Certificazione CSX Practitioner + Cybersecurity Lab

Laboratori pratici di Cybersecurity e preparazione all'esame di certificazione CSX Practitioner di ISACA

(CSX-P)

Corso di certificazione CSX-P – CSX Practitioner accreditato da ISACA

40 ORE

La certificazione CSX-Practitioner consente di sviluppare ed attestare ufficialmente il possesso delle competenze e delle skill critiche di Cybersicurezza richieste nella vita reale da Incident Handlers, Security Analysts e Security Responders per: (1) identificare e svolgere attività di remediation delle vulnerabilità; (2) configurare ed implementare tecnologie di protezione adeguate; (3) rilevare, rispondere e ripristinare incidenti e disastri.

RISULTATI ATTESI:

Il corso, avvalendosi per almeno il 50% del tempo di numerose attività ed esercizi in ambienti simulati di scenari reali ed Hands-On Lab sui principali Security Tools, prepara ogni candidato al superamento dell'esame CSX Cybersecurity Practitioner di ISACA (CSX-P). e a:

- Utilizzare i processi di valutazione delle vulnerabilità e set di strumenti di scansione per identificare e documentare le vulnerabilità in base alla criticità delle risorse definite e agli impatti tecnici.
- Ottenere e aggregare le informazioni da più fonti, ad esempio registri, dati sugli eventi, valutazioni della rete, per l'utilizzo in intelligence delle minacce, rilevamento degli incidenti e risposta.
- Implementare i controlli di sicurezza informatica specifici - per rete, applicazione, endpoint, server e altro - e verificare che i controlli funzionino come richiesto dalle Policy e procedure aziendali.
- Implementare e documentare le modifiche ai controlli di sicurezza informatica, ad esempio sicurezza degli endpoint e sicurezza della rete, in conformità con le procedure di gestione delle modifiche.
- Identificare attività anomale e potenziali minacce interne, esterne e di terze parti alle risorse di rete utilizzando monitor di traffico di rete o sistemi di rilevamento e prevenzione delle intrusioni, oltre a garantire il rilevamento tempestivo di indicatori di compromissione.
- Eseguire analisi di attacco iniziale per determinare vettori di attacco, obiettivi, portata e impatto potenziale.
- Eseguire piani di risposta definiti per contenere il danno sulle risorse interessate.

39 CPE validi per il mantenimento delle certificazioni ISACA

Sconto 5% per iscrizioni entro 30 giorni

Sconto 10% aggiuntivo per almeno 3 iscritti della stessa azienda

INFO: corsi@aiea-formazione.it - Tel: 02.8716.9246

MODULO D'ISCRIZIONE AL CORSO Certificazione CSX Practitioner + Cybersecurity Lab

DATI FATTURAZIONE

Ragione Sociale - Cognome e nome	Partita iva/C.f.	Codice Destinatario/Pec
Via e Numero	CAP	Città e (PR)
E-mail Amministrazione	Telefono Azienda	Nr. Ordine d'acquisto/RdA

DATI PARTECIPANTI

Nome e Cognome	E-mail personale	Socio ISACA	Socio AIEA	ID ISACA

DATA E LOCATION: Verificare date e location sul sito www.aiea-formazione.it e specificare le proprie scelte di seguito

MODALITA' DI PAGAMENTO: Bonifico Bancario anticipato intestato a Profice
Coordinate Bancarie: IBAN:IT46 J030 3211 7020 1000 0806 292
Causale: Indicare cognome del partecipante e ragione sociale

PREZZO: Corso CSX Cybersecurity Practitioner

- ☐ 2.100,00€ + IVA
- ☐ 2.000,00€ + IVA (Riservato Soci ISACA)
- ☐ 1.900,00€ + IVA (Riservato Soci AIEA/ISACA MI)

