Blekinge Tekniska Högskola
Institutionen för datavetenskap

Revision: 1
Dnr: BTH-4.1.14-0827-2021

KURSPLAN

Datastyrd säkerhet

Data-Driven Security

3 högskolepoäng (3 credits)

Kurskod: DV2610
Huvudområde: Datavetenskap, Programvaruteknik
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Engelska
Gäller från: 2022-01-17
Fastställd: 2021-09-01

1. Beslut

Denna kurs är inrättad av dekan 2021-04-29. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2021-09-01 och gäller från 2022-01-17.

2. Förkunskapskrav

För tillträde till kursen krävs minst 120 hp varav 90 hp inom ett tekniskt område och minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare.)

3. Syfte och innehåll

3.1 Syfte

Dagens organisationer producerar en stor mängd av data. Denna kurs behandlar hur dessa data går att använda för cybersäkerhetsändamål. Kursen syftar till att studenterna skall lära sig hur man förvärvar (till exempel genom SIEM) och förbereder säkerhetsdata, från insamling och lagring till hantering och analys samt visualisering och presentation, hur data kan analyseras för att prediktera illasinnad beteende samt korrelera säkerhetshändelser. Kursen ger en förståelse för att lära sig att förstå och kommunicera säkerhetsproblem.

3.2 Innehåll

Kursen är en introduktion till tillämpning av data science inom säkerhet. Eftersom våra enheter och användare producerar stora mängder data behöver säkerhetspersonal ha en förståelse för hur vi kan extrahera användbar information ur den. Inom kursen kommer vi att fördjupa oss I grunderna för datainsamling, dess förberedelse och bearbetning, datahantering, analys och visualisering, inklusive grunderna för maskininlärning.

Kursen innefattar följande moment:
- Introduktion till Datastyrd Säkerhet
- Bygga en analytisk verktygslåda
- Utforskande analys för säkerhetsdata
- Repetition av nätverkssäkerhet
- Källor för insamling av nätverksdata
- Datainsamling
- Dataanalys
- Maskininlärning
- Visualisering av säkerhetsdata
- Design av instrumentbrädor för säkerhet

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten kunna:
- Kunna principerna för datainsamling, integrering, rensning och förbehandling.

• Förstå omfattningen av området datastyrd säkerhet, vad som räknas som spetskunskap inom området och målen att tillämpa datastyrd säkerhet.
• Kunna förklara begränsningar och svårigheter i tillämpningen av datastyrd säkerhet.

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:
• Tillämpa verktyg för att bearbeta säkerhetsdata och för att extrahera information ur den.
• Implementera färdiga men även anpassade lösningar för att hantera säkerheten genom data.

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:
• Utvärdera lämpliga applikationer av verktyg och metoder som presenteras I kursen och som är mest lämpliga för dess olika syften.

5. Läraktiviteter

Undervisningen sker i form av online föreläsningar, inspelat videomaterial, tillsammans med skrivet material, litteratur och forskningslitteratur. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare att ske via e-post, kursens lärplattform och via online möten.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2205	Inlämningsuppgift 1	1 hp	GU
2215	Inlämningsuppgift 2	1 hp	GU
2225	Inlämningsuppgift 3	1 hp	GU

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

Material såsom forskningsartiklar och annat kursmaterial tillhandahålls på kursens lärplattform, och rekommendationer för vidare läsning.