Certified Cybersecurity Technician (CCT)

CODICE	DT0228
DURATA	5 gg
PREZZO	3.500,00 €
EXAM	

DESCRIZIONE

La certificazione C|CT prepara i professionisti dell'IT e della cybersecurity a gestire una vasta gamma di questioni complesse relative alla sicurezza di software, reti e sistemi IT contro le minacce e gli attacchi informatici più comuni. Il corso "Certified Cybersecurity Technician", CCT, offre un approccio sfaccettato che incorpora la difesa della rete, l'hacking etico e le operazioni di sicurezza per garantire che i possessori della certificazione abbiano un background completo che permetta loro di configurare, analizzare e identificare i problemi all'interno di un'organizzazione. Il corso fornisce ai partecipanti le competenze necessarie per i seguenti ruoli:

- IT networking specialist
- Cybersecurity technician
- IT manager
- Network administrator
- Network engineer
- Security operations center (SOC) analyst

Il corso C|CT di EC-Council immerge gli studenti in un concentrato di nozioni ben strutturate. La formazione è accompagnata da sfide di ragionamento critico ed esperienze di laboratorio coinvolgenti che permettono ai candidati di applicare le loro conoscenze e passare alla fase di sviluppo delle abilità nella classe stessa. Al completamento del programma, gli studenti avranno una solida preparazione nei principi e nelle tecniche di cybersecurity così come nella pratica dei compiti richiesti nei lavori del mondo reale.

OBIETTIVI RAGGIUNTI

- Concetti chiave della cybersecurity, compresa la sicurezza delle informazioni e la sicurezza della rete Minacce alla sicurezza delle informazioni, vulnerabilità e attacchi
- I diversi tipi di malware
- Identificazione, autenticazione e autorizzazione.
- Controlli di sicurezza della rete:
    - Controlli amministrativi (leggi, programmi di governance e conformità, politiche di sicurezza)

    - Controlli fisici (politiche di sicurezza fisica e del posto di lavoro, controlli ambientali)
    - Controlli tecnici (network security protocols; network segmentation; firewalls; intrusion detection and prevention systems; honeypots; proxy servers; VPNs; user behavior analytics; network access control; unified threat management; security information and event management; security orchestration, automation, and response; load baancers; anti-malware)
- Tecniche e strumenti di valutazione della sicurezza di rete (threat hunting, threat intelligence, vulnerability assessment, ethical hacking, penetration testing, configuration and asset management)
- Tecniche di progettazione e test della sicurezza delle applicazioni
- Fondamenti di virtualizzazione, cloud computing e sicurezza del cloud
- Fondamenti di rete wireless, crittografia wireless e relative misure di sicurezza. Fondamenti di dispositivi mobili, IoT e OT e relative misure di sicurezza. Crittografia e infrastruttura a chiave pubblica
- Controlli di sicurezza dei dati, metodi di backup e conservazione dei dati e tecniche di prevenzione della perdita di dati. Risoluzione dei problemi di rete, monitoraggio del traffico e dei log e analisi del traffico sospetto
- Il processo di gestione e risposta agli incidenti
- Fondamenti di informatica forense e prove digitali, comprese le fasi di un'indagine forense
- Concetti di continuità aziendale e disaster recovery
- Concetti, fasi e strutture di gestione del rischio

TARGET

Il corso è l'ideale per chiunque desideri iniziare la propria carriera nella sicurezza informatica o raggiungere una solida comprensione dei concetti e delle tecniche di sicurezza informatica necessari per essere efficaci sul posto di lavoro.

PREREQUISTI

Non ci sono prerequisiti obbligatori ma una precedente conoscenza e l'esperienza nell'IT e nel networking con particolare attenzione alla sicurezza informatica è consigliata.

CONTENUTI

- Minacce e vulnerabilità alla sicurezza delle informazioni
- Attacchi alla sicurezza delle informazioni
- Nozioni fondamentali sulla sicurezza della rete
- Identificazione, autenticazione e autorizzazione
- Controlli di sicurezza di rete: controlli amministrativi
- Controlli di sicurezza di rete: controlli fisici
- Controlli di sicurezza di rete: controlli tecnici
- Tecniche e strumenti di valutazione della sicurezza della rete
- Sicurezza delle applicazioni
- Virtualizzazione e cloud computing

- Sicurezza della rete wireless
- Sicurezza dei dispositivi mobili
- Internet of Things (IoT) e sicurezza delle tecnologie operative (OT)
- Crittografia
- Sicurezza dei dati
- Risoluzione dei problemi di rete
- Monitoraggio del traffico di rete
- Monitoraggio e analisi dei registri di rete
- Risposta agli incidenti
- Informatica forense
- Business Continuity e Disaster Recovery
- Gestione del rischio