KURSPLAN

Cybersecurity operations och incidenthantering, 7,5 högskolepoäng

Cybersecurity Operations and Incident Response, 7.5 credits

Kurskod:	TCOS25	**Utbildningsnivå:**	Avancerad nivå
Fastställd av:	VD 2024-03-01	**Utbildningsområde:**	Tekniska området
Gäller fr.o.m.:	2025-01-01	**Ämnesgrupp:**	DT1
Version:	1	**Fördjupning:**	A1F
		Huvudområde:	Datavetenskap

Lärandemål

Efter genomgången kurs skall studenten:

Kunskap och förståelse
- visa kunskap om centrala standarder och ramverk för cybersecurity operations och incidenthantering
- visa kunskap om centrala koncept och tekniker för nätverkssäkerhet och intrångsdetektering
- visa kunskap om olika verktyg för övervakning, digital forensik och bevisinsamling

Färdighet och förmåga
- visa färdighet i att använda övervakningsverktyg för digital forensik, intrångsdetektering och logghantering
- visa färdigheter i att skapa och använda en incidenthanteringsplan

Värderingsförmåga och förhållningssätt
- visa insikt om de olika faserna av en cyberattack och föreslå hur en organisation kan skydda sig mot cyberattacker under de olika faserna
- visa insikt i de samhälleliga, juridiska och etiska aspekterna av cybersecurity operations och incidenthantering

Innehåll

Cybersecurity operations är avgörande för att skydda en organisations tillgångars konfidentialitet, integritet och tillgänglighet. Kursen inleds med att diskutera centrala standarder och ramverk för cybersecurity operations och incidenthantering. Kursen innehåller tekniska begrepp som rör nätverkssäkerhet, intrångsdetektering, övervakning och digital forensik. Under kursen kommer studenterna att få praktisk erfarenhet av vanliga verktyg som används för övervakning, digital forensik och intrångsdetektering.

Kursen innehåller följande moment:
- Centrala standarder och ramverk för cybersecurity operations, konceptet Security Operations Center (SOC), blue team, etc....

- Centrala standarder och ramverk för incidentrespons (t.ex. NIST SP800-61), olika faser i incidentresponsplanen och hantering av cybersäkerhetsincidenter
- Olika faser av en cyberattack (t.ex. Cyber Kill Chain, MITER ATT&CK, attackträd, hotintelligens, etc.)
- Nätverkssäkerhetskoncept inklusive intrångsdetektering, brandväggar, network admission control, virtuella privata nätverk, etc.)
- Digital forensik och digital bevisning, inklusive dator- och nätverksforensik
- Säkerhetsrelaterad övervakning, analys av intrångsdata, security information and event management (SIEM)

Undervisningsformer

Föreläsningar, laborationer och projekt.

Undervisningen bedrivs på engelska.

Förkunskapskrav

Godkända kurser med lägst 90 hp i huvudområdet Datavetenskap, Informatik, Informationssystem, Datateknik eller motsvarande, samt genomgången kurs Etisk hackning och penetrationstestning, 7,5 hp eller motsvarande. Dessutom krävs kunskaper i Engelska 6 eller motsvarande.

Examination och betyg

Kursen bedöms med betygen 5, 4, 3 eller Underkänd.

Poängregistrering av examinationen för kursen sker enligt följande system:

Examinationsmoment	Omfattning	Betyg
Projekt[I]	4 hp	5/4/3/U
Laboration	2 hp	U/G
Seminarium	1,5 hp	U/G

[I] Bestämmer kursens slutbetyg vilket utfärdas först när samtliga moment godkänts.

Kurslitteratur

Kurslitteraturen fastställs åtta veckor före kursstart.