification.

Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The following additional guidance is given in furtherance of these goals.

Objectives for Guidance

In arriving at the following guidance, the committee is mindful of its responsibility to:

- Give guidance for resolving good v. good and bad v. bad dilemmas.
- To encourage right behavior such as:
    - Research
    - Teaching
    - Identifying, mentoring, and sponsoring candidates for the profession
    - Valuing the certificate
- To discourage such behavior as:
    - Raising unnecessary alarm, fear, uncertainty, or doubt
    - Giving unwarranted comfort or reassurance
    - Consenting to bad practice

- Attaching weak systems to the public net
- Professional association with non-professionals
- Professional recognition of or association with amateurs
- Associating or appearing to associate with criminals or criminal behavior

However, these objectives are provided for information only; the professional is not required or expected to agree with them.

In resolving the choices that confront him, the professional should keep in mind that the following guidance is advisory only. Compliance with the guidance is neither necessary nor sufficient for ethical conduct.

Compliance with the preamble and canons is mandatory. Conflicts between the canons should be resolved in the order of the canons. The canons are not equal and conflicts between them are not intended to create ethical binds.

Protect society, the commonwealth, and the infrastructure

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service to principals

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and protect the profession

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

ISACA - CODE OF PROFESSIONAL ETHICS

The Information Systems Audit and Control Association, Inc. (ISACA) sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

OSSTMM CODE OF ETHICS (from the OSSTMM 2.1)

Those who are partners with ISECOM or publicly claim to use the OSSTMM for security testing must uphold the following rules of engagement. These rules define the ethical code of acceptable practices in marketing and selling security testing or security consulting, performing security testing work, and handling the results of security testing engagements.

1. Sales and Marketing

1. The use of fear, uncertainty and doubt may not be used in the sales or marketing presentations, websites, supporting materials, reports, or discussion of security testing for the purpose of selling or providing security tests. This includes but is not limited to crime, facts, criminal or hacker profiling, and statistics.
2. offering of free services for failure to penetrate or provide trophies from the target is forbidden.
3. Public cracking, hacking, and trespass contests to promote security assurance for sales or marketing of security testing or security products are forbidden.
4. Performing security tests against any network without explicit written permission from the appropriate authority is strictly forbidden.
5. The use of names of past clients who you have provided security testing for is forbidden even upon consent of said client. This is as much for the protection of the client's confidentiality as it is for the security testing organization.
6. It is required to provide truthful security advice even when the advice may be to advise giving the contract to another company. An example of this would be in explaining to a company that your security testers should not be verifying a security implementation your organization designed and installed rather it should be tested by an independent 3rd party.

2. Assessment / Estimate Delivery

1. Verifying possible vulnerable services without explicit written permission is forbidden.
2. The security testing of obviously highly insecure and unstable systems, locations, and processes is forbidden until the security has been put in place.

3. Contracts and Negotiations

1. With or without a Non-Disclosure Agreement contract, the security tester is ethically bound to confidentiality, non-disclosure of customer information, and security testing results.
2. The tester must always assume a limited amount of liability as per responsibility. Acceptable limited liability is equal to the cost of service. This includes both malicious and non-malicious errors and project mismanagement.

3. Contracts must clearly explain the limits and dangers of the security test.
4. In the case of remote testing, the contract must include the origin of the testers by telephone numbers and/or IP addresses.
   5. Contracts must contain emergency contact persons and phone numbers.
5. The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
6. Contracts must contain the process for future contract and statement of work (SOW) changes.

4. Scope

1. The scope must be clearly defined contractually before verifying vulnerable services.
2. The scope must clearly explain the limits of the security test.

