ÓBUDAI EGYETEM JUBILEUMOK ÉVE
ÓE 15 145 630
HAGYOMÁNY ÉS INNOVÁCIÓ

THE World University Rankings 2025 TOP 800

NIS 2 támogatás kibergyakorlatokon keresztül

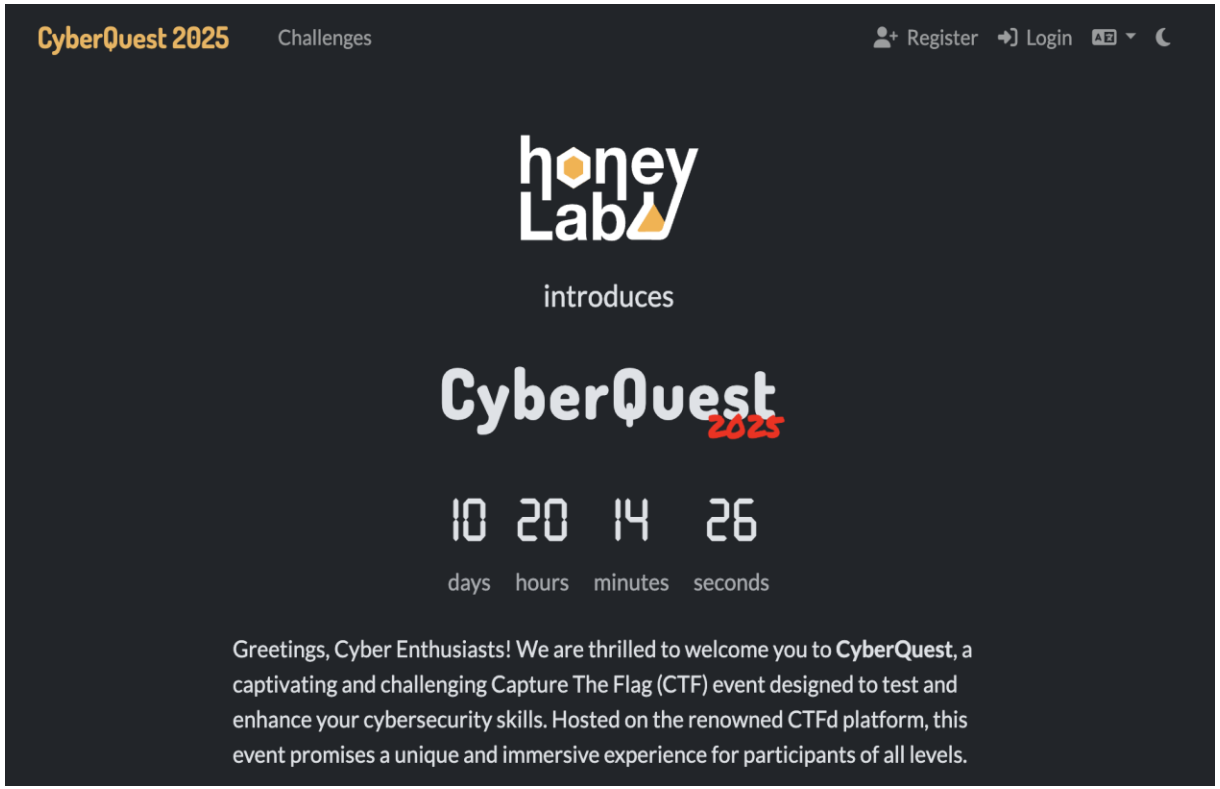
Dr. Bánáti-Baumann Anna

2025.09.17.

