Swascan Academy

Cyber defense

security e data protection in azienda

Giugno 2022

Con il patrocinio di:

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

formazione@swascan.com

Swascan Academy

Descrizione

Un percorso accademico affidato ai migliori esperti di cyber italiani che sposa casi reali e LAB tecnici d'eccellenza, strutturato con l'obiettivo di supportare i corsisti nella gestione della Sicurezza Informatica.

- **Conoscenza è difesa:** impara a conoscere le minacce che mettono a rischio la tua organizzazione
- **Resilienza:** padroneggia le best practice e gli strumenti per difendere il tuo perimetro digitale
- **Il fattore umano:** la Cyber non è solo tecnologia, impara a proteggere i tuoi dipendenti
- **Vai oltre la superfice:** impara a conoscere la Threat Intelligence e il dark web
- **Costruisci:** come impostare un framework efficace ed efficiente
- **Worst case scenario:** come affrontare un Data Breach

Sei punti fondamentali, un percorso completo ed esaustivo per comprendere i rischi, riconoscerli e contrastarli in maniera efficace.

swascan.com
Formazione@swascan.com

Swascan Academy

Programma didattico

Giornata 1

Ore 09:00 – 13:00
Human Risk

La tutela del business aziendale e della sua reputazione comincia dalla consapevolezza e dai comportamenti responsabili del personale. I dati dimostrano come la tecnologia non sia più sufficiente. È dunque importante sensibilizzare i propri dipendenti aziendali nel potenziare le proprie difese ed aumentare la propria cybercultura al fine di proteggere l'azienda dall'errore umano che, in senso lato, è responsabile della più parte degli incidenti di sicurezza e data breach conosciuti. È importante incrementare il livello della human security ed elaborare una policy di sicurezza aziendale.

Ore 14:00 – 18:00
Technology Risk

Se lavori in un'organizzazione - piccola o grande che sia -, è probabile che la tua infrastruttura digitale si affidi a una varietà di strumenti IT, come dispositivi intelligenti, PC e sistemi basati su cloud. Potresti avere in mano i dati dei clienti, le informazioni sui dipendenti e possibilmente progetti di prodotti dettagliati... Un'entropia informatica che potrebbe essere difficile da gestire, soprattutto quando tutti gli oggetti che rendono possibile il nostro lavoro, sono anche un possibile punto debole. In questo focus, parleremo degli attacchi machine to machine. Dagli attacchi che sfruttano i device IoT fino alle modalità di Criminal hacking che fanno leva sulle tecnologie abilitanti per lo smart working come le VPN.

Swascan Academy

Giornata 2

ore 09:00 – 13:00
Compliance Risk

Rischio compliance: è «il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina)».
Tra le normative generali che generalmente vengono fatte rientrare in tutte le aziende nell'ambito della compliance vi sono:

- Antiriciclaggio e contrasto del finanziamento del terrorismo;
- Lgs. 231/01 sulla "responsabilità amministrativa delle persone giuridiche";
- Privacy e protezione dei dati personali;
- Lgs 141/10 e Codice del Consumo;
- Security – sicurezza informatica;
- Safety – d. lgs. 81/2008 sulla "sicurezza sul posto di lavoro";
- Qualità e certificazione ISO9001 (per chi è soggetto).

Forniremo una panoramica delle principali normative da rispettare e gli strumenti e le metodologie da intraprendere affinché le aziende possano considerarsi Compliant.

Ore 14:00 – 18:00
Risk Analysis e Management

Ha lo scopo di illustrare le principali tecniche ed i principali strumenti di Cyber Risk Analysis e come utilizzarli sul campo, con focus soprattutto sull'Information Security Risk e Privacy Risk. Nello specifico partendo da un accenno ai principali standard internazionali di riferimento.
Lo scopo della lezione è fornire la terminologia, metodologie, tecniche e strumenti di base per:

- Fornire le competenze base relative alla gestione del Rischio Cyber
- Applicare diversi modelli recepiti dalle best practice del settore
- Policy compliance (Identity e Access Management, Information Security Event Management)
- Audit e verifiche di sicurezza (Vulnerability Assessment, Penetration Test, Code Review, Audit dei processi)

Swascan Academy

Giornata 3

Ore 09:00 – 13:00
OSINT

In questo modulo vengono esposte le nozioni e le conoscenze di base per coloro che si affacciano per la prima volta al mondo dell'intelligence e nello specifico dell'OSINT (open source intelligence). L'obiettivo non è quello di diventare "esperti di OSINT" in un giorno, bensì di imparare una metodologia di lavoro, come strutturare un Report OSINT, ed acquisire le basi di installazione ed utilizzo dei principali strumenti on-line e risorse software.

