IT-säkerhetstekniker

400 YH-poäng

Motsvarande ca 2 års studier

Platsbunden undervisning i Stockholm

Lernia Yrkeshögskola avser starta en YH-utbildning inriktad mot praktisk IT-säkerhet i Stockholm. Utbildningen är utformad för att möta ett växande behov av kvalificerade IT-säkerhetstekniker inom området cyber- och informationssäkerhet. Genom att fokusera på hands-on-färdigheter och avancerade säkerhetslösningar, förbereder vi våra studerande på att skydda IT-infrastruktur, förebygga cyberintrång och hantera säkerhetsincidenter. Vi söker nu företag som vill vara med och stötta vår satsning och tillsammans säkerställa kompetensförsörjningen för en robust och säker IT-infrastruktur.

Kort om utbildningen

Utbildningen är planerad att bedrivas med ett hybridupplägg från Stockholm. Den blandar platsbunden undervisning med digitala föreläsningar, vilket innebär att den kan attrahera sökande från närliggande orter och regioner likväl som på huvudorten. För att bli antagen till utbildningen krävs gymnasieexamen samt godkänt i kurserna Engelska 6 och Svenska 2 eller Svenska som andraspråk 2.

Innehållet är framtaget av branschexperter och flertalet arbetsgivare har varit med att forma både innehåll och upplägg. Vi strävar alltid efter att våra ledningsgrupper ska bestå av representanter från olika verksamheter för att ta in flera olika perspektiv och säkerställa kvalitet i genomförandet.

Kursöversikt som kommer att gälla vid beviljandebeslut från MYH

5 Yrkeshögskolepoäng motsvarar en veckas heltidsstudier

Brandväggar	30
Examensarbete	20
Härdning av Linux	30
Härdning av Windows Server	30
IAM	30
IT-juridik och informationssäkerhet	30
LIA – lärande i arbete	70
Logghantering	25
Nätverksteknik	30
Operativsystem Linux	40
Operativsystem Windows Server	40
Penetrationstestning	25
Totalt	**400**

Senast uppdaterad: 2026-08

Kursbeskrivning

Brandväggar
I kursen arbetar de studerande med konfiguration och administration av brandväggsystem genom användning av Linux-baserade verktyg. Studenterna kommer lära sig de grundläggande och avancerade funktioner för att bygga brandväggar som skyddar nätverk mot obehörig åtkomst och andra cyberhot. Kursen inkluderar hands-on övningar där studenterna kommer lära sig att konfigurera och optimera brandväggar i verklighetsbaserade scenarier, inklusive teknologier som NAT, VPN och trafikfiltrering och principer inom Zero Trust. Detta hjälper eleverna att utveckla de färdigheter som krävs för att effektivt säkerställa nätverkssäkerhet och hantera komplexa säkerhetssystem

Examensarbete
Syftet med kursen är att den studerande ska fördjupa sig inom ett område som är centralt för utbildningen genom att utföra ett självständigt projekt. Examensarbetet kan med fördel utföras i samband med LIA för företaget som tillhandahåller platsen och innehållet ska bygga på genomförda kurser. Målet är att den studerande självständigt ska planera, utföra och presentera ett IT-säkerhetsprojekt, samt hantera de problem som kan uppstå under projektets gång. Målet är även att lära sig reflektera och utvärdera det egna arbetet samt att kunna presentera resultatet i olika former. Arbetet ska korrekt dokumenteras och utföras på ett professionellt sätt, och den studerande ska kunna presentera projektet med hänsyn till formella regler, källkritik och struktur. Examination sker skriftligen i form av en rapport och muntligen i form av en presentation.

Härdning av Linux
Kursen ger de studerande kunskaper och färdigheter att säkra Linux-system mot flera olika typer av hot och attacker. Kursen fokuserar på härdning av operativsystemet Linux enligt best practice, där de studerande lär sig att genomföra säkerhetsåtgärder för att skydda system. Genom praktiska moment får de studerande tillämpa sina kunskaper genom att konfigurera och administrera säkerhetsinställningar, brandväggar och tjänster. Vid avslutad kurs ska de studerande ha utvecklat förmågan att härda och administrera Linux-system för att skydda dem mot hot och attacker.

Härdning av Windows Server
I kursen behandlas tekniker som stärker säkerheten i Windows Server-miljöer, genom att analysera och minska sårbarheter och förhindra intrång. De studerande lär sig om olika säkerhetskonfigurationer och policyinställningar som krävs för att skydda serverar mot interna och externa hot. Kursen täcker hela processen från installation till full drift av en härdad Windows Server, vilket ger de studerande färdigheter som direkt kan tillämpas i arbetslivet. Kursen inkluderar praktiska moment där de studerande lär sig att administrera säkerhetsåtgärder, optimera servrars säkerhet och hantera komplexa säkerhetsutmaningar.

IAM
Kursen ger de studerande kunskaper om principer och tekniker för identitets- och åtkomsthantering (IAM) inom IT-säkerhet. Kursen omfattar både teoretiska och praktiska aspekter av IAM, inklusive autentisering, auktorisering, och användarhantering. De studerande lär sig att implementera och administrera IAM-system för att säkerställa att rätt personer har tillgång till rätt resurser vid rätt tidpunkt. Kursen behandlar även hur IAM kan användas för att uppfylla juridiska och regulatoriska krav, såsom GDPR och NIS2. Genom praktiska moment får de studerande tillämpa sina kunskaper genom att konfigurera och administrera IAM-lösningar, inklusive Single Sign-On (SSO), Multi-Factor Authentication (MFA), och rollbaserad åtkomstkontroll (RBAC).

