Vzdelávací program: Špecialista pre riešenie kybernetických incidentov

Profil absolventa

Absolvent vzdelávacieho programu „Špecialista pre riešenie kybernetických incidentov“ je odborník schopný detegovať, analyzovať, mitigovať a dokumentovať kybernetické bezpečnostné incidenty. Disponuje hĺbkovými vedomosťami o sieťových technológiách, kryptografických mechanizmoch, forenznej analýze a procesoch riadenia rizík. Je pripravený koordinovať reakcie na incidenty, podporovať plánovanie kontinuity činností a obnovy po havárii, ako aj spolupracovať s orgánmi verejnej moci. Absolvent kombinuje technické zručnosti s analytickým a strategickým myslením na zabezpečenie ochrany informačných aktív organizácie.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
    - Ovláda procesy riadenia kybernetickej bezpečnosti, sieťových technológií (napr. model OSI, protokoly) a forenznej analýzy (BL 2–6).
    - Rozumie kryptografickým mechanizmom, správe dát a bezpečnostným štandardom (napr. PCI, klasifikácia údajov) (BL 4–6).
    - Pozná princípy riadenia rizík, identifikácie hrozieb (napr. phishing, malware) a reakcie na incidenty (BL 5–6).
    - Chápe podnikové architektúry (napr. TOGAF), operačné systémy, virtualizáciu a cloudové prostredia (BL 4–6).
    - Má prehľad o právnych predpisoch a normách týkajúcich sa kybernetickej bezpečnosti a ochrany údajov (BL 3–5).
    - Rozumie štádiám kybernetických útokov, analýze sieťového prenosu a konfigurácii bezpečnostných systémov (BL 6).
2. **Zručnosti**:
    - Deteguje, analyzuje a rieši kybernetické bezpečnostné incidenty.
    - Navrhuje a implementuje opatrenia na mitigáciu rizík a prevenciu incidentov.
    - Koordinuje procesy obnovy prevádzky (Business Continuity, Disaster Recovery).
    - Analyzuje sieťový prenos a spracováva digitálne stopy pomocou nástrojov (napr. Wireshark, VMWare).
    - Implementuje bezpečnostné mechanizmy (napr. šifrovanie, VPN, hardening systémov).
    - Spolupracuje s audítormi a orgánmi činnými v trestnom konaní.
3. **Postoje**:
    - Proaktívny a zodpovedný prístup k riešeniu bezpečnostných incidentov.
    - Etické správanie pri manipulácii s citlivými údajmi a dôkazmi.
    - Objektivita pri analýze incidentov a koordinácii reakcií.
    - Schopnosť efektívne komunikovať technické zistenia netechnickému publiku.
4. **Špecifické kompetencie**:
    - Schopnosť prijímať rozhodnutia a myslieť v súvislostiach.
    - Analytické myslenie a tvorivosť pri navrhovaní riešení.

- Organizačné zručnosti pri koordinácii reakcií na incidenty.

Požiadavky na vstup:

- **Vzdelanie**: Úplné stredné všeobecné alebo odborné, vysokoškolské I., II. alebo III. stupňa.
- **Odborná prax**: Nie je špecifikovaná konkrétna dĺžka praxe, avšak odporúča sa skúsenosť v oblasti IT, kybernetickej bezpečnosti alebo forenznej analýzy.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické, praktické a operatívne metódy zamerané na rozvoj zručností v riešení kybernetických incidentov:

