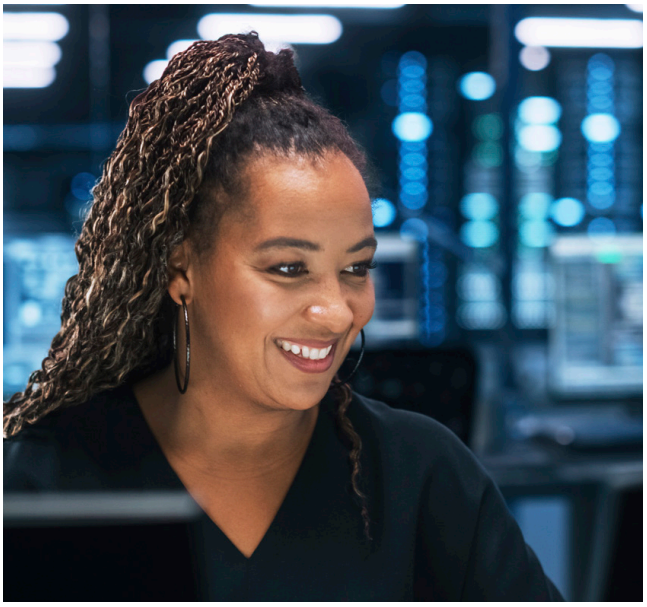
IT-säkerhetschef - diplomutbildning

9 dagar

- Så får du en säkerhetsmedveten organisation
- Riskhantering, förstå hot och risker och prioritera rätt
- Så här leder du verksamheten genom ett cyberangrepp



Ta ditt IT-säkerhetsansvar på bästa sätt

Som IT-säkerhetschef ansvarar du för det operativa IT-säkerhetsarbetet i din verksamhet. Du gör sannolikt risk- och sårbarhetsanalyser och har det yttersta ansvaret för utformande av säkerhetslösningar och IT-säkerhetssystem utifrån verksamhetens behov. Som bekant är det sällan tekniken som är problemet, utan det absolut mest viktiga är styrningen.

Samtidigt står det klart att det i princip inte är en fråga om om, utan om när verksamheten utsätts för någon form av cyberattack. Det ska ställas emot alla rapporter som visar att IT-säkerhetskompetensen generellt inte är tillräcklig hög.

Här finns därför en unik chans för dig som tidigare har arbetat inom IT, IT-säkerhet eller inom informationssäkerhet och som ska ta över IT-säkerhetsansvaret fullt ut – eller för dig som är ny i din roll som IT-säkerhetschef/CIO.

Styrning – så leder och utvecklar du IT-säkerhetsarbetet

IT-säkerhetschef – diplomutbildning är en totalt nio dagar lång utbildning (tre dagar i månaden i tre månader) och syftar till att ge en större trygghet i yrkesrollen. Du får kunskap inom områden som cybersäkerhet, säkerhetsarkitektur och säkerhetsområdet i stort, hotlandskapet, förändringsledning och hur ni implementerar säkra lösningar som inte gör processerna svårarbetade. Du får även en generell förståelse om juridik och ramverk samt lär dig hur du leder verksamheten genom cyberangrepp.

Utbildningen ger en ökad förståelse för förväntningarna på en IT-säkerhetschef och hur denne mäter och rapporterar om verksamhetens säkerhetsförmåga. Den kommer också att ge kunskap om hur man på ett effektivt sätt hanterar säkerhetsincidenter och det efterföljande arbetet. Framför allt får du konkreta verktyg att jobba utifrån.

Efter genomförd utbildning kommer du att ha goda kunskaper om hur du visar för ledning, styrelse eller andra intressenter hur du systematiskt stärker verksamhetens säkerhet genom beprövade och välkända standarder och således skyddar organisationens information.

Under hela utbildningen kommer vi tillsammans att förankra det teoretiska lärandet till verkligheten, med exempel från kända cyberangrepp, som SolarWinds och NotPetya men även mindre kända svenska attacker.

Utbildningen är utformad på ett sätt som innebär flera interaktiva inslag under varje utbildningsdag, med allt från filmer till pop-quiz.