AGEVOLAZIONI	☐ Sconto 5% per iscrizioni entro 30 giorni	☐ Sconto 10% aggiuntivo per almeno 3 iscritti
ACQUISTO VOUCHER ESAME	☐ 500,00€ + IVA	☐ 500,00€ + IVA (Riservato Soci AIEA/ISACA MI)
ACQUISTO MEMBERSHIP ISACA	☐ 250,00€ + IVA	
ACQUISTO MATERIALI	☐ 900,00€ + IVA	

REFERENTE ORGANIZZATIVO E AMMINISTRATIVO: Profice srl - P.iva 02487960201 - Codice Destinatario: M5UXCR1
Sede Legale: Via Fernelli, 28 - 46100 - Mantova (MN) - Tel: 02.8716.9246 - Fax: 02.8715.1741 - Email: direzione@profice.it
PARTNER DI AIEA (Associazione Italiana Information System Auditor) www.aiea-formazione.it - www.aiea.it

PRIVACY E DIRITTI DELL'INTERESSATO: I Suoi dati personali saranno trattati sia su supporto informatico che cartaceo e il loro conferimento è necessario per l'iscrizione al corso: la mancata fornitura dei dati non consentirà pertanto l'iscrizione. Accettando il presente regolamento, Lei autorizza il trattamento dei Suoi dati personali solo per fini organizzativi, contabili, e per aggiornarLa sulle nostre iniziative formative, nella piena tutela dei Suoi diritti e della Sua riservatezza e in conformità alle disposizioni di legge ai sensi del GDPR UE 679:2016 e del D.lgs. n. 101:18. Titolare del trattamento dei dati è Profice srls. In qualsiasi momento Lei potrà richiedere l'aggiornamento o la cancellazione dei Suoi dati personali scrivendo a direzione@profice.it.
RECESSO/DISDETTA : Il cliente, tramite fax o e-mail a corsi@aiea-formazione.it, potrà disdire dal contratto senza penali entro e non oltre il 15mo giorno precedente la data di inizio del corso: in questo caso Profice provvederà a rifondere l'intera quota versata. Oltre tale termine Profice potrà trattenere una penale di 50 Eu, o, qualora la richiesta di cancellazione pervenga negli ultimi 3 giorni dall'inizio corso, l'integrale quota di iscrizione.
ANNULLAMENTO DEL CORSO: Profice si riserva il diritto di annullare il corso per gravi impedimenti o per mancato raggiungimento del numero minimo di partecipanti, in qualsiasi momento, rifondendo quanto versato.
ASPETTI ORGANIZZATIVI: (1) L'iscrizione si intende perfezionata al momento del ricevimento, da parte della segreteria corsi, della presente scheda compilata in tutte le sue parti. Al raggiungimento del numero minimo di partecipanti verrà inviata una conferma d'iscrizione tramite fax o e-mail, al più tardi entro 10 giorni di calendario dalla data di inizio del corso. (2) Gli attestati verranno emessi in formato digitale successivamente alla partecipazione al corso ed a pagamento avvenuto.
PAGAMENTO: Il pagamento dovrà avvenire, a seguito della conferma inviata dalla segreteria corsi, a mezzo bonifico bancario (o Carta di Credito con 3% di sovrapprezzo)
FORMAZIONE FINANZIATA: è possibile avvalersi della Formazione Finanziata concordando con Profice gli adempimenti amministrativi prima del corso

Il Cliente previa lettura delle condizioni al presente contratto, in particolare delle clausole "aspetti organizzativi", "pagamento", "recesso/disdetta", "annullamento del corso",dichiara espressamente di approvarli specificatamente ai sensi e agli effetti di cui agli art. 1341 e 1342 cod. civ.

