CISO komandos praktikantas – kibernetinio saugumo rizikų analitikas / vertintojas praktika

Apie poziciją

Ieškome 3–4 kurso bakalauro arba magistrantūros studento, norinčio specializuotis tikslinėje kibernetinio saugumo valdymo srityje – rizikų analizėje ir vertinime. Praktikos metu dirbsi tiesiogiai su įmonės CISO (saugumo vadovu) ir padėsi nustatyti, kokios skaitmeninės grėsmės kelia didžiausią pavojų organizacijai, bei kaip efektyviausiai valdyti ir kontroliuoti rizikas.

Pagrindinės atsakomybės

- **Turto ir grėsmių identifikavimas:**
    - Bendradarbiauti su IT ir verslo komandomis, surenkant bei atnaujinant įmonės IT turto (*Assets*) sąrašą.
    - Identifikuoti galimus grėsmių scenarijus (pvz., išpirkos reikalaujančios įrangos atakos, tiekimo grandinės pažeidžiamumai, socialinė inžinerija).
- **Kibernetinių rizikų analizė ir vertinimas:**
    - Taikyti tarptautines rizikos vertinimo metodikas (ISO/IEC 27005, NIST SP 800-30, FAIR).
    - Apskaičiuoti rizikos lygį pagal formulę:
        - $$\text{Rizikos Lygis} = \text{Tikimybė (1–5)} \times \text{Poveikis (1–5)}$$
    - Įvertinti esamų saugumo kontrolių efektyvumą ir apskaičiuoti liekamąją riziką (*Residual Risk*).
- **Rizikų registro (*Risk Register*) ir ataskaitų valdymas:**
    - Pildyti ir palaikyti centrinį įmonės rizikų registrą (*Excel* / GRC platformose).
- **Rizikos valdymo strategijų rengimas (*Risk Treatment*):**

- Formuoti pasiūlymus, kaip sumažinti (*Mitigate*), perduoti (*Transfer*), išvengti (*Avoid*) arba priimti (*Accept*) nustatytas rizikas

- **Kibernetinio saugumo gairių (*Roadmap*) kūrimas:**
  - Remiantis nustatytomis rizikomis, padėti rengti ir prioritetizuoti įmonės kibernetinio saugumo strateginį planą (*Roadmap*).
  - Paskirstyti saugumo priemones bei projektus pagal svarbą (pvz., Q1–Q4 / 1–3 metų perspektyvoje) siekiant sumažinti kritines rizikas.

Reikalavimai kandidatui

- **Išsilavinimas:** Informatikos, kibernetinio saugumo, informacinių sistemų, verslo informatikos ar susijusių krypčių 3–4 kurso studentas arba magistrantas.
- **Teorinės žinios:**
  - Baziniai kibernetinio saugumo principai (CIA triada: konfidencialumas, vientisumas, prieinamumas).
  - IT standartų supratimas (ISO 27001 / ISO 27005 / NIST CSF).
  - Grėsmių ir pažeidžiamumų karkasų išmanymas (OWASP Top 10, MITRE ATT&CK pagrindai).
- **Įgūdžiai:**
  - Stiprūs analitiniai įgūdžiai ir gebėjimas dirbti su struktūrizuotais duomenimis.
  - Gebėjimas sudėtingas technines grėsmes paaiškinti verslui suprantama kalba.
  - Gebėjimas dirbti komandoje.
  - Anglų kalbos žinios (B2/C1 lygis – standartai ir dokumentacija).

Ką siūlome?

- **Lanksčias darbo valandas:** įgyvendinama praktika, kurią lengva suderinti su paskaitomis ar egzaminų sesija.
- **Mentorystę:** tiesioginį darbą su patyrusiu CISO, kuris padės suprasti realius verslo rizikos valdymo sprendimus.

- **Praktinę patirtį:** įgūdžius dirbant su tarptautiniais reikalavimais (ISO 27001, NIS2, DORA).
- **Karjeros galimybes:** galimybę po praktikos prisijungti prie komandos kaip *Junior Cybersecurity Risk Analyst*.

Kandidatus kviečiame siųsti savo CV el. paštu: mindaugas@soc.lt arba raimond@soc.lt.