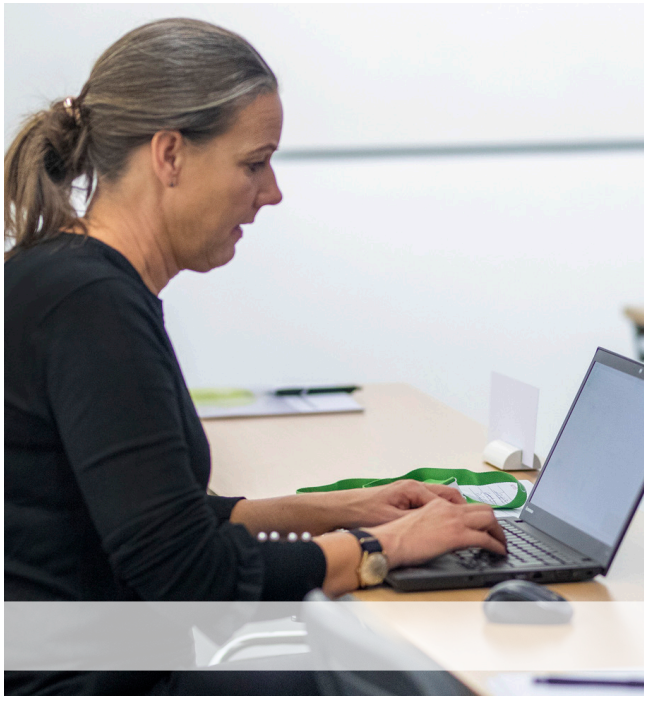
IT-säkerhetsspecialist - diplomutbildning

12 dagar

- Så identifierar du hotaktörerna, ransomwareattackerna och tillvägagångssätten
- Bygg den bästa säkerhetsarkitekturen
- Lär dig hantera och kommunicera IT-risker och IT-incidenter

Få en gedigen helhetsbild av verksamhetens IT-säkerhet

IT-systemen är en del av verksamhetens nerv och måste fungera på ett säkert, optimalt och tillgängligt sätt. Som IT-säkerhetsspecialist måste du kunna förebygga, identifiera och hantera hot och incidenter och se till att all information är skyddad. Därför behöver du också känna till hotbilder, risker, tillvägagångssätt och naturligtvis även de lagar och regler vi har att förhålla oss till. Digitaliseringen ställer som bekant helt nya krav- för att inte nämna den numera uttalade risken för ännu fler och besvärligare cyberattacker i kölvattnet av utvecklingen i samhället. En rapport visar exempelvis att 82 procent av 200 tillfrågade svenska beslutsfattare inom IT-säkerhet uppgivit att de drabbats av en betydande säkerhetsincident inom sin organisation som krävt en incidentresponsinsats, mellan februari 2021 och februari 2022. En annan rapport visar att 80 procent av svenska företag anser att verksamhetens säkerhetsriktlinjer, policyer och verktyg inte håller jämna steg med hackarnas TTP:er. Den befintliga bristen på kompetens inom cybersäkerhet anges många gånger som ett verkligt hinder i arbetet. Rollen som IT-säkerhetsspecialist har alltså aldrig varit mer efterfrågad och viktig. Här finns därför den perfekta utbildningen för dig som snabbt vill vidareutveckla dig, från att kanske tidigare ha verkat som utvecklare eller motsvarande, till att ta klivet in som it-säkerhetsspecialist i offentlig eller privat sektor.



En konkret utbildning som ger dig nödvändiga verktyg

Utbildningen ger en fördjupning i alla de kompetenser som en IT-säkerhetspecialist behöver och är framtagen i samarbete med flera IT-säkerhetsexperter. Du får bland annat lära dig att implementera och göra tekniska och administrativa säkerhetsgranskningar, ta fram rekommendationer på motåtgärder och konfigurationer och bidra i de processer som skapar en säker IT-struktur.

Du får även kunskap om säkerhetsarkitektur, moln- och nätverkssäkerhet, forensik, krypto, incidenthantering, "etiskt hackande", säker utveckling och scriptverktyg, lagstiftning och regelefterlevnad samt hur man gör säkerhetsgranskningar på leverantör/tredje part.

Bokning och rådgivning

För bokning ring 08-600 62 00 eller skicka e-post till bokning@foretagsuniversitetet.se. För information och kursrådgivning ring 08-600 62 00 eller skicka e-post till kurs@foretagsuniversitetet.se.

