Åbent værk. AI, IT awareness, sikkerhed, praksis

Fag: Digitale kompetencer til online undervisning

Fagnummer: 20996	**Varighed** 1 dag
AMU-pris: DKK 218,00	**Uden for målgruppe:** DKK 822,55

Målgruppe: Uddannelsen er rettet mod AMU-målgruppen, herunder ufaglærte og faglærte inden for erhvervsuddannelsesområdet.

Beskrivelse: Deltageren:
kan anvende udvalgte redskaber (PC, tablet, mobil) som arbejdsredskab ved online undervisning.
kan udføre simple handlinger på en læringsplatform.
kan i online forum anvende udvalgte funktioner, f.eks. logge på, dele materialer og anvende chat.
kan skelne mellem synkron og asynkron undervisning og kender forudsætninger og egen rolle ved deltagelse i disse.
har viden om digitale redskaber til læsning og skrivning og kan anvende disse efter behov.

Fag: Machine Learning i praksis

Fagnummer: 22044	**Varighed** 5 dage
AMU-pris: DKK 1.090,00	**Uden for målgruppe:** DKK 4.325,00

Målgruppe: Kurset henvender sig til faglærte medarbejdere, inden for det datatekniske område, og andre inden for AMU-målgruppen med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med programmering.

Beskrivelse: Deltageren kan med den opnåede viden:
Anvende og håndtere forskellige maskinlæringsmetoder.
Fortolke og analysere datasæt.
Anvende maskinlæring aktivt til at løse avancerede praktiske opgaver.
Selvstændigt samle og forberede data til maskinlæring.
Træne og teste sin model.
Anvende klassificering og regression til at løse praktiske opgaver.
Anvende et maskinlærings-framework til at løse en praktisk opgave.
Anvende centrale modeller, der bruges til at bearbejde data med.

Kontakt

Skolen
74124242
eucsyd@eucsyd.dk

Kursuspris

AMU:
DKK 11,00

Uden for målgruppe:
DKK 11,00

Tilmelding

Fag: Informations- og cybersikkerhed 1

Fagnummer: 23214	**Varighed** 5 dage
AMU-pris: DKK 1.090,00	**Uden for målgruppe:** DKK 3.258,25

Målgruppe: Kurset henvender sig til faglærte personer, inden for det datatekniske område, og andre med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med informations- og cybersikkerhed.

Beskrivelse: Efter gennemført kursus kan lærlingen:
Redegøre for nøglebegreber inden for informationssikkerhed og cybersikkerhed herunder privacy, databeskyttelse og trusselvektorer samt risikovurdering.
Udarbejde en adgangskontrolpolitik til regulering af brugeradgang herunder en passwordpolitik.
Redegøre for gængse interessekonflikter, herunder deres årsager og konsekvenser.
Har viden om, hvordan man ændrer, begrænser og håndterer konflikter.
Har viden om, hvordan machine-learning kan anvendes i for eksempel sikkerhedsovervågning til identifikation af trusler.

Fag: Informations- og cybersikkerhed 2

Fagnummer: 23215	**Varighed** 7,5 dage
AMU-pris: DKK 1.635,00	**Uden for målgruppe:** DKK 4.757,38

Målgruppe: Kurset henvender sig til faglærte personer, inden for det datatekniske område, og andre med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med informations- og cybersikkerhed.

Beskrivelse: Efter gennemført kursus har lærlingen:
Kendskab til formålet med gængse sikkerhedsstandarder (fx ISO 27001 og ISO 27002) og har kendskab til relevante organisationer som for eksempel Center for cybersikkerhed og Center for Internet security (CIS).
Kan forklare begreberne compliance og regulering samt værdien af en beredskabsplan.
Viden om multifaktor-authentificering, som kombinerer noget man ved, noget man har og noget man er.
Kan anvende sin teoretiske forståelse for fysisk adgang og sikkerhed til at udarbejde implementeringsforslag.

Fag: Udvikling af egen AI

Fagnummer: 22605	**Varighed** 6 dage
AMU-pris: DKK 1.308,00	**Uden for målgruppe:** DKK 3.857,90

Målgruppe: Kurset henvender sig til faglærte medarbejdere, inden for det datatekniske område, og andre inden for AMU-målgruppen med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med programmering.

Beskrivelse: Deltageren kan anvende AI-værktøjer til at assistere i udviklingsopgaver.
Deltageren kan integrere AI-funktionaliteter i eksisterende applikationer for at forbedre brugeroplevelsen.
Deltageren kan udvikle autonome AI-løsninger, der kan træffe beslutninger på baggrund af dataanalyse.
Deltageren kan anvende promptingteknikker for at få det bedste ud af AI-modeller.
Deltageren kan identificere relevante anvendelsesområder for AI i deres arbejdsprocesser.
Deltageren kan evaluere og justere AI-løsninger baseret på brugerfeedback og dataindsamling.
Deltageren kan arbejde med både teoretiske og praktiske aspekter af kunstig intelligens for at udvikle funktionelle løsninger.
Deltageren kan skabe AI-baserede løsninger, der forbedrer effektiviteten af eksisterende arbejdsprocesser.