DATUM	Ort	Kursavgift
7-9 juni, 28-30 augusti och 18-20 september 2023	Stockholm	47 900
4-6 oktober, 6-8 november och 4-6 december 2023	Stockholm	47 900

Stockholm: Kurser i Stockholm äger rum på Företagsuniversitetet i Globen-City i Stockholm. Hotellrum kan bokas till specialpris, uppge att du deltar i kurs hos oss eller ange kundnummer CH2005318. Boka på Quality Hotel Globe, tre minuters promenad från kurslokalerna: 08-686 63 20 eller per mail q.globe@choice.se

Tider, 10.00-17.00 första dagen i varje block och 09.00-16.00 övriga dagar.

I kursavgiften ingår kursdokumentation, luncher samt för- och eftermiddagskaffe. Moms tillkommer.

PROGRAM

Block 1

➔ **Grundläggande komponenter för en lyckad säkerhetsorganisation**
- så får du en säkerhetsmedveten organisation
- säkerhet och det mänskliga elementet
- förändringsledning
- säkerhet vs verksamhet – den eviga avvägningen
- myt eller sanning? Slå hål på eller förankringar av de vanligaste säkerhetsmyterna

➔ **Riskhantering och hotlandskap**
- trender inom cybersäkerhet
- riskhantering, förstå hot och risker och prioritera rätt
- hotaktörerna – så arbetar de för att hacka er
- olika typer av tester och varför man gör dem – förstå rapporterna och agera rätt

Block 2

➔ **Juridik, ramverk och best practise**
- legala aspekter som säkerhet måste ta i beaktande
- generell förståelse och kunskap om ramverk, som NIST, SIS, ISO, OWASP, MITRE m.fl.
- externa och strategiska samarbeten
- så bygger du upp en SOC (Security Operations Centre)

➔ **Hantera angrepp**
- så här leder du verksamheten genom ett cyberangrepp/en kris
- dessa verktyg finns att tillgå för att förebygga, identifiera och hantera incidenter
- incidenthantering och kontinuitetshantering

Block 3

➔ **Systematiskt säkerhetsarbete**
- rapportera cyberrisker. till ledning och styrelse – så här gör du!
- styrning – att leda och utveckla IT-säkerhetsarbetet
- roller och ansvar
- kontrollfunktioner
- 3:e partsrisker
- geopolitiska och andra makrotrender som påverkar säkerhetsarbetet

➔ **Diplomeringsuppgift**

Diplomeringsuppgiften är uppdelad i flera moment;
- IT-säkerhetsarkitektur – bygg din egna säkerhetsarkitektur (fiktiv)
- hantera ett cyberangrepp – scenariobaserad händelseutveckling där du testar dina incidentledningskunskaper (interaktivt test)
- grupparbeten – presentationer och utmaningar (genomgående)

FAKTA

Deltagare / förkunskaper

Utbildningen vänder sig till dig som tidigare har arbetat som IT-säkerhetsspecialist eller informationssäkerhetschef och som ska ta över IT-säkerhetsansvaret fullt ut – eller för dig som är ny i din roll som IT-säkerhetschef/CIO.

Metod och upplägg

Kursen består av tre undervisningsblock om tre dagar vardera, som innehåller föreläsningar, diskussioner samt praktiska övningar.

Krav och grunder för diplomering i programmet

➔ Minst 90 procent närvaro under utbildningen

➔ Godkänd diplomeringsuppgift

Kursledare

Baris Färnman

Utbildningens mål

Målet är att tillhandahålla metoder, kunskap och övningar som behövs för att kunna:

➔ skapa, styra och leda en säkerhetsmedveten organisation

➔ förstå riskerna, hoten och och prioritera rätt

➔ leda verksamheten genom ett cyberangrepp

➔ förstå pen-tester och andra rapporter och göra korrekta bedömningar utifrån dessa

➔ incidenthantering och kontinuitetshantering

➔ upphandlingar och utvärderingar ur säkerhetssynpunkt

➔ rapportera cyberrisker till ledning och styrelse