AIEA

ISACA
Sistemi informativi: averne fiducia e trarne valore
Capitolo di Milano

Profice
AIEA Training Partner

CYBER SECURITY e PEN TEST: METRICHE e ANALISI EVIDENZE +(opzionale) HANDS ON Tecnico

Fondamenti, tecniche, analisi di scenari reali + Hands-on Lab

- Corso 1: Corso pratico + esercitazioni interattive su 3 giornate
- Corso 2: Hands on con laboratori in ambiente di simulazione

CORSO 1: (3 gg) CYBER SECURITY e PEN TEST: METRICHE e ANALISI EVIDENZE

Destinatari: Auditor e addetti alle attività di Cybersecurity Detection

- Modulo 1: CYBER Security in Pratica
  - Sessione dedicata ai non tecnici, finalizzata alla comprensione dei fondamenti e delle tecniche di Cybersecurity e Incident detection & Management tramite spiegazioni teoriche supportate da esempi pratici ed interattivi, con particolare focus:
    - sulle principali tecniche di attacco della struttura IT di un'organizzazione, di detection ed analisi delle vulnerabilità
    - sull'individuazione e gestione delle contromisure
- Modulo 2: CYBER Security e PEN Test: Metriche e Standards
  - Sessione basata sul confronto interattivo e l'approfondimento di scenari reali, e dedicata:
    - alle tematiche di organizzazione, progettazione e gestione delle attività di Penetration Test e Vulnerability Assessment,
    - alle modalità di Misurazione e rappresentazione dei risultati,
    - agli standard internazionali di riferimento per i processi di Cybersecurity e per le attività di Penetration Testing
- Modulo 3: CYBER Security e PEN Test: comprensione e analisi evidenze
  - Sessione basata sul confronto interattivo e l'approfondimento di scenari reali, e dedicata:
    - all'analisi e comprensione delle evidenze risultanti dalle relazioni tecniche di Cybersecurity e Penetration Testing

CORSO 2: (1 gg) CYBER SECURITY e PEN Test: HANDS ON E LABORATORIO TECNICO

Destinatari: tecnici addetti alle attività di Vulnerability Assessment e Penetration Testing

- Sessione di Hands-On per «addetti ai lavori»,con esercitazioni tecniche in ambiente di simulazione finalizzate all'applicazione su scenari reali di tool e tecniche di Cybersecurity, Vulnerability Assessment e Penetration Testing
- **Numero chiuso per favorire interazione nei «Test di Laboratorio»: necessario PC per attività di Hands-On**

- 5% Sconto per iscrizioni entro il 30 giorni da inizio corso (salvo diversa segnalazione)
- **Ulteriore 10% di sconto** per iscrizioni di almeno 3 persone della stessa azienda
- **Fino a 30 CPE (23 Corso 1 + 7 corso 2)**, validi per il mantenimento delle proprie certificazioni ISACA
- Materiale didattico ed integrazioni pratiche in formato digitale

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

Sistemi informativi: averne fiducia e trarne valore

Capitolo di Milano

AIEA Training Partner

Scheda d'Iscrizione → Inviare a corsi@aiea-formazione.it o via fax a 02.8715.1741 **(INFO:02.8716.9246)**

Cyber-Security + Pen Test: Metriche e Analisi Evidenze + *(Opzionale)* Hands-On e Laboratorio Tecnico

Posti limitati

DATI DI FATTURAZIONE

Ragione Sociale / Cognome Nome | Partita IVA | Codice Fiscale

Via | Numero

CAP | Città | Provincia

E-mail dell'Azienda | Telefono dell'Azienda | FAX dell'Azienda

Ordine d'acquisto nr. *(facoltativo, solo se necessario per la società richiedente)* | Richieste amministrative specifiche

DATI DEI PARTECIPANTI

Nome e Cognome	Ruolo	Email	Socio AIEA	Socio ISACA NON AIEA	ID ISACA
			☐	☐	
			☐	☐	
			☐	☐	

L'offerta formativa AIEA è aperta anche ai non Soci, a condizioni di mercato.

