Biomatika és Alkalmazott Mesterséges Intelligencia Intézet			Mintatanterv szerinti 2. félév 2025-26-2			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tgy	lab
Logelemzés és SOC fejlesztés	NBXNF1ISLF	5	Levelező össz.	10	0	10
Tárgyfelelős: Vörösné Dr. Bánáti-Baumann Anna			Beosztás: adjunktus			
Oktató(k): Vörösné Dr. Bánáti-Baumann Anna						
Előtanulmányi feltételek:						
Számonkérés módja:	Évközi jegy					

A tananyag	
Oktatási cél:	A kurzus célja, hogy a hallgatók megismerkedjenek egy iztonsági Műveleti Központ (Security Operation Center, SOC) céljával és feladataival, a különböző nyílt forráskódú megoldásokkal, naplókezelő eszközökkel és eljárásokkal. A hallgatók egy projektmunka keretében saját SOC-példányt fejlesztenek, ahol egy SIEM-rendszert valósítanak meg a leggyakoribb felhasználási esetekkel és a hozzájuk tartozó riasztásokkal. A SOC-t további komponensekkel egészítik ki, például IDS/IPS rendszerekkel és egy általuk választott honeypot megoldással, miközben megismerkednek ezen eszközök feladataival és típusaival is.
Tematika:	A tanfolyam áttekinti a SOC célját, funkcióját és legfontosabb összetevőit és követelményeit. A kurzus labororientált, és erősíti a hallgatókban a projektszemlélet kialakítását. A félév során az elméleti alapok elsajátítása mellett a hallgatók 2 fős csoportokban kötnek be meglévő SOC technológiákba agenteket, logokon és forgalmi adatokon keresztül elemeznek normális és a normálistól eltérő mintázatokat, illetve riasztásokat definiálnak.

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Bevezetés - Az ellenfél megismerése – támadók, támadások, taktikák és technikák
2.	Bevezetés – A SOC működése – „people, process, technology”
3.	Logmenedzsment – a naplóadatok célja, típusai, gyűjtése
4.	Logmenedzsment – naplóadatok elemzése
5.	Felügyeleti és hálózat monitoring megoldások – eszközök és technikák
6.	Hálózati forgalomelemzés,
7.	Security and Information Event Management (SIEM)
8.	Riasztások megvalósítása és kezelése
9.	Végpontvédelem
10.	Behatolásdetektálás, Honeypotok
11.	Esettanulmányok
12.	Esettanulmányok
13.	Összefoglalás, projekt bemutatók, elméleti teszt
14.	Projektbemutatók, elméleti teszt - pótlás

Félévközi követelmények	
Évközi jegy / aláírás megszerzésének feltételei:	Az órákon való részvétel legalább 70%-ban, online teszt megírása legalább 80%-ra, illetve a projektfeladat elkészítése, dokumentálása és bemutatása a 13. és 14. héten (vagy egy előre egyeztetett időpontban). A féléves projektfeleadat 2 fős csoportokban egy kiberbiztonsági fenyegetés vagy

	támadás szimulálása egy erre a célra kialakított tesztkörnyezetben, a támadás végigkövetése a napló vagy forgalmi adatokon, továbbá detekciós szabály(ok) és riasztás megtervezése és megvalósítása a támadás detektálására.

Zárthelyi dolgozatok	
Oktatási hét	Témakör
13.	Projekt bemutatók, elméleti teszt
14.	Projekt bemutatók, elméleti teszt - pótlás

A féléves feladat (projektmunka) megvalósítására, dokumentálására és a bemutatására, valamint az elméleti tesztre kapott érdemjegyek átlaga.

Pótlás módja	
A ZH / évközi jegy / aláírás pótlásának módja:	Az aláíráspótló héten az online teszt és a projektmunka bemutatása pótolható.

-
-
Az egyes érdemjegyek ponthatárai:
Mind az elméleti teszt, mind a laborvizsga elvárt követelménye 80%-os eredmény.

Irodalom	
Kötelező:	Az órákon elhangzott előadások és jegyzetek.
Ajánlott:	A Cisco CyberOps tananyaga
Egyéb segédletek:	