esac formazione

MASTER

CYBER DEFENSE

Security e data protection in azienda

Dal 19 settembre al 12 dicembre 2024

FORMAZIONE A DISTANZA

Swascan
TINEXTA GROUP

CONFCOMMERCIO
VICENZA

Centro Formazione Esac | tel. **0444 964300** | **www.esacformazione.it**

CYBER DEFENSE È

Un percorso strutturato con l'obiettivo di supportare i corsisti nella gestione della Sicurezza Informatica.

GLI OBIETTIVI

- **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, proteggerà i tuoi dipendenti.
- **Vai oltre la superfice:** approfondisci la Threat Intelligence e conosci il dark web.
- **Costruisci la sicurezza:** come impostare un framework efficace ed efficiente.
- **Worst case scenario:** scegli come affrontare un Data Breach.

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

Swascan
TINEXTA GROUP

Partner tecnico
Swascan è una Cyber Security Company nata da un'idea di **Pierguido Iezzi** e **Raoul Chiesa**. È la prima azienda di **Cyber Security Italiana** proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence**, oltre ad essere un centro di eccellenza di Cyber Security Research. Swascan è stata premiata con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo un'azienda, dunque, ma un gruppo italiano e un hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale.

PROGRAMMA DIDATTICO

PRIMO MODULO
10 ore

19-26 settembre e **3 ottobre**
con orario **14.00-17.30**
L'ultima lezione sarà con orario **14.00-17.00**

Ingegneria Sociale e OSINT: Strumenti e Strategie di Sicurezza Informatica

In questo corso, ti immergerai nel mondo della cybercultura e della sicurezza informatica, con un focus particolare su due aspetti cruciali: l'ingegneria sociale e l'OSINT (Open Source Intelligence).

Cosa imparerai?

1. Difenditi dagli attacchi di ingegneria sociale

- Smaschera le trappole: impara a riconoscere e sventare le diverse tipologie di attacchi di ingegneria sociale, tra cui phishing, spear phishing, smishing, vishing e malware.
- Rafforza le tue difese: sviluppa le competenze necessarie per proteggerti dagli attacchi di ingegneria sociale, sia online che offline.

2. Sfrutta l'OSINT per raccogliere informazioni

- Trasformati in un detective digitale: scopri come utilizzare l'OSINT (Open Source Intelligence) per raccogliere informazioni su persone, aziende e organizzazioni da fonti online aperte.
- Esplora una vasta scelta di risorse: impara a sfruttare un'ampia gamma di fonti OSINT, tra cui motori di ricerca, social media, forum online, database pubblici e archivi storici.

3. Impara (facendo) come nascono gli attacchi di ingegneria sociale personalizzati

- Simula la profilazione dei tuoi target: impara come si creano profili dettagliati degli obiettivi, identificando le loro caratteristiche, interessi e vulnerabilità.
- Scopri come si individuano le vulnerabilità specifiche dei vari target e come si sfruttano per creare attacchi di ingegneria sociale su misura.

SECONDO MODULO

10 ore

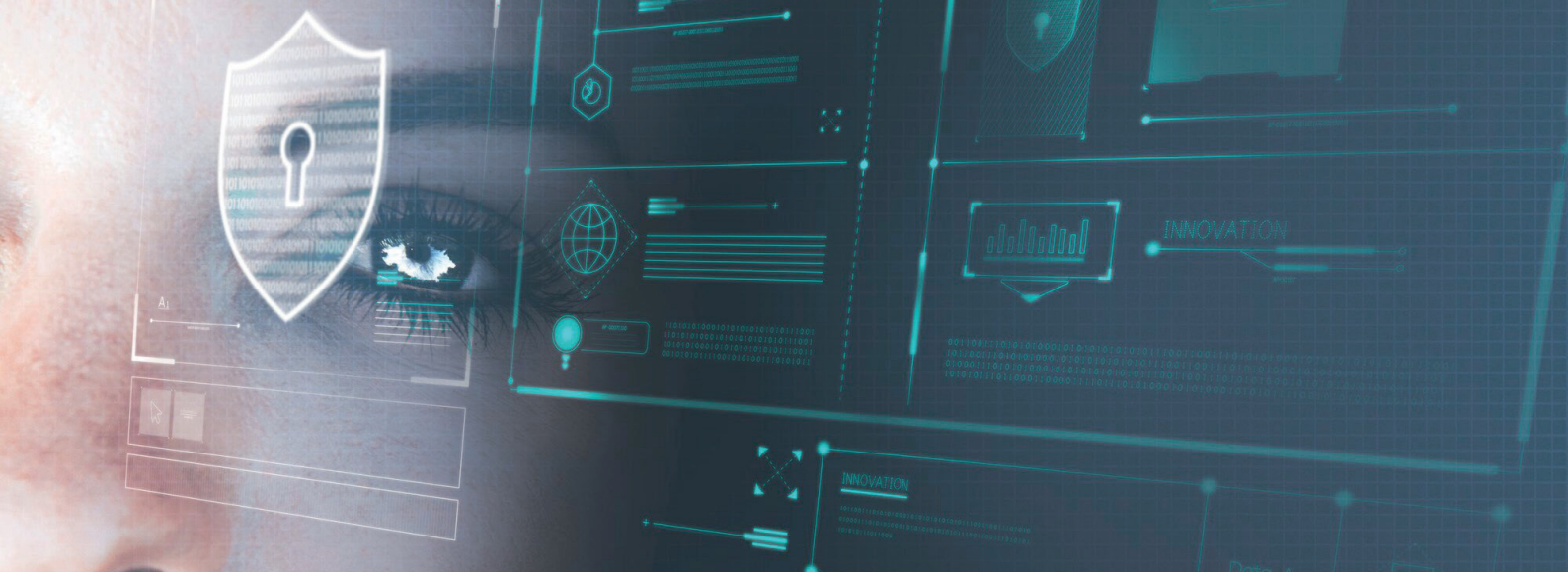
10-17-24 ottobre
con orario **14.00-17.30**
L'ultima lezione sarà con orario **14.00-17.00**