GAMIFIKÁCIÓ – CAPTURE THE FLAG

Az **első CTF verseny** 1993-ban volt a **DEF CON 1** konferencián Las Vegasban

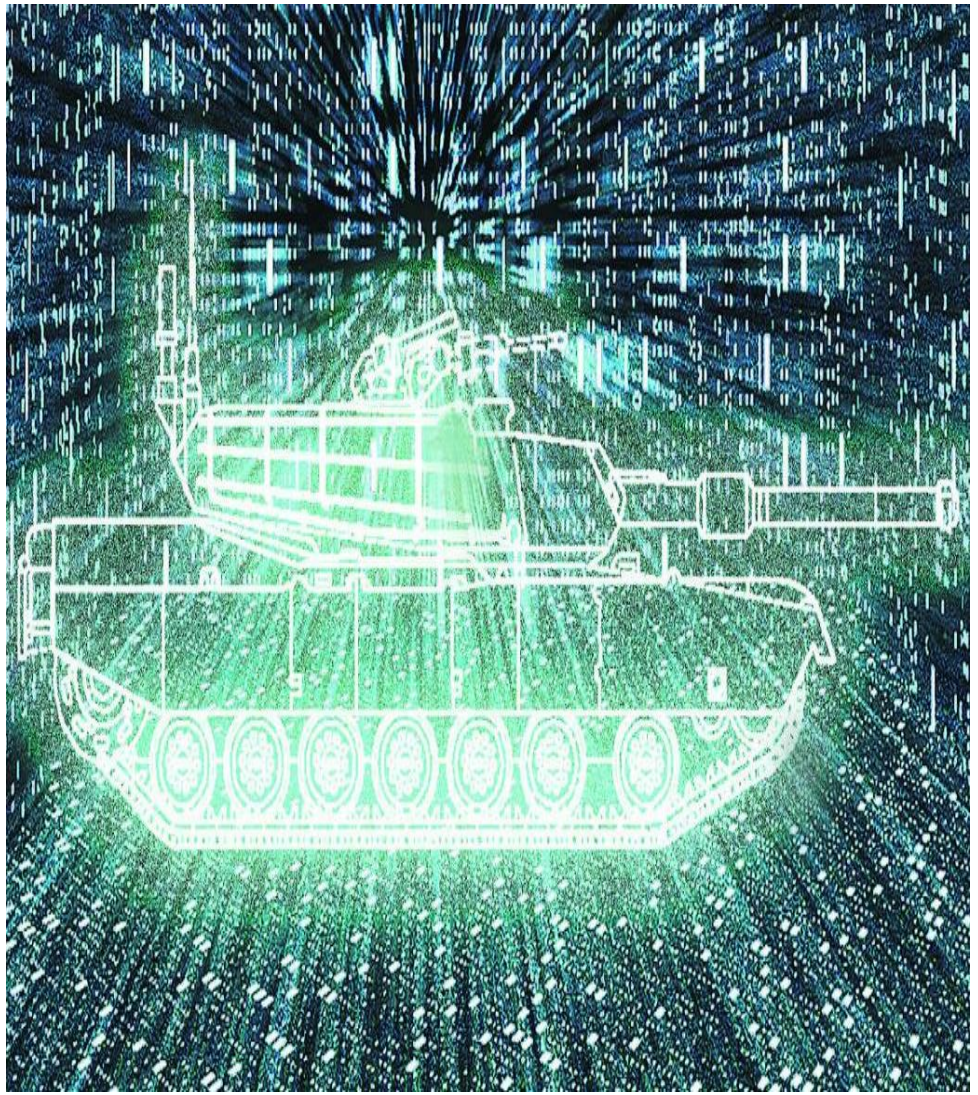
- Attack/Defence
- Jeopardy



KIBERVÉDELEM

2016-ban a NATO vezetői a kiberteret a szárazföld, a tenger és a levegő mellett **műveleti területként (cyber domain)** azonosították.

2010-ben rendezték meg az első **Locked Shields gyakorlatot** a NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE, Tallinn, Észtország) szervezésében.



