A programozott rendszerek kibervédelmének hatékonyságát növelő gyakorlatok tervezéséhez szükséges módszertani útmutató kidolgozása és ehhez kapcsolódó oktatás szervezése

Buttyán Levente

CrySyS Lab, BME

www.crysys.hu

Motivációk

- A kiberbiztonság problémája egyre jelentősebb
  - a különböző kibertámadások száma és kifinomultsága növekszik
  - a célzott támadásokra jellemző a spear phishing és a zero-day sérülékenységek kihasználása
  - a megelőző védelmi megoldások nem nyújtanak 100%-os biztonságot, arra kell felkészülni, hogy mindig lesznek sikeres támadások
- Minden szervezetnek szüksége van használható incidenskezelési képességek kifejlesztésére és folyamatos fenntartására
  - az OAH és az általa felügyelt szervezetek esetében ez különösen fontos
  - a képességeket minden szervezeti szinten érdemes azonosítani, fejleszteni, és mérni
- A felkészülés fontos eszköze a **kiberbiztonsági gyakorlat**

Kiberbiztonsági gyakorlatok

- Valósághű szituációk kezelése szimulált környezetben

- Lehetséges célok:
  - aktuális incidenskezelési képességek felmérése
  - képzési eredmények értékelése
  - aktuális incidenskezlési folyamatok tesztelése
  - új folyamatok validálása
  - rutinszerzés, gyakorlás
  - köztudatformálás

- Releváns képességek skálája:
  - műszaki/technikai képességek
  - stratégiai döntéshozatali képességek
  - együttműködési képességek
  - kommunikációs képességek

A projekt céljai

- Módszertani útmutató kidolgozása kiberbiztonsági gyakorlatok tervezésére és szervezésére
- Rendszeres kiberbiztonsági gyakorlatokat tartalmazó program kidolgozása
- A módszertani útmutató szemléltetése egy több napos tanfolyam keretében

Table top gyakorlatok

- A résztvevők a döntés előkészítés és döntéshozatal folyamatát gyakorolják a moderátor által, jelzésszerűen kialakított történeti háttér és konkrét gyakorlati helyzetek sorában

- A választott megoldások (döntések) indoklásán és hosszabb távú alkalmasságán, valamint a negatív kísérőjelenségek minimalizálásán van a hangsúly

- Nem szükséges a bemutatott megoldást műszaki értelemben tesztelni, nem valós időben zajlik

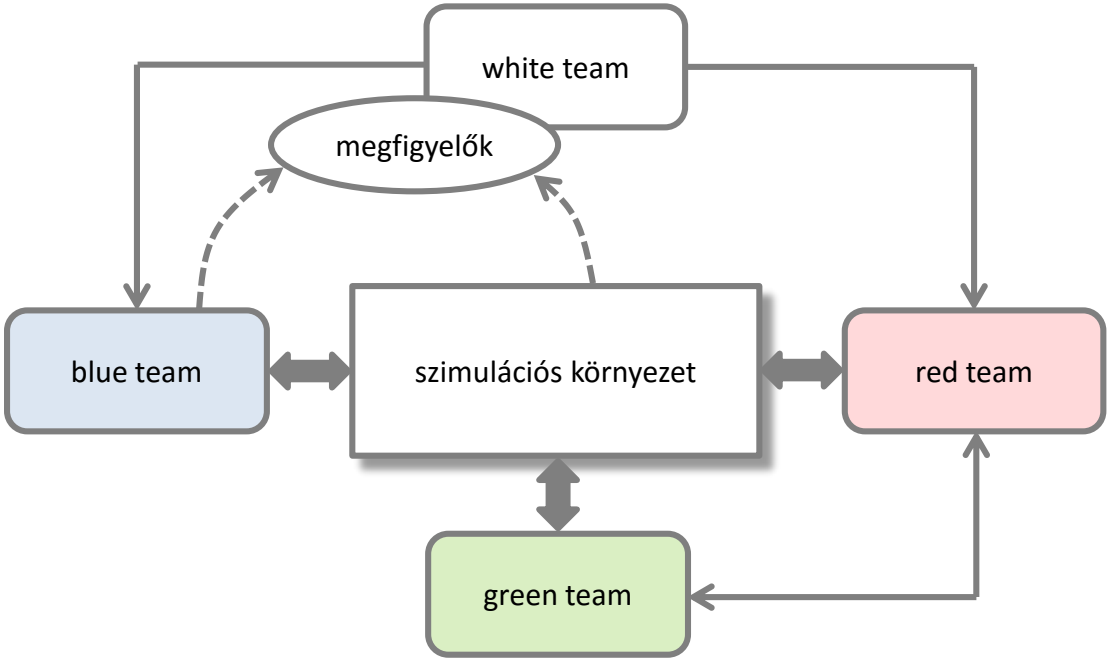
Table top gyakorlatok jellemzői

- Minden szervezeti szinten alkalmazható
- Önmagában általában kevesebb előkészítést és műszaki támogatást igényel, mint a műszaki szimulációt is alkalmazó gyakorlatok
- Alkalmas arra, hogy az információáramlás, döntés-előkészítés és döntéshozatal folyamatait megteremtse, tesztelje, fejlessze
- Tetszőlegesen összetetté tehető különböző, valószerűséget hangsúlyozó eszköz hozzáadásával
- Műszaki eljárások és képességek tesztelésére nem alkalmas, ezért kombinálni szükséges valós vagy szimulált környezetben végzett gyakorlatokkal