Data | Firma e Timbro

INVIARE MODULO a corsi@aiea-formazione.it o via FAX: 02.8715.1741

CORSO:	**Certificazione CSX Practitioner + Cybersecurity Lab** **Laboratori pratici di Cybersecurity e preparazione all'esame di certificazione CSX Practitioner di ISACA (CSX-P)**
DESCRIZIONE:	CSX Cybersecurity Practitioner di ISACA è stato nominato programma di certificazione professionale per il 2016 da SC Magazine Awards e rimane la prima e unica certificazione di prestazioni completa che mette alla prova la propria capacità di eseguire competenze di cyber-sicurezza validate a livello globale che coprono tutti e cinque gli ambiti di sicurezza previsti dal Cyber-security Framework del NIST (NIST CSF): Identify, Protect, Detect, Respond, Recovery.
RISULTATI ATTESI:	Il corso, avvalendosi per almeno il 50% del tempo di numerose attività ed esercizi in ambienti simulati di scenari reali ed Hands-On Lab sui principali Security Tools, prepara ogni candidato al superamento dell'esame CSX Cybersecurity Practitioner di ISACA (CSX-P). e a: - Utilizzare i processi di valutazione delle vulnerabilità e set di strumenti di scansione per identificare e documentare le vulnerabilità in base alla criticità delle risorse definite e agli impatti tecnici. - Ottenere e aggregare le informazioni da più fonti, ad esempio registri, dati sugli eventi, valutazioni della rete, per l'utilizzo in intelligence delle minacce, rilevamento degli incidenti e risposta. - Implementare i controlli di sicurezza informatica specifici - per rete, applicazione, endpoint, server e altro - e verificare che i controlli funzionino come richiesto dalle Policy e procedure aziendali. - Implementare e documentare le modifiche ai controlli di sicurezza informatica, ad esempio sicurezza degli endpoint e sicurezza della rete, in conformità con le procedure di gestione delle modifiche. - Identificare attività anomale e potenziali minacce interne, esterne e di terze parti alle risorse di rete utilizzando monitor di traffico di rete o sistemi di rilevamento e prevenzione delle intrusioni, oltre a garantire il rilevamento tempestivo di indicatori di compromissione. - Eseguire analisi di attacco iniziale per determinare vettori di attacco, obiettivi, portata e impatto potenziale. - Eseguire piani di risposta definiti per contenere il danno sulle risorse interessate.
DURATA:	40 ORE
DESTINATARI:	Security Analysts, Security Responders, Incident Handlers, Cybersecurity Auditors, Security Officers; Security Professionals; Site Administrators; in generale tutti coloro che si occupano dell'integrità delle infrastrutture di rete.
PRE-REQUISITI:	Per partecipare al corso e sostenere l'esame, si raccomanda la conoscenza di base di sistemi operativi (Windows e Linux). Per la frequenza del corso è necessario che ciascun partecipante disponga diun proprio laptop, che consenta un agevole accesso ad Internet via Web-browser per le attività di accesso ai laboratori tecnici
CONTENUTI:	I partecipanti con l'ausilio del docente seguiranno lezioni frontali, miste a laboratori pratici, inerenti i cinque ambiti di sicurezza del NIST Cybersecurity Framework: - Identificazione (Identify): Identificazione, Assessment e Valutazione di Asset, Minacce e Vulnerabilità - Protezione (Protect): Implementazione di controlli di Cybersicurezza, per proteggere un sistema dalle minacce identificate - Rilevamento (Detect): rilevazione di incidenti, eventi ed indicatori di compromissione sia a livello di rete che di sistema, e valutazione del danno potenziale - Risposta (Respond): definizione di piani di risposta agli incidenti a 360 gradi (Incident Response plan) e mitigazione degli incidenti - Ripristino (Recovery): ripristino da incidenti e disastri, redazione della documentazione di post-incident response, implementazione di piani di continuità Ogni giornata prevede almeno il 50% del tempo dedicato ad attività pratiche di durata variabile utilizzando più macchine virtuali messe a disposizione attraverso Laboratori Online a cui ogni partecipante potrà accedere per esercitarsi ed apprendere come e quando utilizzare i vari strumenti informatici di sicurezza, sistemi operativi, strumenti e utilità, la cui conoscenza sarà necessaria ai fini del superamento dell'esame: - Kali Linux - Kibana - Funzionalità di sicurezza Microsoft - Nmap / Zenmap - Comandi per la risoluzione dei problemi di rete - OpenVAS - PfSense - Security Onion - Squil - Applicazioni da console