DATUM	Ort	Kursavgift
18-20 mars, 15-17 april, 21-22 maj och 11-14 juni 2024	Stockholm	64 500

Stockholm: Kurser i Stockholm äger rum på Posthuset, Vasagatan 28 i Stockholm. För dig som deltar i våra utbildningar erbjuder vi specialpris på två fina hotell nära kurslokalen: Nordic Light Hotel: boka på nordiclighthotel.com och ange bokningskod "FUN-deltagare" eller Clarion Hotel Sign: ring 08-676 98 00 eller mejla till cl.sign@choice.se och uppge avtalsnummer CH2005318.

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

KURSLEDARE

Oliver Rosander är Security Operations Manager på Truecaller AB sedan januari 2023. Innan dess har han bland annat arbetat på Cparta Cyber Defense och NTT Security Holdings samt som Cyber Security Consultant på PWC. Han har en Master of Science från Blekinge Tekniska Högskola.

Baris Färnman är VP och CISO på börsnoterade Truecaller AB. Dessförinnan har han jobbat med förändringsledning på Swedbank och som tjänsteområdeschef hos PwC Sverige. Baris har lång erfarenhet av att hjälpa olika typer av organisationers IT- och informationssäkerhetsarbete både i form av utvecklingsarbete men även under incidenter oh kriser.

Viktor Persson är IT Security Consultant och grundare av Alt-Shift. Han har en bakgrund från Intil där han arbetade som full-stack developer och OSINT Investigator. Han har även varit Cyber Security Consultant på NTT och PWC tidigare. Viktor har en Master of Science från Blekinge Tekniska Högskola.

Martin Sjödin Jonsson arbetar som Full Stack Engineer på Regent AB sedan augusti 2022. Han har en Master of Science från Linköpings universitet och har tidigare arbetat bland annat på sQills, Etteplan och som software engineer på Ericsson.

FAKTA

Deltagare / förkunskaper
Utbildningen vänder sig till dig som tidigare arbetat som exempelvis systemadministratör/utvecklare och som behöver vidga din syn på säkerhet och till dig som kanske arbetat med IT-säkerhet en tid men som behöver specialisera dig inom vissa områden.

Metod och upplägg
Kursen består av fyra 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

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

- fungera som ett bollplank åt organisationen i alla IT-säkerhetsfrågor
- kommunicera och hantera alla IT-säkerhetsrisker och incidenter
- identifiera risker, hot och sårbarheter mot informations- och IT-säkerhet
- navigera i tillämpliga lagar, regler och standarder
- genomföra IT-säkerhetsgranskningar på leverantör/tredje part

Kursledare
Baris Färnman, Martin Sjödin Jonsson, Oliver Rosander och Viktor Persson

IT-säkerhetsspecialist - diplomutbildning

– stor efterfrågan på cybersäkerhetsspecialister

Block 1 - 3 dagar

➔ **Systematiskt säkerhetsarbete - introduktion**
- introduktion
- säkerhetstrender
- systematiskt säkerhetsarbete - grunderna

➔ **Juridik och ramverk**
- olika typer av lagkrav, som NIST SIS och ISO
- olika typer av säkerhetsramverk, som OWASP, MITRE och CIS
- best practices

➔ **Riskerna och hoten, inledning**
- hotlandskapet
- attackvektorer
- modus/TTP

Block 2 - 3 dagar

➔ **Säkerhetsarkitektur**
- moderna metoder, som Secure by design och Secure by default
- Zero Trust och Security Automation
- skillnad på säkerhet i molnet och on prem-lösningar

➔ **Incidenter och forensik**
- Security Operations Center
- incident response
- teknisk forensik

➔ **Riskhantering**
- Hantering av cyberrisker
- Kvantifiering av cyberrisker
- så prioriterar man rätt it-säkerhetsinsatser

Block 3 - 2 dagar

➔ **Säker utveckling I**
- introduktion
- implementering av säkerhet i utvecklingskedjan
- DevSecOps

Säker utveckling II
- automatiserade säkerhetskontroller
- vanliga webbapplikationsrisker
- exempel på hur man angriper webbapplikationer

Block 4 - 4 dagar

➔ **En säker IT-miljö - hackning**
- hur genomför man en hackning?
- principer och procedurer för hackning
- casebaserade tillvägagångssätt för hackning baserad på miljö

➔ **En säker IT-miljö - penetratrationstester**
- vad är penetrationstester, red/blue/purple team?
- så beställer man ett penetrationstest
- hur kan rapporten se ut och vad gör man med den?

➔ **En säker IT-miljö - labbdag**
- testa verktyg
- testa att hacka
- testa forensic

➔ **Diplomeringsdag**
- test på att förstå attackscenarion baserat på MITRE Attack Framework
- läs en sårbarhet och förstå vad som hänt
- teoretiskt test

FÖRETAGS UNIVERSITETET

Telefon: 08-600 62 00
E-post: kurs@foretagsuniversitetet.se
www.foretagsuniversitetet.se