Műszaki szimulációs gyakorlatok

- külön erre a célra kialakított, a valóshoz hasonló, ám valójában csak szimulált műszaki gyakorló környezet (cyber range)
  - virtuális számítógépekből álló teljes IT rendszer és azon működő szolgáltatások

- valósághű incidens szenárió, konkrét technikai feladatok
- effektív feladat-megoldás, többnyire valós időben, a gyakorlat virtualizált környezetében



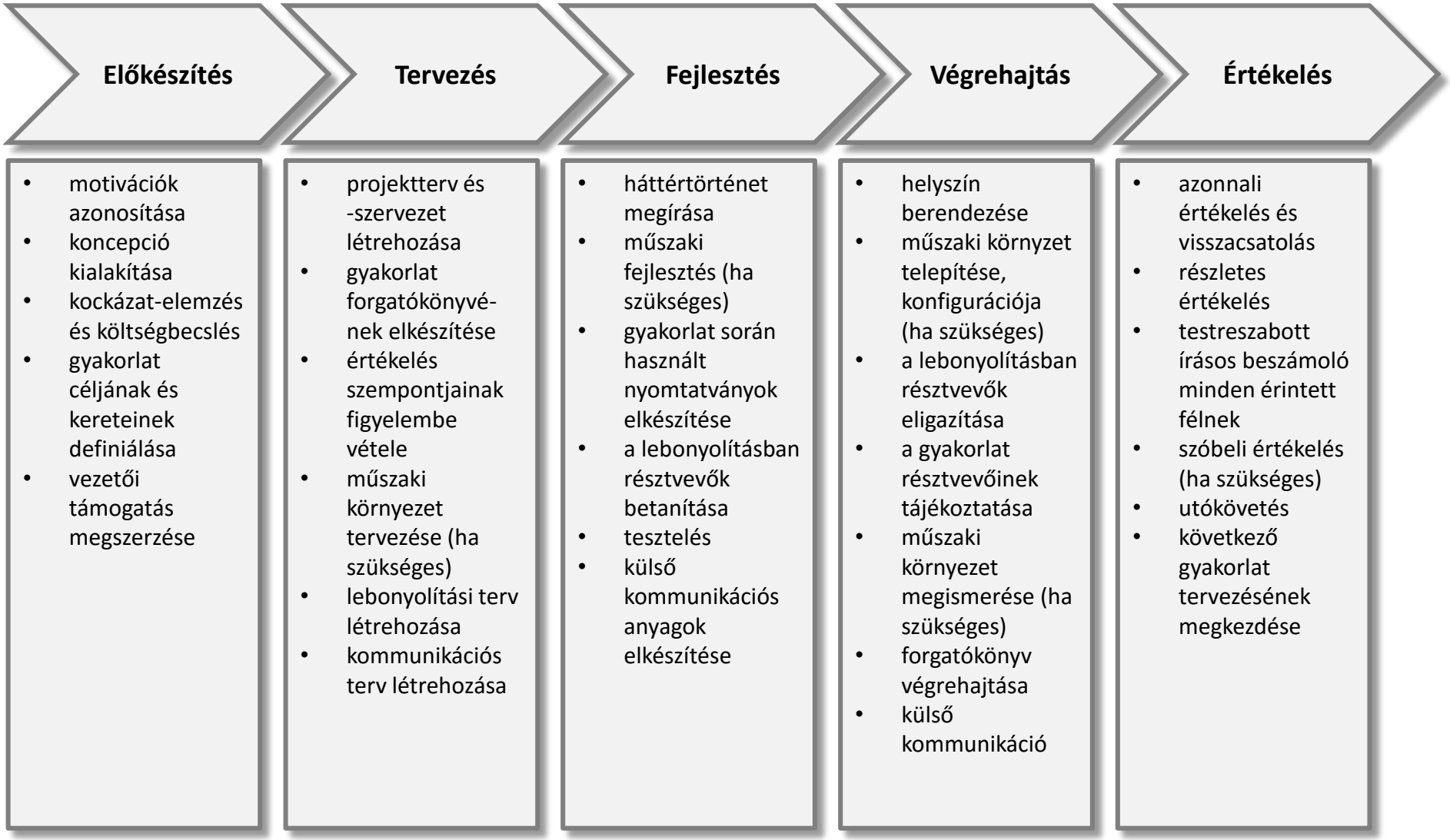
Műszaki szimulációs gyakorlatok előnyei

- Feladatok konkrét elvégzését teszi lehetővé
- Végrehajtási környezet a valóshoz hasonló
- Valós szituációkat jól imitálja
- Műszaki képességek felmérésére, értékelésére, valamint műszaki tevékenységek gyakorlására, rutinszerzésre kiválóan alkalmas
- A virtualizált környezet az igényekhez rugalmasan alakítható, jól skálázható, könnyen visszaállítható egy ismert jó állapotba, könnyen másolható
- A virtualizált környezet a gyakorlat során könnyen menedzselhető
- A virtualizált környezet viszonlyag könnyen szállítható, ami a gyakorlat relokációját teszi lehetővé