	- Wireshark Nello specifico il corso approfondirà le aree di contenuto proporzionalmente alla rilevanza data da ISACA nell'esame: - Domain 1-Business and Security Environment (20%) - Domain 2-Operational Security Readiness (20%) - Domain 3-Threat Detection and Evaluation (20%) - Domain 4-Incident Response and Recovery (40%) Successivamente al termine del corso ogni partecipante potrà accedere per 6 mesi all'ambiente di laboratorio online di ISACA (acquistabile a parte), dove proseguire nella preparazione, esercitandosi in modo mirato ai fini dell'esame.
CERTIFICAZIONE:	CSX-P – CSX Practitioner riconosciuto da ISACA
MATERIALE DI STUDIO:	A ciascun partecipante sono fornite le slide del corso e l'accesso all'ambiente di laboratorio necessario per il tempo delle esercitazioni in aula. Oltre alle cinque giornate di corso e laboratori pratici in aula, chi lo desidera, al fine del sostenimento dell'esame, può richiedere anche l'acquisto dell'esame (online) e dell'abbonamento di 6 mesi ai laboratori online CSX-Practitioner di ISACA, basati su complessi scenari di Cybersecurity mutuati dalle situazioni reali più recenti, grazie ai quali i candidati possono misurarsi nell'utilizzo dei Security Tool più appropriati per risolvere un'ampia e sempre aggiornata varietà di task di Cybersecurity
DATE E LOCATION:	Verificare Date e Location sul sito www.aiea-formazione.it prima di iscriversi
CREDITI FORMATIVI:	39 CPE validi ai fini del mantenimento delle certificazioni ISACA
NOTE:	La certificazione CSX-P si differenzia rispetto alla certificazione CEH (Certified Ethical Hacker), perché quest'ultima approfondisce verticalmente le attività di Ethical Hacking (Vulnerability Assessment e Penetration Test), mentre il CSX-P, pur comprendendo una parte di formazione in comune al CEH soprattuto nei domini Identify e Detect, copre anche argomenti dei domini Protect, Respond e Recover, più orientati a figure che debbano gestire incidenti di sicurezza (analisti di sicurezza e security responder). Oltre alle cinque giornate di corso e laboratori pratici in aula, chi lo desidera, al fine del sostenimento dell'esame, può richiedere anche l'acquisto dell'esame (online) e dell'abbonamento di 6 mesi ai laboratori online CSX-Practitioner di ISACA, basati su complessi scenari di Cybersecurity mutuati dalle situazioni reali più recenti, grazie ai quali i candidati possono misurarsi nell'utilizzo dei Security Tool più appropriati per risolvere un'ampia e sempre aggiornata varietà di task di Cybersecurity
ESAME:	L'esame, acquistabile a parte, può essere schedulato entro 6 mesi dal corso, in una data a discrezione di ciascun partecipante e si svolge accedendo alla piattaforma online d'esame di ISACA, sotto il monitoraggio di un supervisore (proctor) online ISACA. L'esame è in lingua inglese, dura 240 minuti e richiede che il candidato risolva 16 Task di Cybersecurity applicate a Scenari di rischio reali simulati in ambienti virtuali, simili a quelli affrontati nel corso.
DOCENTE:	Docente accreditato CSX-P Cybersecurity Practitioner di ISACA, CEH- Certified Ethical Hacker di EC-Council, CHFI-Computer Hacking Forensics Investigator di EC-Council, Esperto di Cybersecurity ed Ethical Hacker professionista di lungo corso.
FORMAZIONE FINANZIATA:	PROFICE è certificata EN ISO 9001:2015 per il sistema di gestione per la Qualita, settori IAF/EA 35 e 37 - Certificato No. IT18-27105A del 9 Ottobre 2018 (Progettazione ed erogazione corsi di formazione professionale; Consulenza direzionale, organizzativa e di Compliance)
FORMAZIONE PER P.A.:	Profice è iscritta al MEPA per le attività di formazione e servizi specialistici. Questo corso è registrato con codice MEPA: profice_67

