Vzdelávací program: Špecialista riadenia rizík

Profil absolventa

Absolvent vzdelávacieho programu „Špecialista riadenia rizík“ je odborník schopný identifikovať, analyzovať a mitigovať bezpečnostné riziká v oblasti informačných a komunikačných technológií. Disponuje hĺbkovými vedomosťami o procesoch riadenia rizík, kybernetických hrozbách, bezpečnostných mechanizmoch a súlade s právnymi predpismi. Je pripravený navrhovať a implementovať opatrenia na ošetrenie rizík, podporovať bezpečnostné stratégie a participovať na plánovaní kontinuity činností a obnovy po havárii. Absolvent kombinuje analytické myslenie a strategické zručnosti na zabezpečenie ochrany informačných aktív organizácie.

Kľúčové kompetencie absolventa:

1. **Vedomosti**:
    - Ovláda procesy riadenia kybernetickej bezpečnosti, vrátane fyzickej a objektovej bezpečnosti (BL 4–5).
    - Rozumie terminológii, štandardom (napr. KPI, KRI, CMMI) a metodikám klasifikácie údajov (BL 4–5).
    - Pozná princípy riadenia IT služieb, sietí, operačných technológií (OT/ICS) a základov Business Continuity Management (BL 3–5).
    - Chápe procesy analýzy rizík, identifikácie hrozieb (napr. phishing, malware) a návrhu opatrení (BL 4–6).
    - Má prehľad o sieťových protokoloch, kryptografických mechanizmoch, virtualizácii a cloudových prostrediach (BL 3–4).
    - Rozumie právnym predpisom a normám (napr. GDPR, PCI) týkajúcim sa kybernetickej bezpečnosti a ochrany údajov (BL 6).
2. **Zručnosti**:
    - Implementuje procesy identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík.
    - Navrhuje a aplikuje opatrenia na ošetrenie rizík a podporuje bezpečnostnú architektúru.
    - Participuje na plánovaní kontinuity činností a obnovy po havárii.
    - Aplikuje metodiky klasifikácie aktív a kategorizácie sietí.
    - Monitoruje efektivitu bezpečnostných mechanizmov a poskytuje súčinnosť pri auditoch.
    - Podporuje budovanie bezpečnostného povedomia v organizácii.
3. **Postoje**:
    - Proaktívny a analytický prístup k riadeniu rizík a ochrane údajov.
    - Zodpovednosť za súlad s právnymi normami a bezpečnostnými politikami.
    - Etické správanie pri manipulácii s citlivými informáciami.
    - Schopnosť efektívne komunikovať s technickými tímami a vedením.
4. **Špecifické kompetencie**:
    - Schopnosť prijímať rozhodnutia a myslieť v súvislostiach.
    - Analytické a strategické myslenie pri posudzovaní rizík.

- Prezentačné zručnosti a organizácia práce pri koordinácii projektov.

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 alebo riadenia rizík.

Metódy vzdelávania

Vzdelávací program kombinuje teoretické, praktické a analytické metódy zamerané na rozvoj zručností v riadení rizík:

1. **Interaktívne prednášky**:
   - Vysvetlenie procesov riadenia rizík, analýzy hrozieb a právnych rámcov (napr. GDPR, PCI).
   - Diskusie o štandardoch (napr. CMMI, ISO) a metodikách hodnotenia vyspelosti procesov.
2. **Praktické workshopy**:
   - Simulácie analýzy rizík a návrhu opatrení na modelových scenároch (napr. kybernetický útok).
   - Nácvik klasifikácie informačných aktív a kategorizácie sietí.
   - Cvičenia na konfiguráciu bezpečnostných mechanizmov (napr. firewally, šifrovanie).
3. **Prípadové štúdie**:
   - Analýza reálnych alebo hypotetických bezpečnostných incidentov a návrh plánov mitigácie.
   - Skupinové projekty na tvorbu plánov kontinuity činností alebo obnovy po havárii.
4. **E-learning a samoštúdium**:
   - Prístup k online kurzom, certifikačným prípravám (napr. CRISC, CISM) a materiálom o riadení rizík.
   - Interaktívne kvízy na overenie vedomostí o hrozbách, sieťových technológiách a normách.
5. **Simulácie a role-playing**:
   - Simulácie reakcií na kybernetické incidenty s dôrazom na koordináciu a rozhodovanie.
   - Role-playing scenáre na komunikáciu s vedením alebo audítormi pri posudzovaní rizík.
6. **Mentorované projekty**:
   - Samostatné alebo tímové projekty na analýzu rizík a návrh bezpečnostných opatrení.
   - Mentorovanie zamerané na rozvoj analytických a prezentačných zručností.

Forma vzdelávania

Program je navrhnutý ako kombinovaný, aby vyhovoval odborníkom s rôznymi časovými a technickými požiadavkami:

1. **Prezenčná forma**:
    - Intenzívne školenia v školiacich centrách vybavených na simulácie rizikových scenárov.
    - Vhodné na praktické cvičenia, workshopy a tímové diskusie.
    - Trvanie: 2 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 workshopov (napr. na analýzu rizík) 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, analytických zručností a schopnosti navrhovať riešenia:

1. **Znalostné testy**:
    - Písomné alebo online testy zamerané na riadenie rizík, právne normy (napr. GDPR) a bezpečnostné mechanizmy.
    - Formát: výber z možností, analýza scenárov.
2. **Praktické úlohy**:
    - Vykonanie analýzy rizík na modelovom systéme a návrh opatrení.
    - Klasifikácia informačných aktív a návrh plánu obnovy po havárii.
    - Hodnotí sa presnosť, analytický prístup a súlad s normami.
3. **Prípadové štúdie**:
    - Analýza hypotetického bezpečnostného incidentu a návrh stratégie mitigácie.
    - Hodnotí sa schopnosť identifikovať hrozby, posúdiť riziká a navrhnúť opatrenia.
4. **Prezentácie a ústne skúšanie**:
    - Prezentácia analýzy rizík alebo plánu opatrení pred komisiou.
    - Hodnotí sa prezentačná zručnosť, argumentácia a schopnosť obhájiť riešenia.
5. **Simulácie**:
    - Simulácia reakcie na kybernetický incident s dôrazom na koordináciu a rozhodovanie.
    - Hodnotí sa schopnosť efektívne riadiť riziká a komunikovať s tímom.

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 riadenia rizík“ pripravuje odborníkov na efektívne riadenie bezpečnostných rizík v komplexných IT prostrediach. Kombinácia teoretických prednášok, praktických workshopov a projektov zaisťuje, že absolventi sú schopní identifikovať hrozby, navrhovať opatrenia a podporovať súlad s právnymi a technickými normami.