IT-juridik och informationssäkerhet
Kursen ger de studerande en förståelse för juridiska och regulatoriska aspekter som påverkar cybersäkerhet. Under kursen introduceras de studerande till flera aktuella lagar och regler, såsom GDPR, NIS2 och DORA, och hur dessa tillämpas i hanteringen av personuppgifter och företagsdata samt identitets- och åtkomsthantering. Kursen behandlar även juridiska konsekvenser av dataintrång samt ansvar och rättigheter relaterade till informationssäkerhet. Genom praktiska moment får de studerande möjlighet att tillämpa sina kunskaper i att hantera juridiska och

regulatoriska utmaningar inom cybersäkerhet. Vid avslutad kurs ska de studerande ha utvecklat förmågan att förstå, tillämpa och kommunicera juridiska och regulatoriska krav på svenska och engelska för att hantera information och data.

LIA – lärande i arbete

I kursen får de studerande en fördjupad kunskap om yrkesrollen och de får i praktiken tillämpa intjänade teoretiska kunskaper. Kursen förbereder de studerande för verkliga yrkessituationer så att de efter avslutad utbildning kan ta sig an uppdrag och tjänster på ett professionellt sätt i linje med branschens förväntningar. De studerande ska självständigt, med tillgång till handledning, utföra arbetsuppgifter som en IT säkerhetstekniker inom en verksamhet. De arbetsuppgifter som genomförs i LIA-kursen ska ha en direkt koppling till tidigare kursmoment och inkluderar moment som att arbeta med brandväggar, informationssäkerhet och härdning av olika system. Andra relevanta moment som utförs under LIA är att ta fram och presentera säkerhetsanpassningar med förankring i aktuella lagar och regelverk, övervaka logghantering och identifiera potentiella hot för den digitala IT-miljön. Efter kursen ska de studerande förstå hur organisationen har implementerat IT-säkerhet i sin verksamhet och kunna beskriva organisationens digitala infrastruktur, säkerhetsstrategier och rutiner för att hantera och motverka säkerhetshot.

Logghantering

I kursen får de studerande kunskaper om insamling, övervakning och analys av loggdata för att säkerställa IT säkerhet. Kursen behandlar hur loggdata kan användas för att upptäcka och reagera på säkerhetshot, prestandaproblem och systemfel. Kursen täcker även compliance, inklusive hur man hanterar loggar enligt riktlinjer från lagstiftning som GDPR och andra dataskyddslagar. Den inkluderar praktiska övningar där de studerande får möjlighet att hantera loggdata och identifiera kritiska aspekter av relevans för IT-säkerheten, samt föreslå och implementera relevanta åtgärder.

Nätverksteknik

I denna kurs får de studerande förståelse för hur datanätverk fungerar. Kursen omfattar design, konfiguration och underhåll av datanätverk, med fokus på nätverkssäkerhet och användning av nätverksverktyg och protokoll. Kursen syftar till att utveckla de studerandes färdigheter i relation till konfiguration av routing, nätverkssegmentering och brandväggar, samt integration med molntjänster. I kursen används olika modeller och verktyg för nätverkskommunikation, exempelvis OSI-modellen och TCP/IP-modellen. Därutöver introduceras de studerande till NIST Cybersecurity Framework och ISO/IEX 27001. I kursen behandlas även diagnostik och felsökning i nätverksmiljöer, vilket inkluderar användning av avancerade nätverksverktyg för att identifiera och lösa problem och risker. Kursen inkluderar praktiska moment där de studerande får möjlighet att planera, implementera och övervaka nätverk som stöder moderna datatjänster.

Operativsystem Linux

Kursen behandlar installation, konfiguration och administration av operativsystemet Linux, med fokus på att de studerande ska lära sig att hantera bastjänster som webbserver, databasserver och andra vanligt förekommande tjänster. Genom kursen får de studerande kunskaper om säkerhetshantering i Linux, inklusive rättighetshantering och användning av brandväggar. De utvecklar de färdigheter och kunskaper som behövs för att administrera Linux-miljöer och säkerställa att de fungerar pålitligt och säkert. Kursen inkluderar praktiska laborationer där de studerande får möjlighet att tillämpa sina kunskaper i komplexa Linux-miljöer och identifiera och hantera potentiella hot.

Operativsystem Windows Server

Kursen behandlar installation och administration av Windows Server-miljöer, vilket inkluderar både grundläggande och avancerade funktioner. Kursen omfattar hantering av olika roller och tjänster som Active Directory, DNS och DHCP. Kursen lägger särskilt fokus på användaradministration och de studerande lär sig att hantera användarkonton, grupper och behörigheter för att säkerställa en säker och kontrollerad miljö. Genom praktiska laborationer får de studerande möjlighet att underhålla Windows Server-miljöer och bygga robusta system, samt att identifiera och hantera säkerhetshot.

Penetrationstestning

Kursen behandlar både grundläggande och avancerade tekniker för etiska hackningsaktiviteter och säkerhetstestningar, inklusive riskhantering och sårbarhetsanalys. I kursen får de studerande förståelse

för hur angripare tänker och agerar för att hitta sårbarheter i IT system, webbapplikationer, nätverk, servermiljöer och molntjänster. De lär sig verktyg och metoder för att genomföra penetrationstestning, såsom Metasploit och Wireshark, med syftet att kunna genomföra säkerhetstestningar och skydda IT miljöer mot potentiella hot.