Tietoturvapäällikkö palveluna

Organisaatioilla ei aina ole omaa nimettyä tietoturvapäällikköä. Toimenkuvaan kuuluvia tehtäviä on saatettu määritellä hoidettavaksi jonkin toisen roolin yhteydessä ”oman toimen ohella”.

Tehtävää hoitamaan nimetyllä henkilöllä ei välttämättä ole asiantuntemusta, kokemusta tai aikaa paneutua mahdollisesti monimutkaisiinkin tietoturvahaasteisiin ja -projekteihin sekä tehtävien edellyttämiin prosesseihin.

Tietoturvallisuuden asianmukaisella hallinnoinnilla on kuitenkin keskeinen rooli organisaation toiminnan jatkuvuuden varmistamisessa, käsiteltävien tietojen suojaamisessa ja sähköisten palveluiden toiminnan turvaamisessa.

Experis tarjoaa käyttöösi tietoturvapäällikön, jolla on mittava kokemus tietoturvallisuuden johtamisessa ja strategisessa sekä operatiivisessa kehittämisessä.

Tietoturvapäällikköpalvelumme ansiosta voit varmistaa, että sinulla on käytettävissäsi tarkoituksenmukainen tietoturvallisuuden asiantuntemus kulloiseenkin tarpeeseesi.

Palvelun kolme vaihetta

1. **Kartoitus**
   - Prosessien, roolien, järjestelmien ja turvallisuusratkaisujen kartoitus
   - Tarpeiden ja tavoitteiden määrittely
   - Toimintasuunnitelman laatiminen

2. **Toimenpiteiden toteuttaminen**
   - Toimintasuunnitelman toteuttaminen
   - Turvallisuusosaamisen kehittäminen
   - Tilannekuvan ylläpito

3. **Tehtävien siirto**
   - Tietoturvallisuusvastuiden siirto organisaation sisäisille vastuuhenkilöille

Esimerkkejä tietoturvapäällikön tehtävistä

- Toimii neuvonantajana tietoturvallisuuteen liittyvissä asioissa.
- Kehittää tietoturvallisuusstrategiaa ja tietoturvallisuuden visiota sekä tavoitteita liiketoiminnan strategisten tavoitteiden mukaisesti.
- Tukee johdon raportointia varten tarvittavien prosessien ja mittaristojen määrittelyä sekä tuottaa menetelmiä tietoturvallisuuden kypsyystason arviointiin
- Johtaa tietoturvallisuustyötä yhdessä liiketoiminnan kanssa, määrittelee ja kehittää dokumentaatiota ja prosesseja
- Tunnistaa lainsäädännön, regulaation, sopimusten ja muiden tekijöiden asettamat tietoturvavaatimukset ja määrittelee tarvittavat kontrollit, prosessit ja dokumentaation.
- Seuraa tietoturvauhkien kehitystä ja viestii muutoksista
- Tukee tietoturvakontrollien käyttöönottoa ja koordinoi auditointien tekemistä
- Edistää riskienhallintaprosessien määrittelyä ja toteuttamista, muodostaa ja ylläpitää riskiprofiilia tietoturvallisuuden osalta
- Tukee tietoturvapoikkeamien käsittelyprosessin määrittelyä ja toteuttamista

Joustavin ratkaisu organisaatiosi tietoturvan kokonaisvaltaiseen kehittämiseen