Certnexus - Incident Response pre manažérov

Kód kurzu: IRBIZ

Tento kurz pokrýva metódy a postupy reakcie na incidenty, ktoré sa vyučujú v súlade s priemyselnými rámcami, ako je NCISP (Národný plán reakcie na kybernetické incidenty) od US-CERT a Smernica prezidentskej politiky (PPD) 41 o politike koordinácie kybernetických incidentov. Je ideálny pre uchádzačov, ktorí sú zodpovední za dodržiavanie právnych predpisov a iných regulačných požiadaviek týkajúcich sa reakcií na incidenty a za vykonávanie štandardizovaných opatrení pri takýchto incidentoch.Kurz predstavuje postupy a prostriedky na splnenie legislatívnych požiadaviek týkajúcich sa reakcie na incidenty. Tento kurz je určený na pomoc študentom pri príprave na CertNexus Incident Responder Credential (CIR-110). To, čo sa naučíte a precvičíte v tomto kurze, môže byť významnou súčasťou vašej prípravy.

Pre koho je kurz určený

Tento kurz je určený predovšetkým pre IT lídrov a manažérov spoločností, ktorí sú zodpovední za dodržiavanie legislatívy v oblasti reakcie na incidenty. Zameriava sa na znalosti, zdroje a zručnosti, ktoré sú potrebné na splnenie požiadaviek k reakcii na incidenty a proces spracovania incidentov.

Čo Vás naučíme

V tomto kurze pochopíte, vyhodnotíte a budete vedieť reagovať na bezpečnostné hrozby a tiež prevádzkovať platformu na analýzu bezpečnosti systému a siete.

Naučíte sa:

- Vysvetliť dôležitosť osvedčených postupov pri príprave na reakciu na incidenty
- Vzhľadom na scenár budete vedieť vykonať proces reakcie na incident
- Vysvetliť všeobecné metódy a dokázať zmierniť riziko
- Posudzovať a dodržiavať aktuálne požiadavky k reakcii na incidenty

Požadované vstupné znalosti

Všeobecné chápanie pojmov kybernetickej bezpečnosti

Študijné materiály

Oficiálna príručka pre tento kurz

Osnova kurzu

Lekcia 1: Hodnotenie rizík informačnej bezpečnosti

- Význam riadenia rizík
- Integrácia dokumentácie do riadenia rizík

Lekcia 2: Reakcia na incidenty kybernetickej bezpečnosti

- Nasadenie architektúry spracovania incidentov a odozvy
- Zadržiavanie a zmierňovanie incidentov
- Príprava na forenzné vyšetrovanie ako CSIRT

Lekcia 3: Vyšetrovanie kybernetických bezpečnostných incidentov

- Používanie plánu forenzného vyšetrovania
- Bezpečné zbieranie a analýza elektronických dôkazov
- Téma C: Sledovanie výsledkov vyšetrovania

Lekcia 4: Dodržiavanie legislatívy

- Príklady legislatívy (ak je to zahrnuté vo vyššie uvedených témach, tu nie je potrebné uvádzať) GDPR, HIPPA, voľby
- Prípadová štúdia: Reakcia na incidenty a GDPR (pomocou legislatívy GDPR tvorba odpovedí, ktorá je s ňou v súlade – môže ísť aj o aktivitu založenú na diskusii)
- Zdroje a príklady štátnej legislatívy – hľadanie výrazov na nájdenie štátnej legislatívy

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

- Použitie NYS ako príklad NYS Privacy Response akt alebo iný zákon na vytvorenie podobnej prípadovej štúdie ako predchádzajúcej
- Poskytnutie odpovedí na otázku kedy použiť "federálne" a kedy "štátne", či sledovať obe?

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