Certnexus - CyberSec First Responder

Kód kurzu: CFR

Tento kurz pokrýva metódy, taktiky a postupy na obranu siete a reakcie na incidenty, ktoré sú v súlade s priemyselnými rámcami, ako je NIST 800-61r2 (Sprievodca riešením incidentov v oblasti počítačovej bezpečnosti), Národný plán reakcie na kybernetické incidenty (NCIRP) US-CERT a prezidentská politika. Smernica (PPD)-41 o koordinácii kybernetických incidentov, NIST 800.171r2 (Ochrana kontrolovaných neutajovaných informácií v nefederálnych systémoch a organizáciách). Je ideálny pre kandidátov, ktorí majú za úlohu monitorovať a odhaľovať bezpečnostné incidenty v informačných systémoch a sieťach a vykonávať štandardizované reakcie na takéto incidenty. Kurz predstavuje nástroje, taktiky a postupy na riadenie rizík kybernetickej bezpečnosti, obranu aktív kybernetickej bezpečnosti, identifikáciu rôznych typov bežných hrozieb, hodnotenie bezpečnosti organizácie, zhromažďovanie a analýzu spravodajských informácií o kybernetickej bezpečnosti a nápravu a hlásenie incidentov, keď sa vyskytnú. Tento kurz poskytuje komplexnú metodiku pre jednotlivcov zodpovedných za obranu kybernetickej bezpečnosti ich organizácie.Tento kurz je navrhnutý tak, aby pomohol študentom pripraviť sa na certifikačnú skúšku CertNexus CyberSec First Responder (skúška CFR-410). To, čo sa naučíte a precvičíte v tomto kurze, môže byť významnou súčasťou vašej prípravy.Okrem toho tento kurz a následná certifikácia (CFR-410) spĺňajú všetky požiadavky na personál vyžadujúci základnú certifikáciu pozícií podľa smernice DoD 8570.01-M:- analytik CSSP- Podpora infraštruktúry CSSP- Odpovedač na incidenty CSSP- audítor CSSP

Pre koho je kurz určený

Tento kurz je určený predovšetkým pre odborníkov v oblasti kybernetickej bezpečnosti, ktorí sa pripravujú alebo v súčasnosti vykonávajú pracovné funkcie súvisiace s ochranou informačných systémov zabezpečením ich dostupnosti, integrity, autentifikácie, dôvernosti a neodvolateľnosti. Je ideálny pre tie úlohy v rámci federálnych zmluvných spoločností a firiem zo súkromného sektora, ktorých poslanie alebo strategické ciele vyžadujú vykonávanie operácií defenzívnych kybernetických operácií (DCO) alebo informačnej siete DoD (DoDIN) a riešenie incidentov. Tento kurz sa zameriava na znalosti, schopnosti a zručnosti potrebné na zabezpečenie obrany týchto informačných systémov v kontexte kybernetickej bezpečnosti, vrátane procesov ochrany, detekcie, analýzy, vyšetrovania a reakcie.
Okrem toho kurz zabezpečuje, že všetci členovia IT tímu – bez ohľadu na veľkosť, hodnosť alebo rozpočet – rozumejú svojej úlohe v procese kybernetickej obrany, reakcie na incidenty a riešenia incidentov.

Čo Vás naučíme

V tomto kurze budete identifikovať, hodnotiť, reagovať a chrániť pred bezpečnostnými hrozbami a prevádzkovať platformu na analýzu bezpečnosti systému a siete.
Budete vedieť:

- Posúdiť riziká kybernetickej bezpečnosti pre organizáciu
- Analyzovať prostredie hrozieb
- Analyzovať rôzne prieskumné hrozby pre počítačové a sieťové prostredia
- Analyzovať rôzne útoky na počítačové a sieťové prostredia
- Analyzovať rôzne techniky po útoku
- Zhodnotiť stav zabezpečenia organizácie prostredníctvom auditu, správy zraniteľnosti a penetračného testovania
- Zbierať informácie o kybernetickej bezpečnosti z rôznych sieťových a hostiteľských zdrojov
- Analyzovať údaje denníka a odhaliť dôkazy o hrozbách a incidentoch
- Vykonať analýzu aktívneho majetku a siete na zistenie incidentov
- Reagovať na incidenty kybernetickej bezpečnosti pomocou taktiky obmedzovania, zmierňovania a obnovy
- Vyšetriť incidenty kybernetickej bezpečnosti pomocou techník forenznej analýzy

