Cybersikkerhedsspecialist

Om stillingen Cybersikkerhedsspecialist – Security Operations (Detection & Response)
Vil du være med til at styrke Aalborg Kommunes evne til at opdage, reagere på og håndtere cybertrusler?

Vi søger en cybersikkerhedsspecialist, der brænder for Detection & Response, herunder men ikke begrænset til log management, SIEM, incident management og sårbarhedshåndtering. Rollen er en central brik i kommunens cyberforsvar.
Som en del af informationssikkerhed i Fælles Digitalisering er du ansat under CISO og arbejder tæt sammen med IT og forretningen på tværs af hele kommunen. Du vil også indgå i samarbejdet med 11 nordjyske kommuner i Nordig-fællesskabet, hvor videndeling og fælles projekter styrker regionens samlede cybersikkerhed.

Om jobbet
Aalborg Kommune løfter cyberrobustheden markant og udvider fokus fra klassisk logmanagement til et bredt Security Operations-område, hvor du får ansvar for:

- Detektion af sikkerhedshændelser
- Reaktion og håndtering af angreb
- Anskaffelse/tilpasning af sikkerhedsteknologier, herunder SIEM/log management
- Modning af incident management-processen og playbooks
- Understøttelse af teknisk sårbarhedsstyring og løbende styrkelse af IT-sikkerheden

Arbejdet kombinerer hands-on teknik (f.eks. EDR/XDR og SIEM) med procesmodning, rådgivning og samarbejde på tværs af organisationen.

Dine ansvarsområder
Detection & Response (primært fokus)

- Udvikle, vedligeholde og forbedre detektionskapacitet og alarmer, herunder koble endpoint, netværks- og cloudtelemetri sammen til effektive use cases
- Udvikle og vedligeholde playbooks for Security Incident Response
- Holde sig orienteret inden for Threat Intelligence og overfører denne viden til proaktive handlinger Aalborg Kommune
- Indgå i triage, eskalering og håndtering af sikkerhedshændelser, herunder sikring af dokumentation og rapportering
- Understøtte NIS2-krav om hændelsesrapportering

Sårbarhedsstyring & løbende styrkelse af IT-sikkerheden

- Bidrage til prioritering og kvalificering af tekniske sårbarheder
- Understøtte initiativer der forbedrer IT-sikkerheden i Aalborg Kommune
- Samarbejde med ITdrift om udbedring og verifikation

Samarbejde, rådgivning og governance

- Give sikkerhedsmæssig sparring i forbindelse med anskaffelser, implementering og PoC-forløb
- Samarbejde med forvaltninger, driftsteams, Nordig-kommuner og leverandører
- Bidrage til ledelsesrapportering om detektion, logdækning, m.m.

Din profil
Forventede kompetencer

- Erfaring med anvendelsen af SIEM og logmanagement-teknologier
- Erfaring med analyse af telemetri fra EDR/XDR, netværk og cloud
- Erfaring med hændelseshåndtering og playbooks (triage, inddæmning og analyse)
- Forståelse for MITRE ATT&CK og relevante rammeværker (NIST, ISO, CIS)
- Evne til at overskue komplekse tekniske miljøer og skabe struktur

Herudover kan du med fordel, men uden det er et krav, have kompetencer indenfor:

- Erfaring med cloud-sikkerhed i Microsoft 365/Azure

- Erfaring med Digital Forensics and Incident Response-værktøjer (DFIR) til undersøgelse, analyse og håndtering af sikkerhedshændelser
- Scripting (PowerShell, Python)

Personlige egenskaber

- Analytisk, nysgerrig og detaljeret
- Du kan holde hovedet koldt i pressede situationer
- Evner at kommunikere både teknisk og ikke-teknisk på dansk idet der skal kommunikeres med forskellige interessenter fra forskellige forvaltninger og leverandører
- Trives i en rolle med både drift, udvikling og procesmodning
- Proaktiv og samarbejdsorienteret

Hvorfor vælge Aalborg Kommune?
Grundlæggende bliver du en del af en fed arbejdsplads, og med gode kollegaer og med et fagligt fællesskab på et højt niveau. Du kan forvente:

- Du bliver en del af en stor, kompleks og spændende organisation med samfundskritiske services
- Du bliver en del af en af Danmarks største kommuner, der investerer i sikkerhedsområdet og ser det som en strategisk, taktisk og operationel kerneopgave
- Du får stor indflydelse på kommunens cyberresiliens, herunder på hvordan vi opdager og håndterer cybertrusler
- Du arbejder i et stærkt fagligt miljø med fokus på udvikling og samarbejde.
- Du gør en reel forskel for borgere og medarbejdere hver dag

Praktisk

- *Arbejdssted:* Danmarksgade 17A under CISO i informationssikkerhed under Fælles Digitalisering
- *Ansøgningsfrist:* 7. april 2026
- *1. samtale*: der afholdes første samtaler 13. april
- *2. samtale*: hvis det vurderes nødvendigt, afholdes der anden samtaler 21. april

Forud for endelig ansættelse indhentes der straffeattest samt reference

Send ansøgning
Du sender din ansøgning ved at trykke på knappen "Send ansøgning" og udfylde den formular, som kommer frem. Det er også muligt at vedhæfte bilag som f.eks. ansøgning og CV i begrænset omfang.

Bliv en del af Dobbelt A – få dobbelt op på muligheder
Hos os bliver du en del af et fedt fællesskab med 17.500 kolleger. Glæd dig til at få dobbelt op på udviklingsmuligheder, gode ansættelsesforhold og fokus på trivsel. Vi tror på, at forskellighed gør os stærkere, og opfordrer alle til at søge – uanset alder, køn, baggrund, religion eller handicap.
Se alle fordelene ved et job hos os og bliv klogere på ansættelsesprocessen trin-for-trin.