Chi è AIEA (ISACA Milan Chapter)

L'Associazione Italiana Information Systems Auditors - AIEA -, costituita in Milano nel 1979, riunisce coloro che in Italia svolgono professionalmente attività di Auditing e Controllo di sistemi ICT promuovendo la conoscenza e ampliando l'esperienza dei suoi aderenti nel campo dell'Information Systems Audit , Assurance, Governance e Security. L'Associazione,Capitolo di Milano di ISACA, favorisce lo scambio di metodologie, promuove un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo sia di affidabilità dell'organizzazione che di sicurezza dei sistemi. Promuove inoltre ricerche quale quella sulla Governance IT commissionata a SDA Bocconi, organizza un Convegno annuale, cura la traduzione in italiano di Val IT, COBIT®, e da oltre 15 anni del Manuale CISA e delle correlata documentazione, sostiene la diffusione delle certificazioni professionali CISA (Certified Information Systems Auditor), CISM(Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems).

Chi è ISACA

Con oltre 100.000 associati in 180 Paesi, ISACA® (www.isaca.org) è leader mondiale nel fornire competenze, certificazioni, community, patrocinio e formazione nei settori dell'assurance e sicurezza, del governo dell'impresa,della gestione dell'IT e dei rischi e della compliance correlati all'IT. Fondata nel 1969, ISACA, associazione indipendente senza fini di lucro, organizza conferenze internazionali, pubblica l'ISACA Control Journal®, e sviluppa standard internazionali relativi all'audit e al controllo dei sistemi IT, che contribuiscono a garantire i propri componenti sull'affidabilità e a trarre valore dai sistemi informativi. ISACA favorisce inoltre l'acquisizione delle competenze e delle conoscenze IT e le attesta mediante le certificazioni riconosciute a livello internazionale quali: CISA® (Certified Information Systems Auditor™),CISM® (Certified Information Security Manager®), CGEIT™ (Certified in the Governance of Enterprise ITTM) e CRISC™ (Certified in Risk and Information Systems Control™). ISACA aggiorna continuamente COBIT® che assiste i professionisti dell'IT e i manager delle imprese ad adempiere le proprie responsabilità relativamente all'IT governance e alla gestione manageriale, in particolare nell'ambito dell'assurance, sicurezza, rischio e controllo e a fornire valore al business.

Quali vantaggi per i soci AIEA

E' possibile iscriversi ad AIEA tramite ISACA, selezionando il Milan chapter (http://www.isaca.org/Membership/Join-ISACA).

I soci possono accedere a:

1) accesso gratuito
- a più di 20 Sessioni di Studio annuali, con crediti CPE utili al mantenimento delle certificazioni;
- all'ISACA eLibrary (raccolta di quasi tutte le pubblicazioni ISACA/ITGI);
- alle versioni elettroniche dei framework ISACA;
- ai webcasts e agli e-Simposi organizzati da ISACA;

2) sconti
- sulle pubblicazioni nel Bookstore ISACA;
- sulle quote d'iscrizione e sulle pubblicazioni di preparazione agli esami CISA, CISM, CGEIT e CRISC;
- su corsi ed eventi organizzati da AIEA Formazone o da altri Enti ed Associazioni in partnership o patrocinati;
- invio gratuito del magazine bimestrale ISACA Journal e delle newsletter AIEA.

Partner dei corsi AIEA Formazione

Profice
AIEA Training Partner