FIŞA DISCIPLINEI
Anul universitar 2022-2023

Decan,
Prof. Vasile-Ion Manta

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică „Gheorghe Asachi” din Iași
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și tehnologia informației
1.5 Ciclul de studii[1]	Masterat
1.6 Programul de studii	Securitatea spațiului cibernetic

2. Date despre disciplină

2.1 Denumirea disciplinei/Cod				Tratarea incidentelor de securitate cibernetică / SSC.IA.201			
2.2 Titularul activităţilor de curs				ș.l. dr. ing. Cristian-Mihai Amarandei			
2.3 Titularul activităţilor de aplicaţii				ș.l. dr. ing. Cristian-Mihai Amarandei			
2.4 Anul de studii[2]	2	2.5 Semestrul[3]	3	2.6 Tipul de evaluare[4]	Examen	2.7 Tipul disciplinei[5]	DS

3. Timpul total estimat al activităţilor zilnice (ore pe semestru)

3.1 Număr de ore pe săptămână	4	din care 3.2 curs	2	3.3a sem.	-	3.3b laborator	2	3.3c proiect	-
3.4 Total ore din planul de învăţământ[6]	56	din care 3.5 curs	28	3.6a sem.	-	3.6b laborator	28	3.6c proiect	-

Distribuţia fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie şi notiţe	34
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	26
Pregătire seminarii/laboratoare/proiecte, teme, referate şi portofolii	26
Tutoriat[8]	4
Examinări[9]	4
Alte activităţi:	

3.7 Total ore studiu individual[10]	94
3.8 Total ore pe semestru[11]	150
3.9 Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum[12]	●
4.2 de competenţe	●

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului[13]	● Tablă, videoproiector
5.2 de desfăşurare a seminarului / laboratorului / proiectului[14]	● Sală de laborator cu calculatoare și acces la internet ● Sisteme de operare: Linux, Windows ● Pachete software: software de virtualizare

[1] *Licenţă / Master*

[2] *1-4 pentru licenţă, 1-2 pentru master*

[3] *1-8 pentru licenţă, 1-3 pentru master*

[4] *Examen, colocviu sau VP A/R – din planul de învăţământ*

[5] *DF - disciplină fundamentală, DID - disciplină în domeniu, DS – disciplină de specialitate sau DC - disciplină complementară - din planul de învăţământ*

[6] *Este egal cu 14 săptămâni* x *numărul de ore de la punctul 3.1 (similar pentru 3.5, 3.6abc)*

[7] *Liniile de mai jos se referă la studiul individual; totalul se completează la punctul 3.7.*

[8] *Între 7 şi 14 ore*

[9] *Între 2 şi 6 ore*

[10] *Suma valorilor de pe liniile anterioare, care se referă la studiul individual.*

[11] *Suma dintre numărul de ore de activitate didactică directă (3.4) şi numărul de ore de studiu individual (3.7); trebuie să fie egală cu numărul de credite alocat disciplinei (punctul 3.9)* x *24 de ore pe credit.*

[12] *Se menţionează disciplinele obligatoriu a fi promovate anterior sau echivalente*

[13] *Tablă, vidoproiector, flipchart, materiale didactice specifice etc.*

[14] *Tehnică de calcul, pachete software, standuri experimentale, etc.*

6. Competenţele specifice acumulate[15]

		Număr de credite alocat disciplinei[16]: **6**	Repartizare credite pe competenţe[17]
Competenţe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	1.4
	CP2	Cercetarea științifică și practică privind securitatea sistemelor informatice complexe.	1.2
	CP3	Rezolvarea problemelor pe baza metodelor și tehnologiilor de securizare a sistemelor informatice complexe.	1
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităților și a amenințărilor de securitate cibernetică.	1
	CP5	Proiectarea și dezvoltarea de soluții software cu un înalt grad de securitate orientate pe prevenția și răspunsul la incidente de securitate cibernetică.	1
	CP6		
	CPS1		
	CPS2		
Competenţe transversale	CT1	Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.	0.1
	CT2	Identificarea rolurilor și responsabilităților într-o echipă specializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei.	0.1
	CT3	Dezvoltarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.	0.2
	CTS	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	• Înțelegerea conceptelor și formarea abilităților de implementare corectă a instrumentelor de securitate la nivelul organizațiilor
7.2 Obiective specifice	• Prezentare generală a contextului standardizat de tratare a incidentelor de securitate cibernetică • Dezvoltarea capacității de gestionare a vulnerabilităților, riscurilor și amenințărilor din domeniul securității cibernetică, în contextul mai larg al securității organizaționale • Dezvoltarea capacității de elaborare a politicii de securitate cibernetică într-o organizație, a planului de răspuns la incidente de securitate.