Ore 14:00 – 18:00
Threat Intelligence

Nel mondo della sicurezza informatica, la Cyber Threat Intelligence riveste ormai un ruolo di primo piano. Ecco perché è fondamentale monitorare Internet e il Dark Web per poter contrastare in maniera efficace possibili attacchi informatici. Questa lezione introduce agli studenti le metodologie fondamentali dell'intelligence e la loro applicazione nella cyber threat intelligence. Implementare un programma di strategie di Threat Intelligence delle minacce consente all'organizzazione di attuare misure predittive.

Swascan Academy

Giornata 4

ore 09:30 – 16:00
Ethical Hacking

Nella prima parte della giornata viene definita la figura dell'Ethical Hacker e i concetti teorici di base. Verranno, inoltre, presentate e messe a confronto le principali tipologie di hacker (White Hat e Black Hat) nel contesto informatico.
Verranno poi illustrate le principali metodologie di attacco informatico e le fasi per veicolare e portare a termine un cyber attack. Infine, verranno presentati gli strumenti necessari per difendere il proprio perimetro aziendale da incursioni esterne.

Ore 16:00 – 18:00
Cyber Lab

Attraverso un test-lab dedicato, simuleremo diverse tipologie di attacco informatico.

Swascan Academy

Giornata 5

Ore 09:00 – 13:00
Cyber Security Framework

Questo modulo ha l'obiettivo di indicare e descrivere i modelli di Cyber Security Framework introducendo i concetti di Sicurezza Predittiva, Preventiva e Proattiva necessari per una gestione dell'infrastruttura tecnica.
Lo scopo della lezione è fornire la terminologia, le metodologie, le tecniche e gli strumenti di base per:

- Valutare un Cyber Security Framework
- Comprendere i Layers di Cyber Security
- Identificare Processi, Tecnologie e Competenze per la gestione del Cyber Security Framework

Ore 14:00 – 17:30
E in caso di Data Breach?

Concluderemo il nostro percorso formativo parlando di Data Breach e Incident Response. I corsisti si concentreranno su come progettare, sviluppare e implementare correttamente i piani di risposta agli incidenti di sicurezza.
Impareremo a conoscere tre aspetti importanti dell'incident response: l'analisi dell'impatto aziendale, il piano di continuità aziendale e il piano di disaster recovery. Dopo aver completato il corso, sapremo come prepararsi agli incidenti e come attuare il processo di mitigazione per aiutare la propria azienda anche nell'immediato.

Swascan Academy

Destinatari

Il Corso si rivolge a tutti coloro che vogliono acquisire conoscenze, metodologie e strumenti per la gestione e la tutela del perimetro aziendale e dei dati sensibili.

Tra i principali professionisti:

- Personale IT e ICT
- Responsabili Cyber Security
- Auditor
- DPO
- Legal Office
- CEO, CISO, CSO, CIO

Le caratteristiche e il taglio formativo particolarmente innovativo ed efficace rendono il percorso adatto anche a Studenti di Ingegneria, Informatica, e Computer Science per integrare il loro curriculum accademico con nozioni, concetti ed esercitazioni pratiche nonché e a tutti coloro che sono appassionati di Cyber Security e vorrebbero arricchire il proprio bagaglio personale.

Swascan Academy

Metodologia

Il Corso sarà erogato in modalità sincrona attraverso la creazione di classi virtuali.

Il Corso avrà una durata di **40 ore** programmate in un appuntamento settimanale della durata di **8 ore** nella fascia oraria **09:00 – 18:00.**

Docenti altamente qualificati

La docenza è affidata a formatori qualificati con anni di esperienza nel settore della Cyber Security.

Modalità DAD

Segui il corso da dove vuoi tu! Il corso è interamente somministrato in modalità DAD.

swascan.com
Formazione@swascan.com