ECCC-10 - CSA - CERTIFIED SOC ANALYST

Categoria: **EC-Council**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
3 Giorni	EC-Council	Certified EC-Council Instructor	Professionista IT	EC-Council

OBIETTIVI

Il corso Certified SOC Analyst (CSA) è una tappa fondamentale per chi aspira a entrare o avanzare all'interno di un Security Operations Center (SOC), concentrandosi sulle sue funzioni, lo sviluppo e la gestione.
Il corso fornisce formazione sui principi e le pratiche fondamentali delle operazioni di sicurezza, dell'intelligence sulle minacce e della risposta agli incidenti. Fornisce una comprensione approfondita dei processi, delle tecnologie e delle tecniche utilizzate per rilevare, investigare e rispondere alle minacce alla sicurezza.
Il programma copre una serie di argomenti, tra cui i vettori di attacco comuni, l'uso di strumenti e tecnologie di sicurezza, la gestione delle informazioni e degli eventi di sicurezza (SIEM), i processi di risposta agli incidenti, il coordinamento e lo sviluppo di un SOC. Gli studenti acquisiscono competenze nella gestione centralizzata dei log (CLM), nel triage degli incidenti, nel riconoscimento e nell'indagine degli indicatori di compromissione (IOC) e nella cyber kill chain, consentendo loro di rispondere in modo proattivo alle potenziali minacce. Inoltre, acquisiscono la capacità di riconoscere i modelli di minaccia emergenti, sviluppare regole di correlazione e creare report efficaci che aiutino le organizzazioni a mantenere una solida postura di sicurezza. Gli studenti imparano anche a sfruttare gli strumenti e le piattaforme abilitati all'intelligenza artificiale per migliorare le funzionalità SIEM, l'analisi del comportamento e la prioritizzazione degli avvisi, e ad automatizzare il rilevamento e la caccia alle minacce utilizzando soluzioni come Splunk AI, Elastic AI, Copilot, ChatGPT e PowerShell AI.

PREREQUISITI

Il conseguimento preventivo delle certificazioni CND - Certified Network Defender e CEH - Certified Ethical Hacker è consigliato.

CONTENUTI

Modulo 01: Security Operations and Management
Modulo 02: Understanding Cyber Threats, IoCs, and Attack Methodology
Modulo 03: Log Management
Modulo 04: Incident Detection and Triage
Modulo 05: Proactive Threat Detection
Modulo 06: Incident Response
Modulo 07: Forensic Investigation and Malware Analysis
Modulo 08: SOC for Cloud Environments

INFO

Esame: 312-39 - Certified SOC Analyst
Materiale didattico: Materiale didattico ufficiale EC-Council in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)