dgroove

Corso di Formazione

CSA – CERTIDIED SECURITY ANALYST

Impara tutte le operazioni e processi di un SOC!

Il Corso CSA –Certified Soc Analyst ti aiuta ad acquisire le competenze tecniche più richieste grazie all'istruzione da parte di alcuni dei formatori più esperti del settore. Il programma si concentra sui fondamenti delle operazioni SOC, prima di trasmettere la conoscenza della gestione e della correlazione dei log, dell'implementazione SIEM, del rilevamento avanzato degli incidenti e della risposta agli incidenti. Inoltre, il candidato imparerà a gestire vari processi SOC e a collaborare con CSIRT al momento del bisogno. Il corso, inoltre, prepara a sostenere l'esame EC- Council Certified SOC Analyst accreditato ANSI.

Durata: 3 giorni

C|SA
Certified SOC Analyst

Fai parte di un Security Operations Center e vuoi ottenere una certificazione ufficiale?
Con questo corso potrai conoscere tutte le operazioni e i processi di un Centro operativo di sicurezza (SOC).





Obiettivi del corso

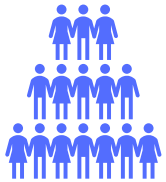
- Acquisire conoscenza dei processi, delle procedure, delle tecnologie e dei flussi di lavoro SOC.
- Ottenere una conoscenza approfondita di minacce alla sicurezza, attacchi, vulnerabilità, comportamenti degli aggressori, cyber killchain, ecc.
- Essere in grado di riconoscere gli strumenti, le tattiche e le procedure degli aggressori per identificare gli indicatori di compromissione (IOC) che possono essere utilizzati durante le indagini attive e future.
- Imparare a monitorare e analizzare log e avvisi da una varietà di tecnologie diverse su più piattaforme (IDS/IPS, protezione degli endpoint, server e workstation).
- Acquisire la conoscenza del processo di gestione centralizzata dei registri (CLM).
- Acquisire conoscenze sull'amministrazione di soluzioni SIEM (Splunk/AlienVault/OSSIM/ELK).
- Comprendere l'architettura, l'implementazione e la messa a punto delle soluzioni SIEM (Splunk/AlienVault/OSSIM/ELK).
- Acquisire esperienza pratica nel processo di valutazione degli avvisi.
- Utilizzare un sistema di ticketing Service Desk.
- Acquisire conoscenze sull'integrazione dell'intelligence sulle minacce in SIEM per una migliore rilevazione e risposta agli incidenti.
- Acquisire conoscenza del processo di risposta agli incidenti.

Programma





- Modulo 1 – Operazioni e gestione della sicurezza
- Modulo 2 – Comprensione delle minacce informatiche, degli IoC e della metodologia di attacco
- Modulo 3 – Incidenti, eventi e registrazione
- Modulo 4 – Rilevamento di incidenti con informazioni sulla sicurezza e gestione degli eventi (SIEM)
- Modulo 5 – Rilevamento avanzato degli incidenti con Threat Intelligence
- Modulo 6 – Risposta agli incidenti



A chi è rivolto

- Analisti SOC (Tier I e Tier II);
- amministratori di rete e sicurezza;
- ingegneri di rete e sicurezza;
- analista della difesa della rete;
- tecnici della difesa della rete;
- specialista della sicurezza della rete;
- operatore della sicurezza della rete e qualsiasi professionista della sicurezza che gestisce le operazioni di sicurezza della rete;
- analista di sicurezza informatica;
- professionisti della sicurezza informatica di livello base;
- chiunque voglia diventare un analista SOC.

Chi siamo

Da oltre 30 anni, Dgroove, si occupa di *digital trasformation* con l'obiettivo di creare una relazione fluida e produttiva tra tecnologie e persone. Con le sue soluzioni e percorsi di formazione IT accompagna e supporta le aziende clienti nel miglioramento e ottimizzazione dei processi aziendali prestando particolare attenzione alle risorse umane e alla loro crescita professionale.

Insieme a PCSnet, organizza corsi di formazione sia in ambito IT che sulle professionalità aziendali in generale.

Fornisce formazione certificata sui principali *vendor* tecnologici: è Microsoft Partner Learning da più di 20 anni, eroga i corsi ufficiali della Oracle University, corsi personalizzati VMware, Cisco, ed EC-Council (come ad esempio Certified Ethical Hacker).

I corsi sono tenuti da docenti professionisti che non si limitano a conoscere la materia ma la mettono in pratica nella quotidianità delle realtà aziendali. Proprio per questa ragione ogni corso ha un approccio fortemente tecnico pratico.



Microsoft

www.dgroove.it