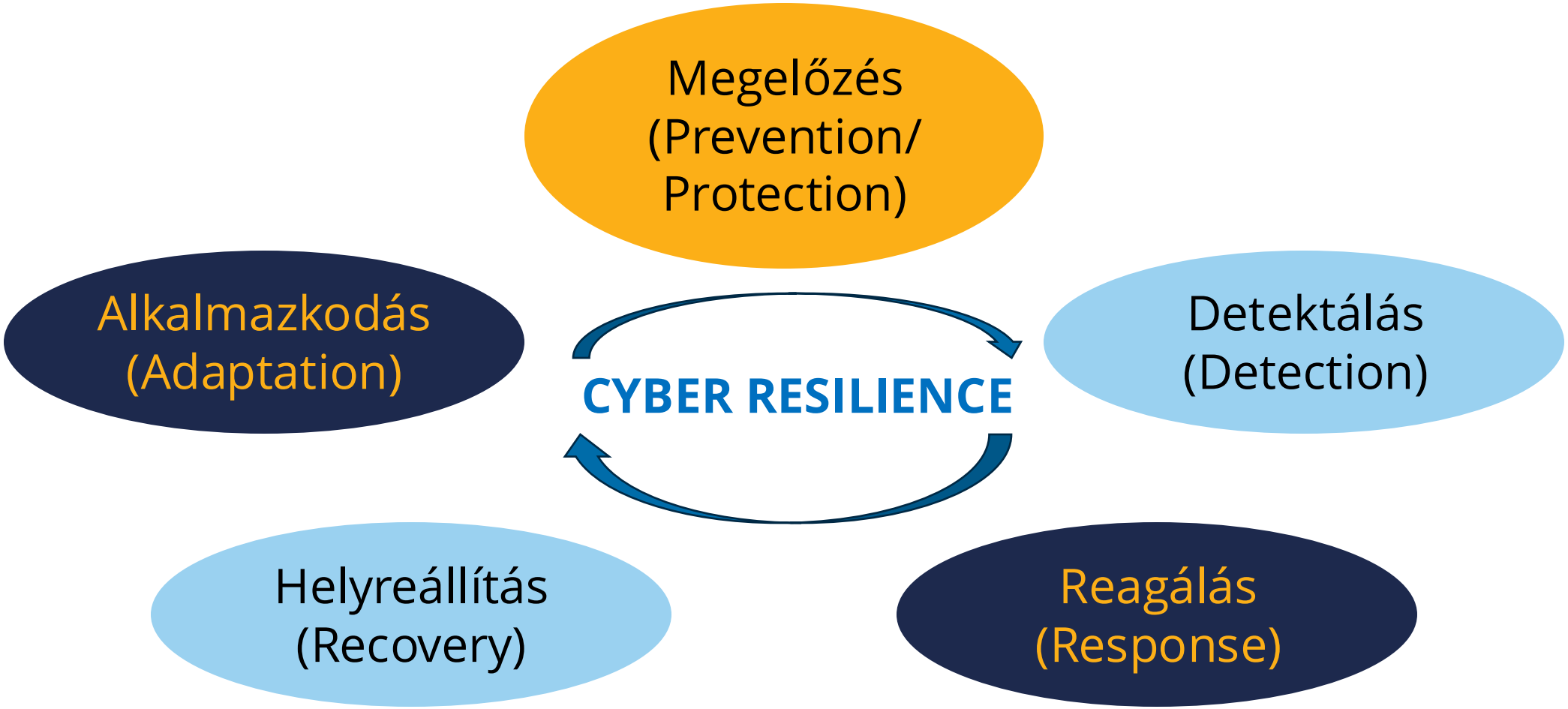
KIBERGYAKORLATOK CÉLKITŰZÉSEI

- **Felkészülés valós kiberfenyegetésekre**
- Valós szcenáriók szimulációja biztonságos környezetben
- Incidenskezelési folyamatok fejlesztése
- Gyakorlati tudás a detektálás és válaszadás területén
- Együttműködés és csapatmunka erősítése
- Tapasztalatgyűjtés kockázat nélkül

CYBER RESILIENCE VS CYBERSECURITY

A kiberreziliencia az a képesség, hogy egy szervezet előre lássa, ellenálljon, alkalmazkodjon és helyreálljon kibertámadásokból és azok hatásaiból, miközben fenntartja az üzleti folytonosságot (ENISA).

