Kiberfizikai Rendszerek Intézet			Mintatanterv szerinti 4. félév 2025-26-2			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tgy	lab
SOAR - Security orchestration, automation and response	NKXSO1HMLF	5	levelező féléves	10	0	10
Tárgyfelelős: Prof. Dr. Lovas Róbert			Beosztás: professzor			
Oktató(lók): Rigó Ernő						
Előtanulmányi feltételek:	NBXNF2HMLF	Nyílt forráskódú SOC fejlesztés II. vagy NMLFKM képzés				
Számonkérés módja:	Évközi jegy					

A tananyag	
Oktatási cél:	A tantárgy célja, hogy a hallgatók megismerkedjenek a korábbi félévek során alkalmazásra kerülő biztonsági eszközkészlet és folyamatok integrációs és automatizálási lehetőségeivel. A tárgy az eddig megszerzett tudás gyakorlati alkalmazását célozza egy komplex biztonsági szolgáltatásokat nyújtó környezetben, projekt jellegű körülmények között.
Tematika:	A tárgy bemutatja a proaktív és reaktív incidenskezelés alapfogalmait, valamint ezek gyakorlati megvalósítási és automatizálási lehetőségeit, open source megoldásokon keresztül. Példákon keresztül illusztrálja a biztonsági környezet gyakori elemeinek konfiguráció menedzsment lehetőségeit. Megismerteti a SOAR koncepcióit és alkalmazási lehetőségeit. Tárgyalja a biztonsági riasztásokra és műveletekre vonatkozó, formalizált folyamat automatizálási lehetőségeket, valamint ismerteti a biztonsági adatok strukturált kezelésének, korrelációjának és gazdagításának módszereit, eszközkészletét. A tárgy különböző biztonsági területekre vonatkozó alkalmazási példák segítségével is tovább támogatja a hallgatók által önállóan megvalósításra kerülő, SOAR környezet kialakítását célzó projektfeladatának megvalósítását.

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Bevezetés az automatizált incidenskezelésbe, minőségi paraméterei (MTTD, MTTR, false ratio) és szintjei (RPA, SOAR, XDR)
2.	Nyílt forrású, automatizált incidensmenedzsment platformok (TheHive és HiveCortex)
3.	Biztonsági infrastruktúra instrumentációja és orkesztrációja (security playbooks)
4.	Riasztások automatizált kezelése
5.	Biztonsági műveletek automatizálása
6.	Automatizált fenyegetettség felderítés (threat hunting)
7.	Adatgazdagítás
8.	Use Case: Végpontvédelem
9.	Use Case: Hálózatvédelem
10.	Use Case: Felhasználóvédelem
11.	Use Case: Megtévesztés, csapdázás

12.	Use Case: Incidens elemzés
13.	Összefoglalás, projektbemutatók
14.	Projektbemutatók

Félévközi követelmények

Évközi jegy / aláírás megszerzésének feltételei:	Az órákon való részvétel legalább 70%-ban.

Zárthelyi dolgozatok

Oktatási hét	Témakör
13.	Projekt bemutató
14.	Projekt bemutató (pót)

Az *évközi jegy* kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)

- Projekt bemutató érdemjegy (100%)

Pótlás módja

A ZH / évközi jegy / aláírás pótlásának módja:	A HKR-ben előírtaknak megfelelően, a vizsgaidőszak első 10 munkanapjának valamelyikén az aláíráspótlás díj ellenében pótolható.

Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)

-

Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)

-

Az egyes érdemjegyek ponthatárai:

Elérhető eredmény	Érdemjegy
0-50%	Elégtelen (1)
51-62%	Elégséges (2)
63-74%	Közepes (3)
75-86%	Jó (4)
87-100%	Jeles (5)

Irodalom

Kötelező:	Moodle kurzusban kiadott elektronikus segédanyagok (előadások, jegyzetek)
Ajánlott:	[1] Aamir Lakhani, Cybersecurity Prevention and Detection, Pearson 2022, ISBN: 0137929358 [2] Gerard Johansen, Digital Forensics and Incident Response - Fourth Edition, Packt 2025, ISBN: 9781836200116 [3] Julien Vehent, Securing DevOps, Manning 2018, ISBN: 9781617294136 [4] Cynthia Brumfield, Brian Haugli, Cybersecurity Risk Management, Wiley 2021, ISBN: 9781119816287
Egyéb segédletek:	-