Fag: Brug af generativ AI i programmering

Fagnummer: 22606	**Varighed** 5 dage
AMU-pris: DKK 1.090,00	**Uden for målgruppe:** DKK 3.258,25

Målgruppe: Kurset henvender sig til faglærte medarbejdere inden for det datatekniske område og andre inden for AMU-målgruppen med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med programmering.

Beskrivelse: Efter gennemført kursus kan deltageren:
Anvende generativ AI til at forbedre programmeringspraksis, herunder brug af værktøjer som GitHub Copilot og OpenAI APIer.
Integrere AI i egne projekter og reflektere kritisk over AI's anvendelse i softwareudvikling.
Forstå grundlæggende principper inden for generativ AI og dens anvendelse i programmering.
Udforske og eksperimentere med nye generative AI-modeller og værktøjer for at vurdere deres potentielle anvendelse i projekter.
Anvende avancerede prompt-teknikker for at forbedre præcision og outputkvalitet i generative AI-værktøjer, med fokus på kontekst og klar kommunikation.
Anvende værktøjer som GitHub Copilot til at assistere i kodning.
Implementere generativ AI i egne programmeringsprojekter.
Opsætte og optimere API-kald til generativ AI, herunder fejlsøgning og ydeevneforbedringer for at sikre effektiv drift.
Kritisk vurdere og reflektere over anvendelsen af generativ AI i softwareudvikling.

Fag: Grundlæggende Cloud-sikkerhed

Fagnummer: 22607	**Varighed** 5 dage
AMU-pris: DKK 1.090,00	**Uden for målgruppe:** DKK 3.258,25

Målgruppe: Kurset henvender sig til faglærte medarbejdere, inden for det datatekniske område, og andre inden for AMU-målgruppen med tilsvarende kvalifikationer, der skal eller ønsker at arbejde med sikkerhed og cloud.

Beskrivelse: Efter gennemført kursus kan deltageren:

Udvise forståelse for cloud-sikkerhed.
Redegøre for cloud sikkerhedsudfordringer, service modeller (IaaS, PaaS, SaaS), og de særlige sikkerhedskrav, som hver model indebærer.
Identificere og forklare risici ved cloud-sikkerhed, og redegøre for anvendelse af grundlæggende sikkerhedsprincipper for at minimere disse risici.
Implementere og administrere rollebaseret adgangskontrol (RBAC) og multi-faktor godkendelse (MFA) for cloud-baserede applikationer og tjenester.
Anvende open-source værktøjer som FreeIPA eller OpenLDAP til IAM-opgaver og kan konfigurere disse systemer til at beskytte adgang til kritiske cloud-ressourcer.
Opsætte sikre, virtuelle netværk og brug af firewalls, VPNer og indbrudsdetekteringssystemer som OpenVPN og Suricata.
Designe og beskytte netværk mod trusler som DDoS-angreb og sikre trafik mellem cloud-ressourcer ved brug af VPN og IPS/IDS.
Anvende kryptering til både data in-rest og under transit ved brug af værktøjer som LUKS og OpenSSL.
Opsætte og administrere nøgler med HashiCorp Vault eller lignende open-source løsninger for at sikre databeskyttelse og opfylde krav til dataintegritet.
Implementere og administrere et lognings- og monitoreringssystem for at kunne opdage og reagere på sikkerhedshændelser.

Fag: Disaster Recovery og genopretning i praksis

Fagnummer:	Varighed
23436	3 dage

Målgruppe: Uddannelsen henvender sig til medarbejdere med ansvar for it-drift og genopretning i små og mellemstore virksomheder. Det kan f.eks. være it-administratorer, driftsmedarbejdere eller andre it-ansvarlige, uanset formelle it-kompetencer, som skal kunne håndtere nedbrud og genoprette systemer på en struktureret og praktisk måde.

Beskrivelse: Deltageren kan arbejde selvstændigt med Disaster Recovery i en SMV og medvirke til at udarbejde, teste og vedligeholde en enkel Disaster Recovery Plan (herefter kaldet DRP). Deltageren kan håndtere nedbrud og recovery på en struktureret og praktisk måde og anvende virksomhedens procedurer for backup og recovery.
Deltageren kan:
redegøre for en DRP og anvendelse af denne.
indsamle oplysninger om systemer, data og afhængigheder og beskrive de vigtigste funktioner i en DRP
udvælge relevante backup-metoder, gennemføre recovery og vurdere RTO og RPO for virksomhedens systemer
udarbejde en enkel DRP med klare trin for recovery af data, servere, applikationer og tjenester
gennemføre praktiske test af backup og recovery og dokumentere resultater i faste skemaer
håndtere nedbrud ved at følge DRP'en, prioritere opgaver og kommunikere status til interne interessenter
bruge procedurer og dokumentation, så DRP'en løbende kan vedligeholdes og holdes opdateret i forhold til ændringer i systemer eller drift

Fag: Cybersikkerhed i OT-miljøer

Fagnummer:	Varighed
23437	5 dage

Målgruppe: Uddannelsen henvender sig til it-professionelle, der arbejder med drift, netværk eller administration af tekniske systemer i virksomheder med produktions- eller automatiseringsudstyr. Det kan f.eks. være it-driftsteknikere, netværksteknikere og systemadministratorer, som skal kunne håndtere sikkerhed i OT-miljøer og arbejde i snitfladen mellem IT og produktion.

Beskrivelse: Deltageren kan arbejde selvstændigt med grundlæggende sikkerhed i OT-miljøer og håndtere opgaver i grænsefladen mellem IT og produktion. Deltageren kan vurdere risici, udføre tekniske kontroller og følge etablerede arbejdsgange, der sikrer stabil og sikker drift af produktions- og automatiseringsudstyr.
Deltageren kan:
identificere centrale OT-komponenter, beskrive deres betydning for produktionen og vurdere cybersikkerheds risici i netværk, udstyr og forbindelser til IT-miljøet
udføre kontroller af netværkssegmentering, adgange, protokoller og overvågning på OT-udstyr og vurdere, om forholdene følger virksomhedens krav
forebygge cybersikkerhedshændelser ved at gennemføre tekniske tiltag, f.eks. kontrol af konfigurationer, brugerstyring, opdateringer og fysisk adgang
indgå aktivt i beredskabsarbejdet ved at registrere hændelser, analysere enkle årsager og eskalere dem efter procedurerne
sikre vedligehold af OT-miljøer ved at følge rutiner for dokumentation, kontrol, ændringshåndtering og opfølgning på tekniske forhold
samarbejde med kolleger fra både IT- og produktionsområder om at løse opgaver i snitfladerne, herunder koordinere mindre tekniske tiltag og sikre ensartede arbejdsgange

Fag: NIS2 og governance i praksis

Fagnummer:	Varighed
23438	3 dage

Målgruppe: Uddannelsen henvender sig til it-professionelle, der arbejder med drift og administration af virksomhedens it-miljø. Det kan f.eks. være driftsteknikere, systemadministratorer eller andre med tilsvarende erfaring, som skal kunne omsætte NIS2-krav til praktiske arbejdsopgaver i den daglige drift og bidrage til virksomhedens sikkerhedsstyring.

Beskrivelse: Deltageren kan arbejde praktisk med de tekniske krav i NIS2-direktivet i den daglige it-drift og udføre grundlæggende opgaver, der understøtter virksomhedens sikkerhedsstyring.
Deltageren kan:
identificere relevante NIS2-krav, der påvirker it-driften, og omsætte dem til konkrete handlinger i systemer, netværk og applikationer
udføre arbejde med adgangsstyring, logning, overvågning og teknisk dokumentation, så opgaverne følger de krav, virksomheden har fastlagt
gennemføre enkle risikovurderinger af systemer eller ændringer og beskrive fund i et forståeligt og brugbart format til intern rapportering
medvirke i interne sikkerhedsprocesser som ændringsstyring, hændelseshåndtering og løbende opfølgning på tekniske kontroller
deltage i planlægning og vedligehold af grundlæggende governance-aktiviteter, så tekniske tiltag og daglige driftsopgaver hænger sammen med virksomhedens sikkerhedsarbejde
bruge standardiserede metoder og arbejdsgange, der understøtter samarbejdet mellem teknikere, sikkerhedsansvarlige og ledelse i implementeringen af NIS2

Fag: Awareness om cybersikkerhed til SMVer

Fagnummer:	Varighed
23458	3 dage

Målgruppe: Uddannelsen henvender sig til faglærte og ufaglærte medarbejdere, der arbejder med IT-support, systemadministration eller drift i små og mellemstore virksomheder.Deltagerne kan fx være it-supportere, driftsteknikere, helpdeskmedarbejdere eller andre med tilsvarende funktioner, som udfører daglige opgaver med brugeradministration, systemtilgang, fejlsøgning og generel driftsunderstøttelse.Uddannelsen er relevant for medarbejdere, der skal kunne indgå i virksomhedens håndtering af grundlæggende cybersikkerhed i den daglige drift og reagere korrekt på simple sikkerhedshændelser.

Beskrivelse: Deltageren arbejder med grundlæggende cybersikkerhed i driftsmiljøer og kan efter kurset udføre sikkerhedsmæssigt korrekte handlinger i almindelige support- og driftsopgaver.
Deltageren kan:
Genkende typiske cybertrusler som phishing, social engineering og usikre filer samt arbejde med metoder til at identificere usikre handlinger.
Anvende sikre arbejdsgange i daglig drift, herunder håndtering af adgangskoder, mails, delte ressourcer og dataoverførsel.
Håndtere simple sikkerhedshændelser ved at reagere korrekt, begrænse skaden og rapportere efter virksomhedens procedurer.
Understøtte virksomhedens IT-sikkerhed ved at omsætte grundlæggende politikker og retningslinjer til praktiske handlinger i support- og driftsopgaver.