Szabályozási szinten meghatározó: 2016-tól (EU, NATO, nemzeti stratégiák), majd **2022-től (NIS2)** kötelező jelleggel.


Megelőzés (Prevention/ Protection)
Detektálás (Detection)
Reagálás (Response)
Helyreállítás (Recovery)
Alkalmazkodás (Adaptation)
CYBER RESILIENCE

NIS2 irányelv és szabályozások

📜 *„Jogszabályi követelmény”*

- Kockázatkezelés
- Incidenskezelés és jelentés
- Üzletmenet-folytonosság
- Ellátási lánc biztonság

Cyber Resilience (reziliencia)

🛡️ *„Ellenállóképesség kiépítése”*

- Protection (védelem)
- Detection (észlelés)
- Response (válaszadás)
- Recovery (helyreállítás)
- Adaptation (alkalmazkodás)

Cyber Exercises

🎯 *„Tesztelés és bizonyítás”*

- Valós szcenáriók kipróbálása
- Gyors reagálás gyakorlása
- Csapatmunka és koordináció
- Hiányosságok feltárása
- Szabályozói megfelelés bizonyítása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

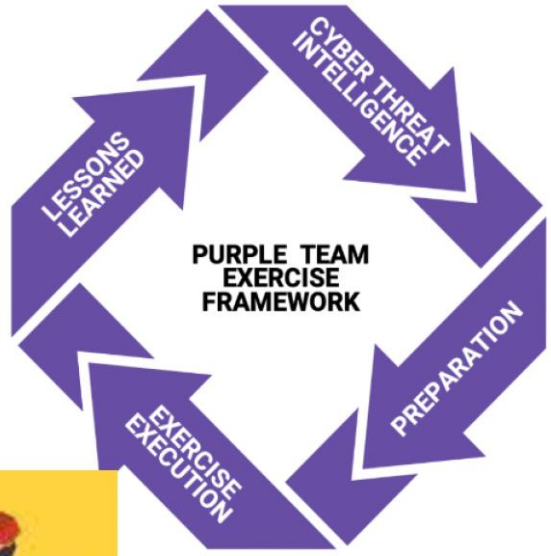
A kibervédelmi gyakorlatok módszerei

Red Team/Blue Team Gyakorlatok

- Red team (támadó csapat)
- Blue Team (Védekező csapat)

Purple Team Gyakorlatok

- Közös munka (Blue & Red team együtt)
- Folyamatok optimalizálása (szervezet gyenge pontjainak meghatározása)



Tabletop Gyakorlatok

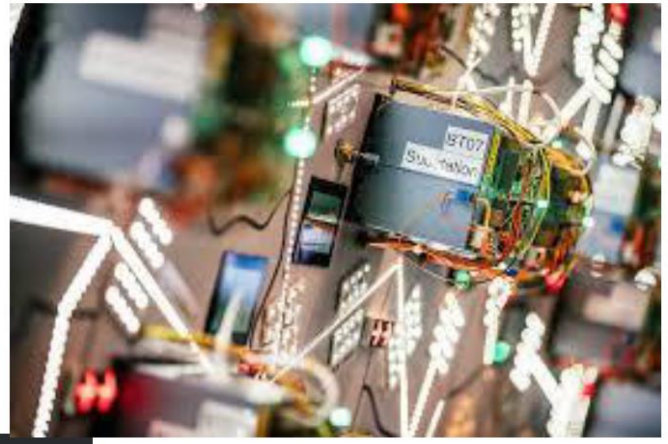
- Forgatókönyv alapú szimuláció
- Interaktív vita