Cyber Risk e sicurezza delle informazioni: dalla Teoria alla Pratica

In questo corso, ti immergerai nelle principali tecniche e nei migliori strumenti per la valutazione e la gestione del Cyber Risk, con un focus particolare sull'Information Security Risk e sul Privacy Risk.

Cosa imparerai?

- **Gli standard internazionali di riferimento:** scoprirai i principali standard come ISO 27001, NIST Cybersecurity Framework e GDPR per comprendere le best practice globali per la gestione del Cyber Risk.
- **Terminologia, metodologie e tecniche:** padroneggerai il vocabolario specifico del Cyber Risk Analysis e acquisirai le competenze necessarie per identificare, valutare e mitigare i rischi informatici.
- **Modelli di gestione del rischio:** applicherai diversi modelli basati sulle best practice del settore, come il modello NIST, per strutturare un approccio efficace alla gestione del Cyber Risk.
- **Policy compliance:** imparerai a implementare e gestire policy di sicurezza conformi agli standard internazionali, tra cui Identity e Access Management, Information Security Event Management e Privacy.



TERZO MODULO
10 ore

7-14-21 novembre
con orario **14.00-17.30**
L'ultima lezione sarà con orario **14.00-17.00**

Ethical Hacking: Come Proteggere i Sistemi dalle Minacce informatiche

In questo corso intensivo, ti immergerai completamente nell'Ethical Hacking, acquisendo una solida conoscenza teorica e pratica delle tecniche utilizzate dagli hacker per penetrare i sistemi informatici.

Cosa imparerai?

- **I concetti base dell'Ethical Hacking:** scoprirai i principi fondamentali dell'hacking etico, le diverse tipologie di hacker e il loro modus operandi.
- **Le principali metodologie di attacco informatico:** apprenderai le tecniche utilizzate dagli hacker per attaccare i sistemi informatici, tra cui scansioni di vulnerabilità, ingegneria sociale, phishing, malware e attacchi DDoS.
- **Strumenti e tecniche di Vulnerability Assessment:** padroneggerai i migliori strumenti e le tecniche utilizzate dai Penetration Tester per identificare e sfruttare le vulnerabilità dei sistemi informatici.
- **Le fasi del Penetration Test:** imparerai a pianificare, eseguire e documentare un Penetration Test completo, dall'engagement iniziale al reporting finale.
- **Come difendersi dagli attacchi informatici:** svilupperai le competenze necessarie per rafforzare la sicurezza dei sistemi informatici e mitigare il rischio di attacchi informatici.

QUARTO MODULO
10 ore

28 novembre e **5-12 dicembre**
con orario **14.00-17.30**
L'ultima lezione sarà con orario **14.00-17.00**

Risposta agli Incidenti e Continuità Operativa: Strumenti e Best Practice

In questo corso immersivo, acquisirai le competenze e gli strumenti necessari per gestire efficacemente gli incidenti di sicurezza informatica nella tua azienda.

Cosa imparerai?

- **Progetta, sviluppa e implementa piani di risposta agli incidenti:** scoprirai le best practice per creare piani di risposta completi e collaudati che ti aiuteranno a minimizzare l'impatto di un incidente informatico.
- **Analizza l'impatto aziendale:** imparerai a valutare le potenziali conseguenze di un incidente informatico sulla tua azienda, in termini di perdite finanziarie, danni alla reputazione e interruzione del servizio.
- **Attua piani di continuità aziendale e disaster recovery:** saprai garantire la continuità operativa della tua azienda in caso di un incidente informatico, grazie a piani di continuità aziendale e disaster recovery ben definiti.
- **Scopri i Framework di riferimento:** approfondirai i principali Framework di riferimento per la gestione degli incidenti informatici, come il NIST Cybersecurity Framework, per allineare le tue pratiche con gli standard del settore.
- **Gestisci Data Breach e Incident Response:** imparerai a gestire efficacemente le violazioni dei dati e gli incidenti di sicurezza, minimizzando i danni e conformandoti alle normative vigenti.

ISCRIZIONE

La partecipazione al percorso formativo è **limitata a 15 persone** per garantire la massima interazione.

I moduli del "Master Cyber Defense" possono essere frequentati singolarmente.

Prezzo **modulo singolo** "Cyber Defense"

Durata: 10 ore

- **660 euro + IVA**

Acquista il **pacchetto completo** "Master Cyber Defense"

Durata: 40 ore

- **2.640 euro + IVA**

Per iscriverti scarica la scheda di adesione nel sito **www.esacformazione.it**
Per maggiori informazioni: tel. **0444 964300** | **info@esacformazione.it**

CONFCOMMERCIO
VICENZA

esac formazione

Centro Formazione Esac
Via Piazzon, 40 - Creazzo
tel. 0444 964300
info@esacformazione.it

www.esacformazione.it