Profice, su delega di AIEA per le attività formative, è responsabile dell'erogazione e della gestione organizzativa, logistica ed amministrativa del corso.

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.

QUOTA DI PARTECIPAZIONE (+IVA): Barrare l'opzione preferita:

- ☐ **CYBER SECURITY & PEN TEST + LAB corso completo + Lab (3+1 gg):** € 1.300 (SOCI AIEA); € 1.400 (ISACA NON AIEA); € 1.500 (NON SOCI ISACA)
- ☐ **SOLO METRICHE E EVIDENZE (3 gg):** € 1.000 (SOCI AIEA); € 1.100 (ISACA NON AIEA); € 1.200 (NON SOCI ISACA)
- ☐ **SOLO HANDS ON LAB TECNICO (1 gg):** € 360 (SOCI AIEA); € 380 (ISACA NON AIEA); € 400 (NON SOCI ISACA)

AGEVOLAZIONI:

☐ **Sconto 5%** per iscrizioni entro 30 giorni da inizio corso

☐ **Sconto 10% aggiuntivo per almeno 3 iscritti** della stessa azienda

DATE e LOCATION: Verificare date e location a cui si intende partecipare su www.aiea-formazione.it , quindi specificarle di seguito

☐ IN PRESENZA:.....

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 per accettazione**

MODALITÀ DI PAGAMENTO: Bonifico bancario anticipato

Profice AIEA Training Partner

Intestato a: PROFICE

Coordinate Bancarie: IBAN:IT30P0503457710000000000433

Causale: Nella causale indicare sigla corso e cognome/ragione sociale del partecipante

SUO IBAN per eventuale rimborso o annullamento:

Inviare il modulo compilato ad corsi@aiea-formazione.it, oppure via FAX a 02.8715.1741

GARANZIE 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 GDPRUE 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.

Training partner: **Profice**

P.IVA 02487960201 – www.aiea-formazione.it – www.profice.it

Tel+39/02.8716.9246 - Fax+39/02.8715.1741– corsi@aiea-formazione.it

Associazione Italiana Information Systems Auditors

AIEA - P.IVA 10899720154 - C.F. 97109000154 - www.aiea.it - aiea@aiea.it

CYBER SECURITY + PENETRATION TEST: METRICHE e ANALISI EVIDENZE + *(OPZIONALE)* HANDS-ON E LABORATORIO TECNICO

OBIETTIVI DEL CORSO	▸ Le tre giornate di corso:
	  ▸ sono strutturate in modo da fornire ad Auditor e Security Manager le competenze fondamentali sugli Standard, le tecniche e le metriche di analisi e comprensione dei processi di Cybersicurezza e delle attività di Penetration Testing
	  ▸ Sono progettate con l'obiettivo di:
	  ▸ Fornire esempi pratici sulle diverse tecniche di attacco e difesa nel mondo della Cybersicurezza
	  ▸ Analizzare sul campo le principali e più recenti tecniche di Cyberattacco, analisi vulnerabilità e individuazione contromisure
	  ▸ Comprendere i riflessi di natura organizzativa (come organizzare e gestire le attività) e contrattuale (quali SLA e punti d'attenzione Privacy)
	  ▸ Approfondire le metriche di misurazione dei risultati delle attività di Cybersecurity e di Penetration Testing e le relative modalità di rappresentazione al Business
	  ▸ Comprendere i concetti chiave dei principali Framework internazionali di riferimento in ambito Cybersecurity e Penetration Testing e le loro implicazioni pratiche
	▸ La giornata aggiuntiva di Hands-on e Laboratorio Tecnico interattivo:
	  ▸ E' progettata per Security Specialist, Security Manager o persone che abbiano frequentato le sessioni precedenti
	  ▸ Prevede di far esercitate i discenti sul proprio PC collegato in un ambiente di simulazione, che saranno guidati nell'utilizzo di tool e nell'applicazione delle tecniche per la gestione e risoluzione di numerosi casi di Cyberattacchi e vulnerabilità basati su scenari reali

