Vzdelávací program: Analytik kybernetickej bezpečnosti

Profil absolventa

Absolvent vzdelávacieho programu „Analytik kybernetickej bezpečnosti“ je vysoko kvalifikovaný odborník schopný strategicky analyzovať, riadiť a optimalizovať procesy kybernetickej bezpečnosti v organizácii. Disponuje hĺbkovými vedomosťami o riadení bezpečnosti, analýze rizík, bezpečnostných mechanizmoch a súlade s právnymi predpismi. Je pripravený vypracovávať bezpečnostné stratégie, koordinovať tímy, navrhovať rozpočty a podporovať audity. Absolvent kombinuje analytické, strategické a riadiace zručnosti na zabezpečenie ochrany informačných aktív a efektívne riadenie bezpečnostných procesov.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
   - Ovláda procesy riadenia kybernetickej bezpečnosti, vrátane fyzickej a objektovej bezpečnosti (BL 5–6).
   - Rozumie terminológii, štandardom (napr. TOGAF, CMMI, PCI) a právnym rámcom (napr. GDPR, ISO) (BL 5–6).
   - Pozná princípy riadenia IT služieb, podnikových architektúr, rozpočtovania a plánovania zdrojov (BL 5–6).
   - Chápe procesy riadenia rizík, analýzy hrozieb, kontinuity činností a obnovy po havárii (BL 4–6).
   - Má prehľad o sieťových technológiách, kryptografických mechanizmoch, cloudových prostrediach a operačných systémoch (BL 3–5).
   - Rozumie vzdelávacím stratégiám a budovaniu bezpečnostného povedomia (BL 6).
2. **Zručnosti**:
   - Strategicky riadi kybernetickú bezpečnosť a vypracováva bezpečnostné stratégie a dokumentáciu.
   - Implementuje procesy riadenia rizík, hrozieb a bezpečnostných opatrení.
   - Koordinuje tímy, audity a spoluprácu s dodávateľmi a orgánmi verejnej moci.
   - Navrhuje rozpočty, monitoruje efektivitu opatrení a riadi projekty kybernetickej bezpečnosti.
   - Podporuje plánovanie kontinuity činností a obnovy po havárii.
   - Aplikuje metodiky klasifikácie aktív a riadenia identít.
3. **Postoje**:
   - Proaktívny a strategický prístup k riadeniu bezpečnosti a ochrane údajov.
   - Zodpovednosť za súlad s právnymi normami a bezpečnostnými politikami.
   - Etické správanie pri správe citlivých informácií a vedení tímov.
   - Schopnosť efektívne komunikovať s vedením, audítormi a zamestnancami.
4. **Špecifické kompetencie**:
   - Schopnosť prijímať rozhodnutia, riešiť konflikty a delegovať úlohy.
   - Analytické, strategické a koncepčné myslenie.
   - Prezentačné zručnosti a schopnosť viesť vzdelávacie programy.
   - Tvorivosť pri tvorbe bezpečnostných riešení a organizácia práce.

Požiadavky na vstup:

- **Vzdelanie**: Úplné stredné všeobecné alebo odborné, vysokoškolské I., II. alebo III. stupňa.
- **Odborná prax**:
    - Minimálne 3–7 rokov praxe v oblasti IT, z toho 1–5 rokov v riadení IT služieb, informačnej bezpečnosti, riadenia rizík alebo IT architektúry.
    - Medzinárodný certifikát (napr. CISSP, CISM) sa považuje za 1 rok praxe.

