Biomatika és Alkalmazott Mesterséges Intelligencia Intézet			Választható tárgy 2025-26-2			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tgy	lab
Blue Team & Security Operations 2.	NBWBT2HBNF	4	heti	2	0	0
Tárgyfelelős: Dr. Póser Valéria			Beosztás: egyetemi docens			
Oktató(k): Dr. Póser Valéria, White Hat szakemberek,						
Előtanulmányi feltételek:	NBWBT1HBNF	Blue Team & Security Operations 1.				
Számonkérés módja:	Évközi jegy					

A tananyag	
Oktatási cél:	A kurzus célja, hogy a piacon hiánypótló, kézzelfogható tudást adjon át a nagyvállalatok biztonsági csapatában szerepkört betöltők vagy betölteni kívánók számára. A két féléves tárgy felöleli a nemzetközi White Hat Certified Defender képzés tananyagát.
Tematika:	A második félévben folytatjuk a tárgy első részében megismert szimulált kiberbiztonsági incidens nyomozását, a támadó további tevékenységeinek felderítésén keresztül. Ezek keretében bemutatunk malware elemzéshez szükséges módszereket és eszközöket, valamint a Windows rendszerek mellett kitekintünk a Linux szerverek, felhőtechnológiák, hálózatok és mobil operációs rendszerek biztonsági kihívásaira és az ilyen környezetekben rendelkezésre álló defenzív megoldásokra. Ahogy az első félévben is, itt is lehetőség nyílik a virtuális labor használatára. A tárgy lezárásaként megtörtént támadásokról mesélünk történeteket, párhuzamot vonva a két félév alatt megismert incidens reagálási módszertannal.

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1. hét 02.19.	Perzisztencia 1. – bevezetés
2. hét 02.26.	Perzisztencia 2. – malware analízis
3. hét 03.05.	Perzisztencia 2. – statikus malware analízis
4. hét 03.12.	Perzisztencia 2. – dinamikus malware analízis
5. hét 03.19.	Lateral movement 1. – Active Directory környezetben
6. hét 03.26.	Lateral movement 1. – Active Directory környezetben
7. hét 04.02.	Lateral movement 2. – Linux és cloud környezetben
8. hét 04.09.	Lateral movement 2. – Linux és cloud környezetben
9. hét 04.16.	Exfiltration 1. – hálózati forgalom, network forensics
10. hét 04.23.	Exfiltration 1. – hálózati forgalom, network forensics
11. hét 04.30.	Detekció és preventív intézkedések

12. hét 05.07.	Mobil operációs rendszerek
13. hét 05.14.	Incident response – történetek, módszertan
14. hét 05.21.	Áttekintés, összefoglalás, jegyajánlás, szóbeli pótlás
Félévközi követelmények	
Évközi jegy / aláírás megszerzésének feltételei:	Rendszeres részvétel az előadásokon (maximum 3 hiányzás). Félévközi gyakorlati feladatok pontszámban legalább elégségesre történő teljesítése.
Zárthelyi dolgozatok	
Oktatási hét	Témakör
13. hét	
14. hét	
Az *évközi jegy* kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)	
A A félévközi gyakorlati feladatok eredménye adja a félévzáró érdemjegyet 0-49% - elégtelen 50-59% - elégséges 60-69% - közepes 70-84% - jó 85+% - jeles	
Pótlás módja	
A ZH / évközi jegy / aláírás pótlásának módja:	14. héten a fenti feltételek teljesítése. A vizsgaidőszakban évközi jegy pótlás alkalmával egyszer van lehetőség pótolni.
Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)	
Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)	
Az egyes érdemjegyek ponthatárai:	
Irodalom	
Kötelező:	
Ajánlott:	• Arun E Thomas: Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence (CreateSpace Independent Publishing Platform (2018)) • Don Murdoch: Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: A condensed field guide for the Security Operations team (Volume 2) (CreateSpace Independent Publishing Platform; 1.0 edition (2018)) • Bryce G. Hoffman: Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything (Crown Business (2017))

	• Chris Sanders: Practical Packet Analysis, 3E: Using Wireshark to Solve Real-World Network Problems (No Starch Press; 3 edition (2017)) • Nik Alleyne: Learning By Practicing - Hack & Detect: Leveraging the Cyber Kill Chain for Practical Hacking and its Detection via Network Forensics (Independently published (2018)) • Michael Sikorski: Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software (No Starch Press; 1st edition (2012)) • Yuri Diogenes, Erdal Ozkaya: Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics (Packt Publishing (2018)) • Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich, David A. Solomon – Windows Internals Part 1. (7th Edition) • Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich, David A. Solomon – Windows Internals Part 2. (7th Edition)