8. Conţinuturi

8.1 Curs[18]	Metode de predare[19]	Observaţii
1. Introducere în Cyber Defence (4h) 1.1. Diferența dintre standard și protocol în securitatea cibernetică 1.2. Standarde în securitatea cibernetică. Context și politică de aplicabilitate ISO 27K. Tehnici de securitate ISO/IEC JTC 1/SC 27 1.3. Framework-uri de răspuns la incidente de securitate. NIST (SP) 800-61, ISO/IEC 27035 1.4. Cuantificarea riscului în domeniul securității cibernetice. NIST (SP) 800-30, ISO/IEC 27005, OCTAVE 2. Cyber Kill Chain (2h) 2.1. AT&T Internal Cyber Kill Chain Model 2.2. Unified Kill Chain 2.3. Matricea MITRE ATT&CK 3. Vectori de atac (2h) 3.1. Specificul țintelor de tip Hosts și Network 3.2. Atacuri active	prelegere cu videoproiector	

[15] *Competenţele din Grilele G1 şi G1bis ale programului de studii, adaptate la specificul disciplinei, pentru care se repartizează credite (www.rncis.ro sau site-ul facultăţii)*

[16] *Din planul de învăţământ*

[17] *Creditele alocate disciplinei se distribuie pe competenţe profesionale şi transversale în funcţie de specificul disciplinei*

[18] *Titluri de capitole şi paragrafe*

[19] *Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuţii cu studenţii (pentru fiecare capitol, dacă este cazul)*

3.3. Atacuri pasive 4. Arhitectura de securitate a infrastructurilor cibernetice (2h) 4.1. Rolul CSIRT / SOC 4.2. Rolul SIEM în SOC 4.3. SOC-as-a-Service 5. Arhitectura și principiile unui SIEM/SOC (4h) 5.1. Procesarea log-urilor - Management, Normalizare, Surse 5.2. Corelări, Alerte, Managementul incidentelor 5.3. Componentele ELK 5.4. Arhitectura și procesele Splunk 5.5. Arhitectura și componentele ArcSight ESM 6. Analiza serviciilor de rețea cu ajutorul SIEM/SOC (4h) 6.1. Precursori SIEM. 6.1.1. HIDS (Host-Based Intrusion Detection Systems). 6.1.2. NIDS (Network-Based Intrusion Detection Systems). 6.1.3. FIM (File Integrity Monitoring). 6.1.4. ND&R (Network Detection and Response). 6.1.5. Studiu de caz - ExtraHop Reveal(x) 6.2. Utilizarea Machine Learning în ND&R 6.3. OSSEC în cadrul unui SIEM 6.4. Analiza la nivelul endpoint 6.4.1. Securizare 6.4.2. Colectare log-uri 6.4.3. Firewall 6.4.4. Logare evenimente 6.5. SIEM YARA Rules 7. Managementul incidentelor de securitate la nivelul SIEM/SOC (2h) 7.1. Security orchestration, automation and response (SOAR) 7.2. Exemplificarea componentelor SOAR folosind DFLabs 7.3. Splunk Phantom 8. Analiza post detecție (2h) 8.1. Principiile analizei tactice 8.2. Reanalizarea traficului de rețea 9. Conlucrarea în cazul unui incident de securitate cu un organism CERT (2h) 9.1. US-CERT Federal Incident Notification. CISA Incident Reporting System. Calculul NCISS. 9.2. CERT-EU. Taxonomii MISP. 9.3. Conlucrarea cu CERT-RO 10. Structura unui raport de incident de securitate. 5W. (2h) 10.1. Definirea workflow-ului schemei de raportare 10.2. Studiu de caz - Standardul CIP-008-6 - NERC 10.3. Studiu de caz - Cloud Security Incident Reporting - ENISA 11. Auditul de securitate. Ghiduri ISACA. Framework-ul COBIT. (2h)		

Bibliografie curs:

1. Eric C. Thompson, “Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents”, Apress, 2018
2. P. Cichonski et al., “Computer Security Incident Handling Guide”, NIST Special Publication 800-61, Revision 2, 2012
3. E. Hutchins, M. Cloppert, R. Amin, “Intelligence-Driven Computer Network DefenseInformed by Analysis of Adversary Campaigns andIntrusion Kill Chains”, Lockheed Martin, 2011
4. Cameron H. Malin, Eoghan Casey BS MA, James M. Aquilina, “Linux Malware Incident Response: A Practitioner’s Guide to Forensic Collection and Examination of Volatile Data”, Syngress, 2013
5. European Union Agency for Network and Information Security (ENISA), “Incident Handling Management Handbook, Document for Teachers”, 2016
6. European Union Agency for Network and Information Security (ENISA), “Good Practice Guide for Incident Management”, 2010
7. P. Kral, “Incident Handler's Handbook”, SANS Institute, 2020

8.2a Seminar	Metode de predare[20]	Observaţii

8.2b Laborator	Metode de predare[21]	Observaţii
1. YARA Rules (2h) 2. MISP (2x2h) 3. Instalare / configurare / utilizare OSSEC (2x2h)	demonstrații, discuții, analiză	

[20] *Discuţii, dezbateri, prezentare şi/sau analiză de lucrări, rezolvare de exerciţii şi probleme*

[21] *Demonstraţie practică, exerciţiu, experiment*

4. Instalare / configurare / utilizare SIEM ELK (3x2h) 5. Instalare / configurare / utilizare SIEM Splunk (3x2h) 6. ExtraHop Reveal(x) (2h) 7. Splunk Phantom Security Orchestration & Automation (2h) 8. SOAR DFLabs (2h)		
8.2c Proiect	Metode de predare[22]	Observaţii

Bibliografie aplicaţii (seminar / laborator / proiect):

1. R. Dias, "Intelligence-Driven Incident Response with YARA", SANS Institute, 2020
2. MISP Community, "User guide of MISP Malware Information Sharing", CIRCL, 2020
3. A. Hay, D. Cid, R. Bray, "OSSEC Host-Based Intrusion Detection Guide", Syngress, 2008
4. P. Shukla, S. Kumar, "Learning Elastic Stack 7.0: Distributed search, analytics, and visualization using Elasticsearch, Logstash, Beats, and Kibana", 2nd Edition, Packt Publishing, 2019
5. T. Marlette, "Splunk Best Practices", Packt Publishing, 2016
6. J. Diakun, P. Johnson, D. Mock, "Splunk Operational Intelligence Cookbook: Over 70 practical recipes to gain operational data intelligence with Splunk Enterprise", Packt Publishing, 2014
7. Dave Shackleford, "ExtraHop Reveal(x) Expands Attack Investigations to Cover All Vectors", SANS Institute, 2020
8. Splunk Phantom User Guide online
9. J. Moran, "Automate Your Incident Response Safely By Automating Selectively", DFLabs, 2019
10. H. Hixon, "The Most Comprehensive eBook on SOAR Use Cases", DFLabs, 2020

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului[23]

- Conţinutul disciplinei şi competenţelor specifice acumulate sunt corelate cu cerinţele academice şi profesionale şi corespund cerinţelor de pe piaţa muncii locală.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare		10.3 Pondere din nota finală
10.4a Examen	• Cunoştinţe teoretice şi practice însuşite (cantitatea, corectitudinea, acurateţea)	Teste pe parcurs[24]:		60% (minim 5)
		Teme de casă:		
		Alte activităţi[25]:		
		Evaluare finală:	100% (minim 5)	
10.4c Laborator	• Cunoaşterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea şi interpretarea unor rezultate	• Chestionar scris • Răspuns oral • Caiet de laborator (lucrări experimentale, referate) • Demonstraţie practică		40% (minim 5)
10.5 Standard minim de performanţă[26]				

Data completării, 13.01.2021

Semnătura titularului de curs,
ş.l. dr. ing. Cristian-Mihai Amarandei

Semnătura titularului de aplicaţii,
ş.l. dr. ing. Cristian-Mihai Amarandei

Data avizării în departament, 13.01.2021

Director departament,
Conf.dr.ing. Andrei Stan

[22] *Studiu de caz, demonstraţie, exerciţiu, analiza erorilor etc.*

[23] *Legătura cu alte discipline, utilitatea disciplinei pe piaţa muncii*

[24] *Se va preciza numărul de teste şi săptămânile în care vor fi susţinute.*

[25] *Cercuri ştiinţifice, concursuri profesionale etc.*

[26] *Se particularizează la specificul disciplinei standardul minim de performanţă din grila de competenţe a programului de studii, dacă este cazul.*