A CHI SI RIVOLGE	▸ Security Manager e/o tecnici specializzati che intendono analizzare gli attacchi/vulnerabilitá informatici in uno scenario più ampio del singolo caso specifico ▸ Tutti coloro che pur non avendo un background tecnico sono interessati a comprendere le diverse tipologie e strategie di attacco informatico e a capire come comprendere ed analizzare le evidenze delle relazioni tecniche di sicurezza. ▸ In particolare manager e decisori aziendali che hanno bisogno di una chiave interpretativa business oriented dei risultati relativi alle evidenze tecniche di Pen Testing e Vulnerability Assessment
DURATA	▸ **CORSO 1: 3 giornate** ▸ **CORSO 2 (Hands on e laboratorio tecnico): 1 giornata**

PREREQUISITI	▸ CORSO 1: Nessuno, ma è utile disporre di conoscenze o esperienze in ambito IT e Information Security
	▸ CORSO 2:
	  ▸ Aver partecipato al corso 1 oppure disporre di competenze tecniche di Vulnerability Assessment e Pen Test
	  ▸ Richiesto utilizzo del proprio PC con privilegi di amministratore per partecipare alle esercitazioni di laboratorio

CONDIZIONI ECONOMICHE *(IVA esclusa)*	**CORSO 1 + CORSO 2 (3 gg + 1gg):** ▸ **1.300 Eu , se socio AIEA** ▸ 1.400 Eu, se socio ISACA non AIEA ▸ 1.500 Eu, se non socio ISACA **SOLO CORSO 1 (3 gg):** ▸ **1.000 Eu , se socio AIEA** ▸ 1.100 Eu, se socio ISACA non AIEA ▸ 1.200 Eu, se non socio ISACA **SOLO CORSO 2 (1gg):** ▸ **360 Eu, se socio AIEA** ▸ 380 Eu, se socio ISACA non AIEA ▸ 400 Eu, se non socio ISACA
AGEVOLAZIONI	▸ **5% di sconto** per ordini entro 30 giorni da inizio corso (salvo diversa segnalazione) ▸ **Ulteriore 10% di sconto** per almeno 3 partecipanti della stessa organizzazione
CPE	**CPE** validi ai fini del mantenimento delle certificazioni ISACA ▸ CORSO 1: 23 CPE ▸ CORSO 2: 7 CPE
DATE	▸ *Calendario aggiornato disponibile online su www.aiea-formazione.it oppure scrivi a corsi@aiea-formazione.it*
LOCATION	▸ *Location aggiornate disponibili online su www.aiea-formazione.it oppure scrivi a corsi@aiea-formazione.it*
METODO DIDATTICO	▸ Tutti i moduli prevedono l'alternarsi di spiegazioni teoriche e pratiche svolte da due docenti in compresenza durante tutto il corso. La spiegazione teorica prenderà in esame gli standard di riferimento mentre la spiegazione pratica prevede l'uso di un laboratorio con server e macchine virtuali installate in modo da poter dare evidenza pratica delle diverse tematiche. I laboratori preparati sono 12 e costituiscono circa 1/3 del corso che ha quindi raggiunge, soprattutto nelle sue fasi finali, una forte connotazione tecnica ▸ Il percorso del laboratorio prevede tre fasi didattiche per ogni argomento: (1) inquadramento teorico della tematica; (2) esempi e dimostrazioni pratiche; (3) esercitazioni guidate che consentano ai partecipanti di provare le tecniche spiegate. ▸ Il metodo didattico strutturato nelle tre fasi consente a tutti i partecipanti di accedere ad una formazione esperenziale e pratica ma guidata da parte del docente.
DOCENTI	▸ **Paolo Gasperi (Loogut) – Security Manager:** Socio AIEA, certificato CISM e Lead Auditor ISO 27001, è consulente esperto nel settore IT & Information sicurezza IT con focus sui sistemi di gestione e impatti di Informatica Giuridica, nonché Manager fondatore del CERT LooCert. ▸ **Alberto Ciresa (Loogut) – IT Security expert ed Ethical Hacker:** Formatosi inizialmente come Sistemista IT e progettista architetture di rete, ha sviluppato una professionalità di oltre 25 anni nella gestione e progettazione tecnica dei sistemi di IT & Information Security, con particolare focus sulle attività di gestione CERT, Incident detection ed Ethical Hacking
PROGRAMMA	▸ *Programma di dettaglio disponibile nella pagina successiva*