Požadované vstupné znalosti

Aby ste v tomto kurze uspeli, mali by ste splniť nasledujúce požiadavky:

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Minimálne dvojročná prax (odporúča sa) alebo vzdelanie v bezpečnostnej technike počítačových sietí alebo v príbuznom odbore
- Schopnosť alebo zvedavosť rozpoznať zraniteľné miesta a hrozby informačnej bezpečnosti v kontexte riadenia rizík
- Základná znalosť konceptov a operačného rámca spoločných bezpečnostných záruk v sieťových prostrediach. Ochranné opatrenia zahŕňajú, ale nie sú obmedzené na firewally, systémy prevencie narušenia a VPN
- Všeobecná znalosť koncepcií a operačného rámca spoločných bezpečnostných záruk vo výpočtovom prostredí. Ochranné opatrenia zahŕňajú, ale nie sú obmedzené na základné overenie a autorizáciu, povolenia zdrojov a mechanizmy proti malvéru
- Zručnosti na základnej úrovni s niektorými bežnými operačnými systémami pre výpočtové prostredia
- Základné pochopenie niektorých bežných konceptov pre sieťové prostredia, ako je smerovanie a prepínanie
- Všeobecné alebo praktické znalosti hlavných sieťových protokolov TCP/IP vrátane, ale nie výlučne, TCP, IP, UDP, DNS, HTTP, ARP, ICMP a DHCP

Študijné materiály

Oficiálna príručka pre tento kurz

Osnova kurzu

Lekcia 1: Hodnotenie rizika kybernetickej bezpečnosti

- Identifikácia dôležitosti riadenia rizík
- Posúdenie rizika
- Zmiernenie rizika
- Integrácia dokumentácie do riadenia rizík

Lekcia 2: Analýza krajiny hrozieb

- Klasifikovať hrozby
- Analýza trendov ovplyvňujúcich pozíciu bezpečnosti

Lekcia 3: Analýza hrozieb prieskumu pre počítačové a sieťové prostredia

- Implementácia a modelovanie hrozieb
- Posúdenie vplyvu prieskumu
- Posúdenie vplyvu sociálneho inžinierstva

Lekcia 4: Analýza techník po útoku

- Posúdenie vplyvu útokov hackerov na systém
- Posúdenie vplyvu webových útokov
- Posúdenie vplyvu malvéru
- Posúdenie vplyvu útokov únosov a odcudzenia identity
- Posúdenie vplyvu incidentov DoS
- Posúdenie vplyvu hrozieb na mobilnú bezpečnosť
- Posúdenie vplyvu hrozieb na bezpečnosť cloudu

Lekcia 5: Analýza útokov na počítačové a sieťové prostredia

- Posúdenie techník velenia a riadenia
- Posúdenie techník vytrvalosti
- Posúdenie techník laterálneho pohybu a otáčania
- Posúdenie techník exfiltrácie údajov
- Posúdenie antiforenzných techník

Lekcia 6: Hodnotenie bezpečnostnej pozície organizácie

- Implementovať audit kybernetickej bezpečnosti
- Implementovať plán riadenia zraniteľnosti
- Posúdiť zraniteľné miesta

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Vykonať penetračný test

Lekcia 7: Zhromažďovanie informácií o kybernetickej bezpečnosti
- Nasadiť platformu na zhromažďovanie a analýzu bezpečnostných informácií
- Zbieranie údajov zo sieťových spravodajských zdrojov
- Zbieranie údajov z hostiteľských spravodajských zdrojov

Lekcia 8: Analýza údajov protokolu
- Používanie bežných nástrojov na analýzu protokolov
- Použitie nástrojov SIEM na analýzu

Lekcia 9: Vykonávanie analýzy aktívneho majetku a siete
- Analýza incidentov pomocou nástrojov systému Windows
- Analýza incidentov pomocou nástrojov založených na systéme Linux
- Analýza indikátorov kompromisu

Lekcia 10: Reakcia na incidenty kybernetickej bezpečnosti
- Nasadiť architektúru spracovania incidentov a odozvy
- Zmierňovanie incidentov
- Odovzdanie informácií o incidente forenznému vyšetrovaniu

Lekcia 11: Vyšetrovanie incidentov kybernetickej bezpečnosti
- Použitie plánu forenzného vyšetrovania
- Bezpečné zbieranie a analýza elektronických dôkazov
- Sledovanie výsledkov vyšetrovania

Príloha A: Mapovanie obsahu kurzu na CyberSec First Responder® (skúška CFR-410)

Príloha B: Regulárne výrazy

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk