HANDS-ON AWARENESS-TRÆNING FOR TEKNISKE PROFILER

Opbyg et stærkt cyberfundament – 30 min. om måneden pr. medarbejder.

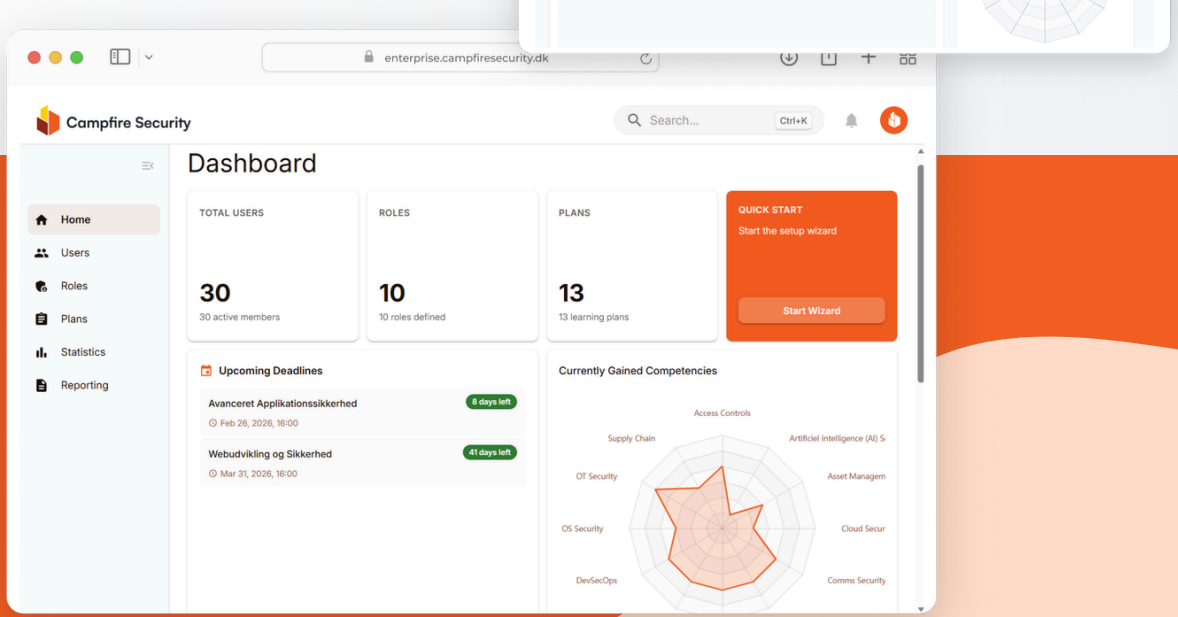
Ved at benytte vores enterprise-platform og vores kursersamling om Techverum Solutions, introduceres I til de 12 centrale cybersikkerhedskompetencer for tekniske profiler. Kursussamlingen opbygger et fælles, grundlæggende vidensfundament, som understøtter daglige beslutninger og forståelse af cybertrusler.

Kurserne giver medarbejderne et solidt fundament til at forstå både tekniske svagheder og organisatoriske beslutninger, der påvirker cybersikkerheden i praksis. Gennem etableringen af et fælles sprog og fælles forståelse for hackernes motiver og værktøjer, bliver det lettere at beskytte sig imod de skjulte trusler.

Enterprise-platformen – dit styringsværktøj

Gennem vores Enterprise-platform tildeles med-arbejderne præcis den træning de har behov for.

- **Tidsinvestering**: Typisk 15 – 30 min. pr. kursusmodul
- **Kompetence-gevinst:** Medarbejderne opnår niveau 1–2 i Campfire Securitys Cyber KPI rammeværk
- **Fleksibel tildeling**: I vælger, hvor ofte træningen tildeles, og hvor længe den er tilgængelig
- **Strategisk overblik**: Kontinuerlig dokumentation af organisationens kompetenceudvikling og bevis for risikobaseret, målrettet arbejde med medarbejdernes generelle cybersikkerhed

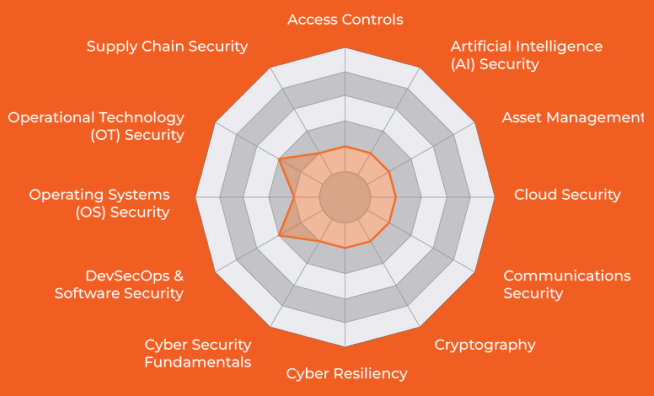


CASE-BASERET LÆRING:
TECHVERUM SOLUTIONS

TECHVERUM SOLUTIONS

Techverum-kursussamlingen tager udgangspunkt i den fiktive virksomhed 'Techverum Solutions' og fokuserer på tre kerneområder:

1. **Relevans:** Hvorfor er læringsområdet vigtigt?
2. **Sårbarhed:** Hvilke sårbarheder eksisterer? (Inkl. praktisk øvelse med ægte sårbarheder og "aha-oplevelse")
3. **Refleksion:** Hvordan kan sårbarheder reduceres, elimineres eller håndteres?



Kursusmoduler og kompetencer:

Kursussamlingen består af 14 kursusmoduler, der hver introducerer centrale aspekter af moderne cybersikkerhed via realistiske scenarier fra Techverum Solutions. Nedenfor ses en kort opsummering på nogle af disse kurser.

SHADOWPROMPT (AI-SIKKERHED)
- Forstå hvordan utilstrækkelig beskyttelse af AI-systemer kan føre til datalæk.
- Viser vigtigheden af at sikre systemprompter og forebygge prompt-injektion.

SIGNAL TRACE (GRUNDLÆGGENDE CYBERSIKKERHEDSFORSTÅELSE)
- Forstå hvordan skjulte metadata kan udgøre en kritisk sikkerhedsrisiko.
- Indblik i typiske fejl, der fører til informationslæk.

SKYBREACH (CLOUD-SIKKERHED)
- Illustrerer risikoen ved manglende patching og opdateringer i cloud-miljøer.
- Understøtter opbygning af gode vaner omkring patch-management og sårbarhedsovervågning.

INDUSTRIAL DEFENCE (OT-SIKKERHED)
- Grundforståelse for industrielle styringssystemer og deres særlige beskyttelsesbehov.
- Kendskab til angrebsmetoder mod OT-miljøer og typiske sikkerhedsgab.

SURVIVAL (CYBER RESILIENS)
- Understøtter forståelsen af, hvorfor modstandsdygtighed er afgørende – ikke kun forebyggelse.
- Fokus på identificering og afhjælpning af svagheder, før de udnyttes.

CHAINBREAK (SUPPLY CHAIN-SIKKERHED)
- Giver kendskab til risici ved tredjepartsafhængigheder og softwareopdateringer.
- Understøtter forståelsen for behovet for validering af leverandører og komponenter.

PANELBREAK (DEVSECOPS)
- Indsigt i hvordan fejlkonfigurationer og manglende vedligehold truer pipelines og deployment-miljøer.
- Fremmer skærpet fokus på at sikre processer i hele udviklings og driftskæden.

Campfire Security

kontakt@campfiresecurity.dk

+45 33 13 13 37

campfiresecurity.dk/business