EP2780 Digital forensik och incidenthantering 7,5 hp

Digital forensics and incident response

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Fastställande

Kursplanen gäller från och med HT 2022 enligt skolchefsbeslut: J-2021-1872.Beslutsdatum: 2021-10-14

Betygsskala

A, B, C, D, E, FX, F

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

Kunskaper i cybersäkerhet, 7,5 hp, motsvarande slutförd kurs DD2391 alternativt slutförda kurser DD2394 och DD2395.

Aktivt deltagande i kursomgång vars slutexamination ännu inte är Ladokrapporterad jämställs med slutförd kurs.

Den som är registrerad anses vara aktivt deltagande.

Med slutexamination avses både ordinarie examination och det första omexamination-stillfället.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna,

inom kunskapsformerna kunskap och förståelse:

- beskriva centrala begrepp, modeller och metoder inom digital forensik och incidenthantering
- beskriva de nationella och internationella sammanhang och de lagar, förordningar och konventioner som förhandlas fram där och hur de tillämpas både internationellt och nationellt
- beskriva skillnader och likheter mellan ett forensiskt scenario och ett incidenthanteringsscenario,

inom kunskapsformerna färdighet och förmåga:

- tillämpa kända metoder för datainsamling och analys i givna situationer
- planera och genomföra datainsamling och analys för att genomföra en forensisk- eller analys eller incidentanalys
- presentera och förklara slutsatser från en forensisk analys
- presentera och förklara slutsatser från en incident samt föreslå framtida åtgärder,

inom kunskapsformerna värderingsförmåga och förhållningssätt:

- förklara begränsningar med forensisk analys med avseende på hur säkra slutsatser som kan dras
- förklara hur föregående skiljer mellan digital forensik och incidenthantering
- kritiskt och källkritiskt granska en forensisk- och incidenthanteringsrapport
- värdera när forensiskt arbete (särskilt när det inte sker i samband med en brottsundersökning) har en negativ inverkan på enskildas personliga integritet.

Kursinnehåll

Kursen ger studenten både praktiska och teoretiska kunskaper om tekniker, metoder, modeller, lagar/regler som gäller vid utredning av digitala brott eller incidenter.

Kursen behandlar bland annat följande:

- Forensikens historia
- Digital forensik och digitala bevis

- Den forensiska/incidenthanterande utredande processen
- Lagstiftning och internationella samarbeten inom digital forensik
- Standarder inom området och kraven på en organisation som arbetar med digital forensik eller incidenthantering
- Datorforensik
- Forensik för inbyggda system och mobila enheter
- Nätverksforensik

Examination

- LAB1 - Laborationer, 2,0 hp, betygsskala: P, F
- PRO1 - Projekt, 2,5 hp, betygsskala: P, F
- TEN1 - Skriftlig tentamen, 3,0 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.