Metódy vzdelávania

Vzdelávací program kombinuje strategické, teoretické a praktické metódy zamerané na rozvoj analytických a riadiacich zručností:

1. **Interaktívne prednášky**:
    - Vysvetlenie procesov riadenia bezpečnosti, analýzy rizík, podnikových architektúr a právnych rámcov (napr. GDPR, ISO).
    - Diskusie o štandardoch (napr. TOGAF, CMMI) a metrikách (KPI, KRI).
2. **Praktické workshopy**:
    - Simulácie analýzy rizík a reakcií na kybernetické incidenty.
    - Nácvik tvorby bezpečnostných stratégií, rozpočtov a plánov obnovy po havárii.
    - Cvičenia na koordináciu tímov a delegovanie úloh.
3. **Prípadové štúdie**:
    - Analýza reálnych alebo hypotetických bezpečnostných scenárov a návrh stratégií.
    - Skupinové projekty na tvorbu bezpečnostnej dokumentácie alebo plánu kontinuity.
4. **E-learning a samoštúdium**:
    - Prístup k online kurzom, certifikačným prípravám (napr. CISM, CRISC) a materiálom o compliance.
    - Interaktívne moduly na precvičenie riadenia rizík, monitorovania metrík a správy sietí.
5. **Mentorované projekty**:
    - Samostatné alebo tímové projekty na návrh bezpečnostnej stratégie alebo analýzu rizík.
    - Mentorovanie zamerané na rozvoj strategického myslenia a prezentačných zručností.
6. **Role-playing a simulácie**:
    - Simulácie krízového manažmentu a koordinácie reakcií na incidenty.
    - Cvičenia na komunikáciu s vedením, audítormi a orgánmi verejnej moci.

Forma vzdelávania

Program je navrhnutý ako kombinovaný, aby vyhovoval analytikom s náročným pracovným harmonogramom:

1. **Prezenčná forma**:

    - Intenzívne workshopy v školiacich centrách, zamerané na strategické plánovanie a tímové aktivity.
    - Trvanie: 3 dni.
2. **Online forma**:
    - Videokonferenčné školenia cez bezpečné platformy s dôrazom na teoretické prednášky a diskusie.
    - Prístup k e-learningovým platformám s nahratými prednáškami a samoštudijnými materiálmi.
    - Vhodné pre samoštúdium a vzdialený prístup.
3. **Kombinovaná forma**:
    - Kombinácia prezenčných workshopov (napr. na strategické projekty) a online samoštúdia.
    - Účastníci absolvujú praktické cvičenia na mieste a teoretickú časť online, čo zvyšuje flexibilitu.

Metódy hodnotenia

Hodnotenie je zamerané na overenie strategických, analytických a praktických kompetencií:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na riadenie rizík, právne normy, podnikové architektúry a bezpečnostné mechanizmy.
    - Formát: otázky, výber z možností, analýza scenárov.
2. **Praktické projekty**:
    - Vypracovanie bezpečnostnej stratégie, rozpočtu alebo plánu obnovy po havárii.
    - Návrh metrík (KPI/KRI) a analýza rizík pre modelovú organizáciu.
    - Hodnotí sa strategický prístup, presnosť a súlad s normami.
3. **Prípadové štúdie**:
    - Analýza komplexného bezpečnostného incidentu a návrh riadiacich opatrení.
    - Hodnotí sa schopnosť identifikovať riziká, navrhnúť riešenia a koordinovať reakcie.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia bezpečnostnej stratégie alebo analýzy pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť návrhy.
5. **Simulácie riadenia**:
    - Simulácia krízového manažmentu s dôrazom na koordináciu tímu a komunikáciu.
    - Hodnotí sa rozhodovanie, delegovanie a efektivita riadenia.

Kritériá úspešnosti:

- Úspešné absolvovanie programu vyžaduje dosiahnutie minimálne 85 % úspešnosti v znalostných testoch, projektoch a simuláciách.
- Účastníci obdržia certifikát o absolvovaní programu po splnení všetkých požiadaviek.

Záver

Vzdelávací program „Analytik kybernetickej bezpečnosti“ pripravuje odborníkov na strategické riadenie a analýzu bezpečnostných procesov v komplexných IT prostrediach. Kombinácia teoretických prednášok, praktických workshopov, projektov a simulácií zaisťuje, že absolventi sú schopní navrhovať efektívne bezpečnostné stratégie, riadiť riziká a podporovať súlad s právnymi a technickými normami.