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

A kibervédelmi gyakorlatok módszerei

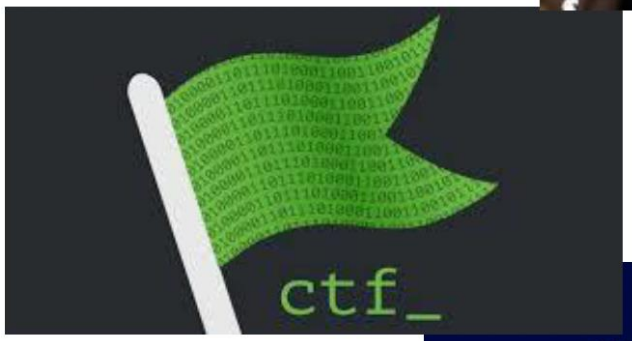
Live Fire Gyakorlatok

- Valós támadások szimulálása
- Kockázatkezelés



Capture the Flag (CTF) Gyakorlatok

- Kihívás-alapú tanulás
- Csapatmunka és verseny



Social Engineering Gyakorlatok

- Phishing szimulációk
- Fizikai biztonsági tesztek

ÓBUDAI EGYETEM JUBILEUMOK ÉVE
ÓE 15 145 630
HAGYOMÁNY ÉS INNOVÁCIÓ

TECHNIKAI KÉSZSÉGEK

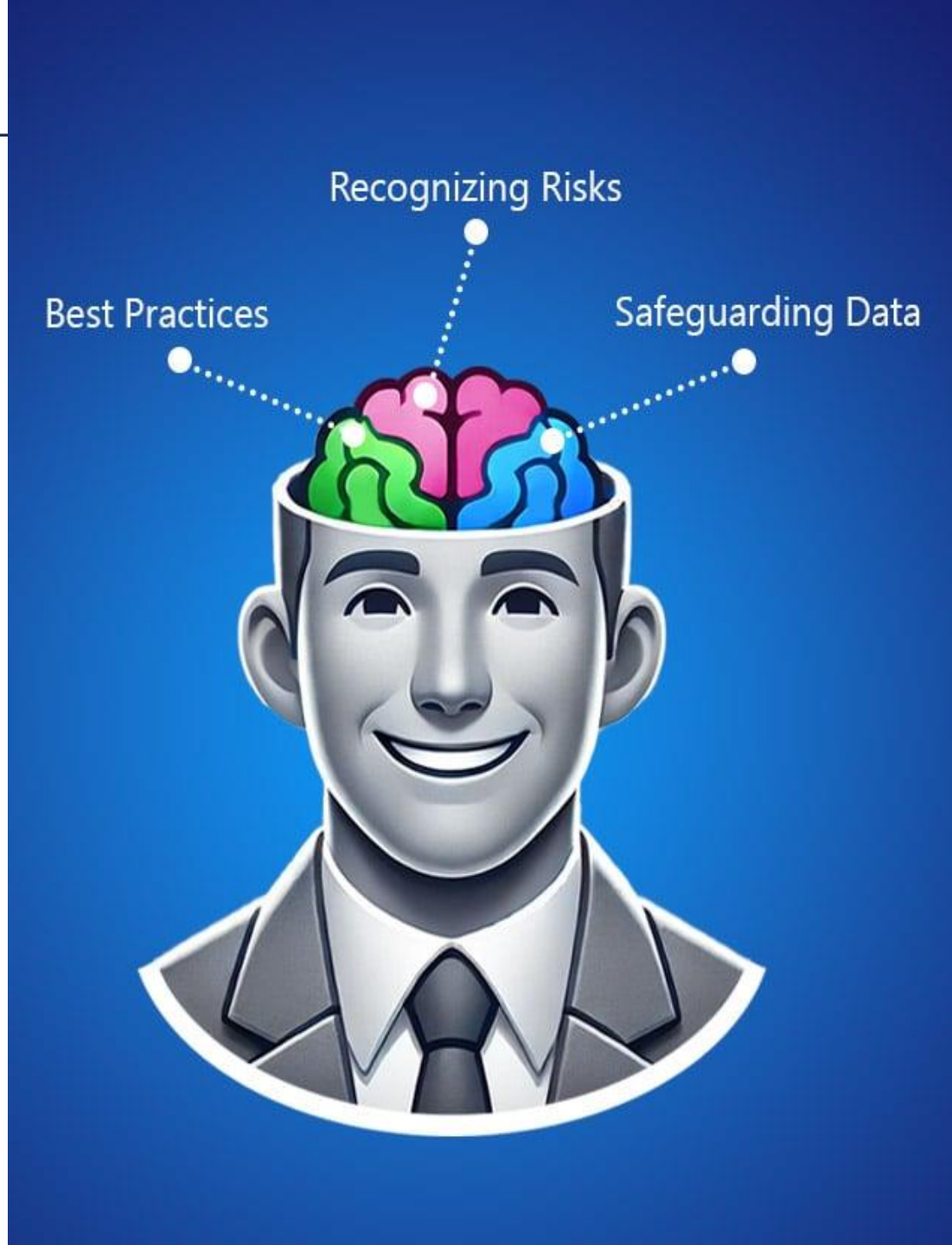
- Hálózati forgalom elemzése
- Sérülékenységvizsgálat
- SIEM rendszerek és naplóelemzés
- Végpontvédelem

