RTU studiju kurss "Kiberdrošības incidentu pārvaldība"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE1041
Nosaukums	Kiberdrošības incidentu pārvaldība
Studiju kursa statuss programmā	Brīvās izvēles
Atbildīgais mācībspēks	Vladislavs Minkevičs - Docents (praktiskais)
Mācībspēks	Rūta Pirta - Doktors, Docents
Apjoms daļās un kredītpunktos	1 daļa, 5.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV
Anotācija	Kiberdrošības incidents ir notikums, kas apdraud ar datortīklu un informācijas sistēmu starpniecību pieejamu datu un pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti. Studiju kurss paredzēts, lai apgūtu kiberdrošības incidentu pārvaldības pamatus. Tas ietver arī praktiskas metodes un rīkus kiberdrošības incidentu atklāšanā un izmeklēšanā. Studiju kurss sniedz nepieciešamās zināšanas ENISA lomai "Kiberdrošības incidentu reaģēšanas speciālists".
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Kursa mērķis ir sniegt zināšanas un prasmes par kiberdrošības incidentiem un to apstrādi. Studiju kursa uzdevumi: - radīt izpratni par kiberdrošību, iespējamiem kiberdrošības incidentiem un to pārvaldību; - izskaidrot kiberdrošības incidentu rašanās cēloņus; - radīt izpratni par datu avotiem, kuri nepieciešami veiksmīgai kiberdrošības incidenta identifikācijai; - sniegt ieskatu par auditācijas pierakstu veidiem; - radīt izpratni par tīkla datu analīzi; - iemācīt eksportēt informāciju no tīkla datu plūsmas; - sniegt ieskatu ielaušanas noteikšanas/novēršanas sistēmu darbībā; - attīstīt prasmes veidot automatizācijas procesus drošības incidentu apstrādē; - attīstīt prasmes veidot skriptus.
Patstāvīgais darbs, tā organizācija un uzdevumi	Kiberdrošības incidentu avotu izpēte. Kiberdrošibas apstrādes rīku pieietojums. Programmēšanas valodu pielietojums kiberdrošības incidentu apstrādei.
Literatūra	Obligātā. / Obligatory: National Institute of Standards and Technology. Guide to Intrusion Detection and Prevention Systems Recommendations of the National Institute of Standards and Technology NIST Special Publication 800-94 NIST. Incident Response Recommendations and Considerations for Cybersecurity Risk Management NIST Special Publication 800 April 2024 wirexsystems.com. Step-By-Step Guide To An Effective Incident Response Plan Incident response refers to the systematic approach taken to address and handle the consequences of a security breach or attack, aiming to minimize harm and restore regular operations promptly. Web lapa 2024.g Omar Santos. Network Security with NetFlow and IPFIX Cisco Press 800 East 96th Street Indianapolis, Indiana 46240 USA Network Security with NetFlow and IPFIX Big Data Analytics for Information Security Cisco Press Papildu. / Additional: cisa.gov. Cybersecurity Incident & Vulnerability Response Playbooks TLP:CLEAR Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems Publication: November 2021 cisa.gov. Cybersecurity Best Practices https://www.cisa.gov/topics/cybersecurity-best-practices tīmekļa lapa
Nepieciešamās priekšzināšanas	Pamata zināšanas par serveru un darbstaciju auditācijas pierakstiem.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Kiberdrošības incidentu pārvaldība.	6	2	0	0
Sistēmu ievainojamības un to izmantošanas veidi.	4	3	0	0
Auditācijas pieraksti.	6	7	0	0
Datu pierakstu veidi (Syslog, Json u.c.).	4	9	0	0
Metodes kā uzkrāt un apstrādāt auditācijas pierakstus.	8	6	0	0
Tīkla datu informācijas apstrāde.	6	6	0	0
Datu eksports no tīkla datu plūsmas.	7	4	0	0
Ielaušanās noteikšanas un novēršanas sistēmas.	5	5	0	0
Auditācijas pierakstu uzkrāšanas un analīzes platformas (SIEM, SOC).	6	4	0	0
Kiberdrošības incidentu pārvaldības automatizācijai nepieciešamo skriptu iztrāde.	11	14	0	0

Mākslīgā intelekta pielietošana drošības notikumu analīzei.	5	5	0	0
Kopā:	68	65	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Izprot kiberdrošības incidentu pārvaldības galvenos jēdzienus un spēj izskaidrot kiberdrošības incidentu rašanās cēloņus.	Tests un eksāmens (zināšanu pārbaudes testa formā). Testi iekļaus teorētiskos un praktiskos uzdevumiem. Lai veiksmīgi nokārtotu testus, ir jāatbild pareizi uz vismaz 70% jautājumu.
Spēj identificēt, uzkrāt, apstrādat un analizēt datu avotus kiberdrošības incidenta identifikācijai.	Praktiskie darbi, tests un eksāmens (zināšanu pārbaudes testa formā). Testi iekļaus teorētiskos un praktiskos uzdevumiem. Lai veiksmīgi nokārtotu testus, ir jāatbild pareizi uz vismaz 70% jautājumu.
Spēj pielietot Ielaušanās noteikšanas un novēršanas sistēmas.	Praktiskie darbi, tests un eksāmens (zināšanu pārbaudes testa formā). Testi iekļaus teorētiskos un praktiskos uzdevumiem. Lai veiksmīgi nokārtotu testus, ir jāatbild pareizi uz vismaz 70% jautājumu.
Spēj izveidot skriptus kiberdrošības incidentu pārvaldības automatizācijai.	Praktiskie darbi. Izveidoti vismaz 3 skripti, kurus var pielietot kiberdrošības incidentu pāvaldības automatizācijai.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Eksāmens	49
Tests	20
Prakstiskais darbs	31
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi			Brīvās izvēles pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs	Ieskaite	Eksām.	Darbs
1.	5.0	40.0	28.0	0.0		*				