1. **Interaktívne prednášky**:
   - Vysvetlenie procesov riadenia incidentov, sieťových technológií, kryptografických mechanizmov a právnych rámcov.
   - Diskusie o štádiách kybernetických útokov, logovaní a bezpečnostnom monitorovaní.
2. **Praktické laboratóriá**:
   - Simulácie kybernetických incidentov (napr. DDoS, malware) a nácvik reakcií.
   - Analýza sieťového prenosu a spracovanie digitálnych stôp pomocou nástrojov ako Wireshark.
   - Konfigurácia bezpečnostných mechanizmov (napr. firewally, IDS/IPS) a hardening systémov.
3. **Prípadové štúdie**:
   - Analýza reálnych alebo hypotetických incidentov a návrh plánov reakcie a obnovy.
   - Skupinové projekty na koordináciu reakcie na incident a dokumentáciu zistení.
4. **Workshopy a simulácie**:
   - Role-playing scenáre na koordináciu tímu pri riešení incidentu.
   - Workshopy na implementáciu opatrení a komunikáciu s orgánmi verejnej moci.
5. **E-learning a samoštúdium**:
   - Prístup k online kurzom a certifikačným prípravám (napr. CEH, GCIH) zameraným na riešenie incidentov.
   - Interaktívne moduly na precvičenie analýzy rizík, šifrovania a správy sietí.
6. **Mentorované projekty**:
   - Samostatné projekty na vypracovanie plánu reakcie na incident alebo forenznej správy.
   - Mentorovanie zamerané na rozvoj analytických a koordinačných zručností.

Forma vzdelávania

Program je navrhnutý ako kombinovaný, aby vyhovoval odborníkom s technickým zameraním:

1. **Prezenčná forma**:

    - Intenzívne školenia v technologických laboratóriách vybavených na simuláciu incidentov a forenznej analýzy.
    - Vhodné na praktické cvičenia, workshopy a tímové projekty.
    - Trvanie: 4 dni.
2. **Online forma**:
    - Vzdelávanie cez bezpečné videokonferenčné platformy s dôrazom na teoretické prednášky a analýzy.
    - Prístup k e-learningovým platformám s nahratými prednáškami a samoštudijnými materiálmi.
    - Vhodné pre samoštúdium a vzdialený prístup.
3. **Kombinovaná forma**:
    - Kombinácia prezenčných laboratórií (napr. na simulácie incidentov) a online samoštúdia.
    - Účastníci absolvujú praktické cvičenia na mieste a teoretickú časť online, čo zvyšuje flexibilitu.

Metódy hodnotenia

Hodnotenie je zamerané na overenie teoretických vedomostí, operatívnych zručností a schopnosti reagovať na incidenty:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na sieťové technológie, kryptografiu, riadenie incidentov a právne normy.
    - Formát: výber z možností, esejové otázky, analýza scenárov.
2. **Praktické úlohy**:
    - Simulácia reakcie na kybernetický incident (napr. detekcia a mitigácia útoku).
    - Analýza sieťového prenosu a vypracovanie správy o incidente.
    - Hodnotí sa technická presnosť, rýchlosť reakcie a súlad s metodikami.
3. **Prípadové štúdie**:
    - Analýza hypotetického alebo reálneho incidentu a návrh plánu reakcie a obnovy.
    - Hodnotí sa schopnosť identifikovať príčiny, navrhnúť opatrenia a dokumentovať zistenia.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia plánu reakcie na incident alebo forenznej správy pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť riešenia.
5. **Simulácie**:
    - Simulácia koordinácie tímu pri riešení kybernetického incidentu.
    - Hodnotí sa schopnosť riadiť reakciu, komunikovať s orgánmi a koordinovať obnovu.

Kritériá úspešnosti:

- Úspešné absolvovanie programu vyžaduje dosiahnutie minimálne 80 % úspešnosti v znalostných testoch, praktických úlohách a simuláciách.
- Účastníci obdržia certifikát o absolvovaní programu po splnení všetkých požiadaviek.

Záver

Vzdelávací program „Špecialista pre riešenie kybernetických incidentov“ pripravuje odborníkov na efektívne zvládanie bezpečnostných incidentov v dynamickom IT prostredí. Kombinácia teoretických prednášok, praktických laboratórií a simulácií zaisťuje, že absolventi sú schopní detegovať, analyzovať a mitigovať incidenty, podporovať obnovu prevádzky a spolupracovať s orgánmi pri vyšetrovaní.