Biomatika és Alkalmazott Mesterséges Intelligencia Intézet			Mintatanterv szerinti 2. félév 2024-25-1			
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, Dr. Leitold Ferenc						
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.	Incidenskezelés k
12.	Esettanulmányok
13.	Összefoglalás, projekt bemutatók
14.	Projektbemutatók

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
14.	Projekt bemutatók

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

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

Pótlás módja

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

Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)

-

Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)

-

Az egyes érdemjegyek ponthatárai:

Eredmény	**Érdemjegy**
81%-100%	**jeles (5)**
71%-80<%	**jó (4)**
61%-70<%	**közepes (3)**
51%-60<%	**elégséges (2)**
0%-50<%	**elégtelen (1)**

Irodalom

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