KURSPLAN

Kurskod: **CYS200**

Cybersäkerhet, 7,5 hp
Cyber Security, 7,5 HE credits

Beslutad: 2018-11-05
Beslutande: Institutionen för Ingenjörsvetenskap
Gäller från: V19

Kursens mål
Studenten skall efter genomgången kurs kunna:

Kunskap och förståelse
- beskriva en cybersäkerhetsanalytikers roll inom industrin
- beskriva skillnader samt fördelar med olika typer av operativsystem såsom Windows och Linux ur säkerhetssynpunkt
- beskriva problematiken med kryptering när det kommer till dataavlyssning
- beskriva hur incidenter hanteras av Computer Security Incident Response Teams (CSIRTs)
- redogöra för olika typer av cybersäkerhetsattacker samt klassifieringar
- beskriva hur man undersöker ändstationers sårbarheter och attacker
- utvärdera olika typer av larmmeddelanden.

Färdighet och förmåga

- klassificera olika typer av cybersäkerhetsattacker
- använda sig av olika metoder för att motverka skadlig åtkomst till nätverk, data samt användare
- analysera datakommunikationsintrång och identifiera sårbarheter i nätet
- använda sig av monitoreringsverktyg för identifiering av olika typer av datakommunikationsattacker

Behörighetskrav
Grundläggande behörighet samt godkänt resultat från följande kurs/kurser:
GRS210-Grundläggande router och switchteknik eller motsvarande.

Formerna för bedömning av studenternas prestationer
Individuell skriftlig tentamen samt projektarbete med muntlig redovisning i grupp

Övriga föreskrifter
Betygskala: Underkänd, Godkänd eller Väl godkänd
Undervisningsspråk: Svenska

Generella regler för examination vid Högskolan Väst finns på www.hv.se.

Om den studerande har ett beslut/rekommendation om särskilt pedagogiskt stöd på grund av funktionsvariation har examinator rätt att examinera den studerande i en anpassad examinationsform.

Nivå
Grundnivå

Successiv fördjupning
G1F - grundnivå, har mindre än 60 hp kurs/er på grundnivå som förkunskapskrav

Huvudområde(n)
Datateknik

Cybersäkerhet, 7,5 hp
Cyber Security, 7,5 HE credits

Kursens innehåll

I dagens samhälle där digitaliseringen utvecklas med stormsteg i form av big data, cloud computing och internet of things, ökar också fokuset på cybersäkerhet. Den största problematiken för cybersäkerhet är den ständiga och framför allt snabba utvecklingen av nya enheter som skall kunna kommunicera med varandra från vart som helst när som helst.
Med bakgrund i dessa ständiga förändringar har cybersäkerhet ett proaktivt och adaptivt förhållningssätt, genom kontinuerlig övervakning och realtidsbedömningar. Kärnan av cybersäkerhet består av metoder för analys och klassificering av datakommunikation för att kunna identifiera samt motverka attacker i realtid.
Kursen utgår från cybersäkerhetsanalytikerns olika roller ur ett industriellt perspektiv. Vidare ingår att kunna analysera olika typer av datakommunikation. Med hjälp av olika typer av monitoreringsverktyg kunna identifiera olika typer av cyberattacker, samt tillämpa olika metoder för att upptäcka samt stoppa pågående cybersäkerhetsattacker.