Vzdelávací program: Špecialista pre analýzu digitálnych stôp

Profil absolventa

Absolvent vzdelávacieho programu „Špecialista pre analýzu digitálnych stôp“ je odborník schopný identifikovať, zhromažďovať, analyzovať a interpretovať digitálne stopy v rámci forenznej analýzy kybernetických incidentov. Disponuje hĺbkovými vedomosťami o sieťových technológiách, kryptografických mechanizmoch, operačných systémoch a bezpečnostných procesoch. Je pripravený na detekciu a riešenie bezpečnostných incidentov, spoluprácu s orgánmi činnými v trestnom konaní a podporu auditu kybernetickej bezpečnosti. Absolvent kombinuje technické a analytické zručnosti na zabezpečenie ochrany informačných aktív a efektívne spracovanie digitálnych dôkazov.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
   - Ovláda princípy organizácie kybernetickej bezpečnosti, sieťových technológií (napr. model OSI, protokoly) a forenznej analýzy (BL 4–6).
   - Rozumie kryptografickým mechanizmom, správe dát a bezpečnostným štandardom (napr. PCI, klasifikácia údajov) (BL 5–6).
   - Pozná procesy riadenia rizík, detekcie hrozieb a reakcie na incidenty (BL 5–6).
   - Chápe architektúru operačných systémov, sieťových zariadení, databáz a nových technológií (napr. cloud, virtualizácia) (BL 5–6).
   - Má prehľad o právnych predpisoch a normách týkajúcich sa kybernetickej bezpečnosti a ochrany údajov (BL 3–5).
   - Rozumie postupom identifikácie digitálnych stôp, analýze sieťového prenosu a konfigurácii forenzných nástrojov (BL 6).
2. **Zručnosti**:
   - Identifikuje a spracováva digitálne stopy v rámci forenznej analýzy.
   - Deteguje, rieši a eviduje kybernetické bezpečnostné incidenty.
   - Analyzuje sieťový prenos a posudzuje zraniteľnosti systémov (napr. pomocou Wireshark, VMWare).
   - Implementuje bezpečnostné mechanizmy (napr. šifrovanie, VPN, hardening systémov).
   - Spolupracuje s audítormi a orgánmi verejnej moci pri vyšetrovaní incidentov.
   - Podporuje riadenie bezpečnosti a budovanie bezpečnostného povedomia.
3. **Postoje**:
   - Etický a zodpovedný prístup k spracovaniu digitálnych dôkazov.
   - Proaktívne riešenie bezpečnostných incidentov a mitigácia rizík.
   - Objektivita pri analýze dát a spolupráci s orgánmi.
   - Schopnosť efektívne komunikovať technické zistenia netechnickému publiku.
4. **Špecifické kompetencie**:
   - Analytické myslenie a schopnosť myslieť v súvislostiach.
   - Tvorivosť pri navrhovaní forenzných postupov.
   - Prezentačné zručnosti pri obhajobe zistení a odporúčaní.

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, forenznej analýzy alebo kybernetickej bezpečnosti.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické, praktické a forenzné metódy zamerané na rozvoj zručností v analýze digitálnych stôp:

1. **Interaktívne prednášky**:
    - Vysvetlenie sieťových protokolov, kryptografických mechanizmov, forenznej analýzy a právnych rámcov.
    - Diskusie o štádiách kybernetických útokov, logovaní a bezpečnostnom monitorovaní.
2. **Praktické laboratóriá**:
    - Analýza sieťového prenosu pomocou nástrojov ako Wireshark a konfigurácia forenzných prostredí (napr. VMWare).
    - Simulácie kybernetických incidentov a spracovanie digitálnych stôp (napr. analýza logov, súborových systémov).
    - Nácvik hardeningu systémov a implementácie bezpečnostných mechanizmov.
3. **Prípadové štúdie**:
    - Analýza reálnych alebo hypotetických kybernetických incidentov a identifikácia digitálnych stôp.
    - Skupinové projekty na vytvorenie forenznej správy alebo plánu reakcie na incident.
4. **Workshopy a simulácie**:
    - Simulácie forenznej analýzy (napr. získanie dát z disku, analýza e-mailov).
    - Role-playing scenáre na spoluprácu s orgánmi činnými v trestnom konaní.
5. **E-learning a samoštúdium**:
    - Prístup k online kurzom a certifikačným prípravám (napr. CHFI, CEH) zameraným na forenznú analýzu.
    - Interaktívne moduly na precvičenie analýzy sietí, šifrovania a správy dát.
6. **Mentorované projekty**:
    - Samostatné projekty na spracovanie digitálnych stôp a vypracovanie forenznej správy.
    - Mentorovanie zamerané na rozvoj technických a analytických zručností.

Forma vzdelávania

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

1. **Prezenčná forma**:
    - Intenzívne školenia v technologických laboratóriách vybavených na forenznú analýzu a simuláciu incidentov.
    - Vhodné na praktické cvičenia, workshopy a tímové projekty.

    - Trvanie: 3 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 forenzne analýzy) 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, forenzných zručností a schopnosti analyzovať digitálne stopy:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na sieťové technológie, kryptografiu, forenznú analýzu a právne normy.
    - Formát: výber z možností, otázky, analýza scenárov.
2. **Praktické úlohy**:
    - Analýza digitálnych stôp v simulačnom prostredí (napr. získanie dát z disku, analýza sieťového prenosu).
    - Konfigurácia forenzných nástrojov a vypracovanie forenznej správy.
    - Hodnotí sa technická presnosť a súlad s metodikami.
3. **Prípadové štúdie**:
    - Analýza hypotetického kybernetického incidentu a identifikácia digitálnych dôkazov.
    - Hodnotí sa schopnosť spracovať stopy, navrhnúť opatrenia a dokumentovať zistenia.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia forenznej správy alebo analýzy incidentu pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť zistenia.
5. **Simulácie**:
    - Simulácia reakcie na kybernetický incident s dôrazom na forenznú analýzu a koordináciu.
    - Hodnotí sa schopnosť identifikovať stopy, analyzovať dáta a komunikovať s orgánmi.

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 analýzu digitálnych stôp“ pripravuje odborníkov na efektívne spracovanie digitálnych dôkazov a reakciu na kybernetické incidenty. Kombinácia teoretických prednášok, praktických laboratórií a forenzných simulácií zaisťuje, že absolventi sú schopní analyzovať digitálne stopy, podporovať bezpečnostné procesy a spolupracovať s orgánmi pri vyšetrovaní.