5. Providing Test Plan

1. The test plan must include both calendar time and man hours.
2. The test plan must include hours of testing.

6. Providing the rules of engagement to the client.

1. No unusual or major network changes allowed by the client during testing.
2. To prevent temporary raises in security only for the duration of the test, the client should notify only key people about the testing. It is the client's judgment which discerns who the key people are however it is assumed that they will be information and policy gatekeepers, managers of security processes, incident response, and security operations.
3. If necessary for privileged testing, the client must provide two, separate, access tokens whether they be logins and passwords, certificates, secure ID numbers, etc. and they should be typical to the users of the privileges being tested (no especially empty or secure accounts).
4. When performing a privileged test, the tester must first test without privileges in a black box environment and then test again with privileges.

7. Testing

1. The testers are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the client organization.
2. The exploitation of Denial of Service tests may only be done with explicit permission. An OSSTMM security test does not require one to exploit denial of service and survivability endangering type vulnerabilities in a test. The tester is expected to use gathered evidence only to provide a proper review of such security processes and systems.
3. Social engineering and process testing may only be performed in non-identifying statistical means against untrained or non-security personnel.

4. Social engineering and process testing may only be performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.
5. High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during testing must be reported to the customer with a practical solution as soon as they are found.
6. Distributed Denial of Service testing over the Internet is forbidden.
7. Any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source is forbidden.
8. Client notifications are required whenever the tester changes the testing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the client should be notified with progress updates weekly.

8. Reporting

1. Reports must include practical solutions towards discovered security problems.
2. Reports must include all unknowns clearly marked as unknowns.
3. Reports must state clearly all states of security found and not only failed security measures.
4. Reports must use only qualitative metrics for gauging risks based on industry accepted methods. These metrics must be based on a mathematical formula and not on feelings of the analyst.

9. Report Delivery

1. The client must be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
2. All communication channels for delivery of report must be end to end confidential.

EC-COUNCIL CODE OF ETHICS

This CODE OF ETHICS expresses the consensus of the profession on ethical issues and is a means to educate both the public and those who are entering the field about the ethical obligations of all e-commerce consultants. By joining EC-Council each member agrees to:

1. Keep private any confidential information gained in her/his professional work, (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.
2. Protect the intellectual property of others by relying on her/his own innovation and efforts, thus ensuring that all benefits vest with its originator.
3. Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public, that she/he reasonably believes to be associated with a particular set or type of electronic transactions or related software or hardware.
4. Provide service in their areas of competence, being honest and forthright about any limitations of her/his experience and education. Ensure that she/he is qualified for any project on which he/she works or proposes to work by an appropriate combination of education, training, and experience.
5. Never knowingly use software or process that is obtained or retained either illegally or unethically.
6. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
7. Use the property of a client or employer only in ways properly authorised, and with the owner's knowledge and consent.
8. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
9. Ensure good management for any project he/she leads, including effective procedures for promotion of quality and full disclosure of risk.
10. Add to the knowledge of the e-commerce profession by constant study, share the lessons of her/his experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
11. Conduct herself/himself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in her/his knowledge and integrity.

APPENDICE B – RIFERIMENTI WEB

(ISC)2 = International Information Systems Security Certifications Consortium, Inc.

www.isc2.org **www.clusit.it/isc2**

ISACA Information Systems Audit and Control Association

www.isaca.org **www.aiea.it**

SANS Institute

www.sans.org

CompTIA

www.comptia.org

OSSTM Open Source Security Testing Methodology

www.isecom.org **www.osstmm.org**

EUCIP - European Certification of Informatics Professionals

www.eucip.org **www.eucip.it**

ISMS Lead Auditor

www.irca.org/certification/certification_8.html

EC-Council

www.eccouncil.org

SCP Security Certified Program

www.securitycertified.net

CHECK POINT

www.checkpoint.com/services/education/certification

CISCO

www.cisco.com/en/US/learning

ISS

www.iss.net/emea/certification

MICROSOFT

www.microsoft.com/italy/traincert/mcp

RSA

www.rsasecurity.com

SYMANTEC

www.symantec.com/education/certification

CLUSIT Associazione Italiana per la Sicurezza Informatica
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO

GRAFICA DI COPERTINA: Giorgio Giudice