STRATÉGIAI DÖNTÉSHOZATAL

- Gyors döntéshozatal stresszhelyzetben
- Önálló hibakeresés és elemzés valós szimulációk során
- Hatékony együttműködés több csapat között

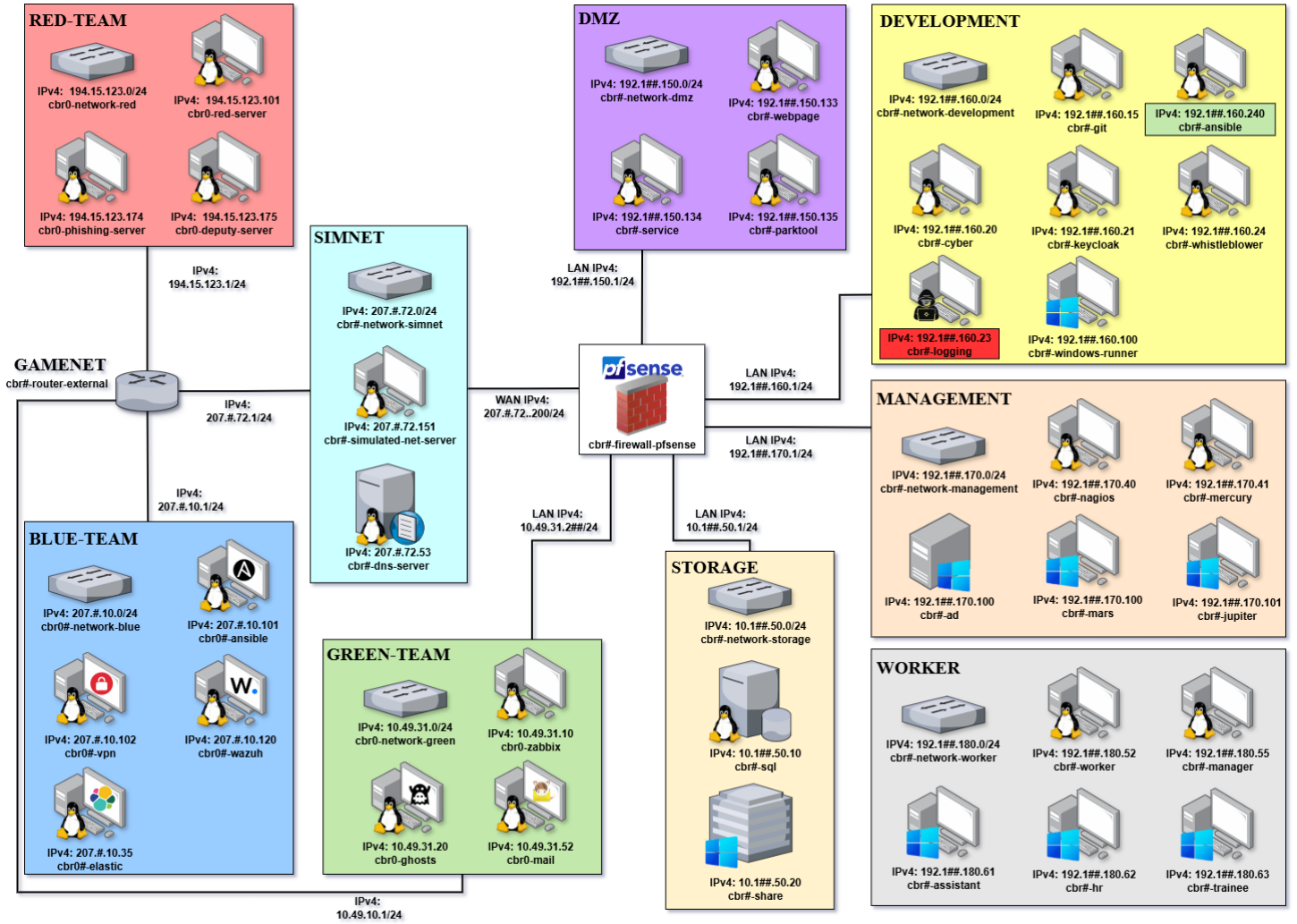
BIZTONSÁGTUDATOSSÁG

- Kibertámadások felismerése
- Azonnali reagálás
- Incidenskezelési folyamatok alkalmazása
- A támadói gondolkodásmód megértése



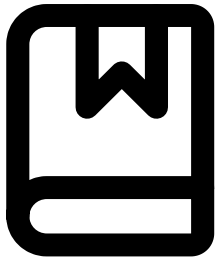
CYBER RANGE

- A környezet egyszerűen példányosítható
- Pontozást és ellenőrzést megvalósító rész (Red team/Organizer hálózata)
- User szimuláció
- Alap támadási forgatókönyvek



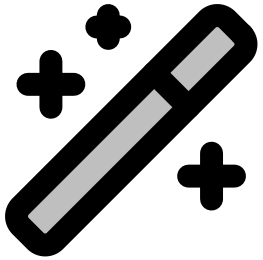
Komplex gyakorlat

- 1/Több napos gyakorlat
- OS-Rendszer független
- SOC szemlélet
- Felkészülési idő
- Élő forgatókönyvek alapján
- User szimuláció
- Távolról végezhető



Vezetett gyakorlat

- Instruktor vagy instruktor nélküli jelenlét
- Támadó vagy védelmi fókusz
- SOC naplóelemzés, felderítés
- „Step-by-step” gyakorlat
- Igény szerinti infrastruktúra
- Személyesen vagy távolról végezhető gyakorlat
- Visszajelzés



Egyedi gyakorlat

- Támadó vagy védelmi fókusz
- Választható:
  - Technológiák
  - Forgatókönyvek
  - Nehézségi szint
- Személyesen vagy távolról végezhető gyakorlat

- Időzített és aktív támadások
- Endpoint védelem, hardening megtervezése és védelem meghatározása, végpontok felderítése
- Levelezési rendszer, a játékosok a ún. blondiekkal kommunikálhatnak vagy akár az elképzelt cégen belüli dolgozókkal.
- SOC – SIEM rendszereken belüli detekciós szabályok éles helyzetben való kialakítása és hibák, sérülékenységek azonnali mitigálása
- Tűzfal szabályok élesítése, szabályozása, felderítése
  – szolgáltatások elérhetősége -
- Felhasználó szimuláció, általános hibák elhárítása, rendelkezésre állás
- Incidens kezelés – report készítés

Control (NIS2)	Check Method	Weight
Privileged accounts	Group analysis	Critical
Password policy	Policy query	High
Logging & retention	Log inspection	High
Patch management	Update review	Critical
Backup & recovery	Backup check	High
Network segmentation	Firewall check	Medium
Audit policy	Audit config	High
Incident reporting	Form submission	Medium
Awareness & training	Quiz score	Medium