Digital forensik och incidentrespons

Digital Forensics and Incident Response
6 hp

Programkurs

TSIT14

Gäller från:

Fastställd av	**Huvudområde**	
Programnämnden för data- och medieteknik, DM	Informationsteknologi, Datateknik, Datavetenskap	
Fastställandedatum	**Utbildningsnivå**	**Fördjupningsnivå**
2023-08-31	Avancerad nivå	A1X
Reviderad av	**Utbildningsområde**	
	Tekniska området	
Revideringsdatum	**Ämnesgrupp**	
	Datateknik	
Gavs första gången	**Gavs sista gången**	
HT 2024		
Institution	**Ersätts av**	
Institutionen för systemteknik		

Kursen ges för

- Masterprogram i cybersäkerhet
- Civilingenjörsprogram i datateknik
- Civilingenjörsprogram i informationsteknologi
- Civilingenjörsprogram i mjukvaruteknik

Rekommenderade förkunskaper

Datornätverk, Etisk hackning

Lärandemål

I kursen undervisas om de grundläggande förutsättningarna och begränsningarna för digital forensik samt metoder för att kunna hitta och säkra spår i digitala system och värdera digital bevisföring.

Studenten ska efter avslutad kurs kunna:

- Definiera grundläggande begrepp och principer för digital forensik
- Redogöra för, välja och använda effektiva metoder för att hitta och säkra spår i digitala system.
- Redogöra för principer, utmaningar, metoder, och verktyg för hantering av cybersäkerhetsincidenter.
- Utreda händelseförlopp för cybersäkerhetsincidenter utifrån spår i digitala system.
- Presentera och värdera digital bevisföring.
- Redogöra för vilka lagar som är tillämpliga och hur de påverkar metodval och forensiska resonemang i exempelfall.
- Exemplifiera betydelsen av digital forensik för ett hållbart samhälle i meningen social och ekonomisk motståndskraft mot inre och yttre hot.

Kursinnehåll

Under kursen tas följande upp:

- Nätverksforensik
- Incidenthantering
- Digital forensik på hårdvara
- Mobil forensik
- Minnesforensik
- Forensik på bilder och filmer
- Logghantering, bevissäkring
- Särskilda frågor i SCADA-miljöer och kritisk infrastruktur
- Teoretiska modeller
- Avancerade och smalare ämnen, adversary simulation
- Lagar och digitalt forensiskt material som bevisföring

Undervisnings- och arbetsformer

Kursen består av ett antal föreläsningar och en laborationsserie

Examination

LAB1	Laboration	4 hp	U, G
TEN1	Skriftlig tentamen	2 hp	U, 3, 4, 5

Betygsskala

Fyrgradig skala, LiU, U, 3, 4, 5

Övrig information

Om undervisnings- och examinationsspråk

Undervisningsspråk visas på respektive kurstillfälle på fliken "Översikt". Examinationsspråk relaterar till undervisningsspråk enligt nedan:

- Om undervisningsspråk är ”Svenska” kan kursen ges i sin helhet på svenska eller delvis på engelska. Examinationsspråk är svenska, men delar av examinationen kan ske på engelska.
- Om undervisningsspråk är Engelska ges kursen i sin helhet på engelska. Examinationsspråk är engelska.
- Om undervisningsspråk är ”Svenska/Engelska” ges kursen i sin helhet på engelska om studenter utan tidigare kunskap i svenska språket deltar. Examinationsspråk följer undervisningsspråk.

Övrigt

Kursen bedrivs på ett sådant sätt att likvärdiga villkor råder med avseende på kön, könsöverskridande identitet eller uttryck, etnisk tillhörighet, religion eller annan trosuppfattning, funktionsnedsättning, sexuell läggning och ålder.

Planering och genomförande av kurs skall utgå från kursplanens formuleringar. Den kursvärdering som ingår i kursen skall därför genomföras med kursplanen som utgångspunkt.

Kursen är campusförlagd på den ort som anges för kurstillfället om inget annat anges under ”Undervisnings – och arbetsformer”. I en campusförlagd kurs kan dock enstaka moment på distans ingå.