CYBER SECURITY + PENETRATION TEST: METRICHE e ANALISI EVIDENZE + *(OPZIONALE)* HANDS-ON E LABORATORIO TECNICO

PROGRAMMA CORSO 1	**CYBER SECURITY + PENETRATION TEST: METRICHE e ANALISI EVIDENZE – GIORNI 1, 2 e 3**
	• MODULO 1: CYBERSECURITY IN PRATICA
	  ◦ Sessione dedicata ai non tecnici, finalizzata alla comprensione dei fondamenti e delle tecniche di Cybersecurity e Incident detection & Management tramite spiegazioni teoriche supportate da esempi pratici ed interattivi, con particolare focus su:
	  ▪ Evoluzione tecniche di Cybersecurity Management e impatto sulle aziende; riferimento ai diversi report ed analisi;
	  ▪ Struttura delle reti, modelli di riferimento. Protocolli di trasmissione dati;
	  ▪ Architettura delle rete (principi di sicurezza);
	  ▪ Principali tecniche di attacco, di detection, analisi vulnerabilità e gestione delle contromisure:
	  ▫ VA, PT, portscan, sniffing e network attacks; enumerazione ed accesso abusivo; Input validation e buffer overflow; password cracking; crittografia dei dati; web application security; cavalli di troia, backdoor e malware; WIFI e relative vulnerabilità; man in the middle attack; sicurezza fisica delle rete tra DMZ e firewall; social engineering.
	• MODULO 2: PEN TEST METRICS & STANDARDS
	  ◦ Sessione basata sul confronto interattivo e l'approfondimento di scenari reali, e dedicata a:
	  ▪ Gli standard di riferimento: Penetration Testing Execution Standard (PTES); PCI Penetration testing guide (PCI DSS Pen Testing Guidance & Requirements); Penetration Testing Framework; Technical Guide to Information Security Testing and Assessment (NIST800-115); Information Systems Security Assessment Framework (ISSAF); Open Source Security Testing Methodology Manual (OSSTMM)
	  ▪ Aspetti organizzativi e legali: Come organizzare un penetration test; Pen test e professionisti esterni (profili di responsabilità e normativa sulla privacy)
	• MODULO 3: ESEMPI, COMPRENSIONE e ANALISI EVIDENZE
	  ◦ Sessione basata sul confronto interattivo e l'approfondimento di scenari reali, e dedicata all'analisi e comprensione delle evidenze risultanti dalle relazioni tecniche di Cybersecurity e Penetration Testing:
	  ▪ dalla riunione iniziale di un PenTest alla rappresentazione dei risultati nella relazione tecnica ed in quella destinata al management;
	  ▪ schemi di analisi dei risultati

PROGRAMMA CORSO 2	**CYBER SECURITY + PENETRATION TEST: HANDS-ON E LABORATORIO TECNICO – GIORNO 4** • Sessione di Hands-On per «addetti ai lavori»,con esercitazioni tecniche in ambiente di simulazione finalizzate all'applicazione su scenari reali di tool e tecniche di Cybersecurity, Vulnerability Assessment e Penetration Testing ◦ VA, PT, portscan, sniffing e network attacks; enumerazione ed accesso abusivo; Input validation e buffer overflow; password cracking; crittografia dei dati; web application security; cavalli di troia, backdoor e malware; WIFI e relative vulnerabilità; man in the middle attack; sicurezza fisica delle rete tra DMZ e firewall; social engineering, • Richiesto utilizzo del proprio PC con privilegi di amministratore e competenza tecnica in ambito Vulnerability Assessment e Penetration Testing

ISACA, AIEA e i suoi Partner

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:

- 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
- 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.

I Partner dei corsi AIEA Formazione

Profice
AIEA Training Partner

techrain
Logistic Partner