Műszaki szimulációs gyakorlatok hátrányai

- Végrehajtási környezet nem egyezik meg teljesen a valós környezettel
- Körültekintő tervezést és jelentős előkészítést igényel (6-12 hónap)
- Potenciálisan nagy szervező csapatot igényel (gyakorlat méretétől függően)
- Jelentős költségei lehetnek
- Ritkábban ismételhető, mint a table-top gyakorlatok
- Elsősorban megfelelő műszaki felkészültséggel rendelkező résztvevők számára hasznos

A gyakorlatok életciklus modellje



3+1 éves program

- Egymásra épülő, fokozatosan emelkedő szakmai szintű gyakorlatok sorozatának létrehozása
- Gyakorlatszervezői know-how megteremtése
- OAH Kiberbiztonsági Tudásközpont kialakítása

1. év

- A gyakorlat stratégiai célrendszere:
  - kiberbiztonsági gyakorlati módszertan megismertetése
  - hazai kapcsolódó szabályzók azonosítása, felmérése, tesztelése
  - nem szabályozott területek azonosítása
  - hazai és nemzetközi információcsere alapfeltételeinek azonosítása, folyamatának tesztelése
  - akcióterv kialakítása a tapasztalt hiányosságok pótlására
- A gyakorlat formája:
  - stratégiai (table top) és vezetett gyakorlati workshop
- Elvárt eredmények:
  - kiberbiztonsági tudatosság emelése
  - információ-megosztás, döntés-előkészítés, döntéshozatal jelentőségének elsajátítása

2. év

- A gyakorlat stratégiai célrendszere:
  - az első év tanulságainak visszacsatornázása
  - eljárások ellenőrzése
  - hazai igényeket lefedő, alapszintű, önálló, incidenskezelési képesség
  - információ-megosztási képesség tesztelése
- Gyakorlat formája:
  - kiberbiztonsági pályarendszeren (cyber range) történő szimulációs gyakorlat
- Elvárt eredmények:
  - érintett szervezetek incidenskezelőinek szervezett, csoportszerű működése
  - szervezeti szintű incidenskezelési képesség felmutatása
  - hazai szervezetek közötti információ-megosztás képességének demonstrálása

3. év

- A gyakorlat stratégiai célrendszere:
  - az előző év tanulságainak visszacsatornázása
  - eljárások ellenőrzése
  - regionális szintű, önálló, incidenskezelési képesség
  - nemzetközi szintű információ-megosztási (IER) eljárás validálása
- Gyakorlat formája:
  - kiberbiztonsági pályarendszeren (cyber range) történő szimulációs gyakorlat
- Elvárt eredmények:
  - érintett szervezetek incidenskezelő csoportjainak országos szintű koordinációja
  - országos szintű, szervezeteken átnyúló incidensek kezelése képességének bemutatása
  - regionális szervezetek közötti együttműködés és információ-megosztás képességének demonstrálása

4. év

- A gyakorlat stratégiai célrendszere:
  - az előző év tanulságainak visszacsatornázása
  - eljárások ellenőrzése
  - OAH Kiberbiztonsági Tudásközpont megalakítása és a szervezeti szintű részfeladatok előkészítése
  - globális szintű, önálló, incidenskezelési és információ-megosztási képesség elérése
- Gyakorlat formája:
  - kiberbiztonsági pályarendszeren (cyber range) történő szimulációs gyakorlat
- Elvárt eredmények:
  - gyakorlattervezési, előkészítési, levezetési és kiértékelési részfeladatok OAH Tudásközpont által történő végrehajtása
  - érintett szervezetek incidenskezelő csoportjainak regionális szintű koordinálása
  - országos vagy regionális szintű, szervezeteken átnyúló incidensek professzionális kezelése
  - globális és regionális szervezetek közötti együttműködés és információ-megosztás képességének demonstrálása

A módszertan szemléltetése

- 2,5 napos workshop az OAH által felügyelt szervezetek képviselőinek (2017. április 19-21.)
  - előadások
  - table top gyakorlat
  - műszaki feladatokat tartalmazó technikai gyakorlat
  - egységes story line:

> Önök egy képzeletbeli nukleáris technológiai vállalat informatikai osztályának incidens kezelő csoportját (CERT) alkotják. A vállalat az OAH felügyelete alá tartozik, mivel mind a kutatás-fejlesztés, mind pedig a gyártási folyamatok hasadó anyagok felhasználásával történnek.
>
> ...
>
> Az informatikai osztály incidens kezelő csoportja (CERT) bejelentést kapott, hogy több részlegben is elérhetetlenné váltak a felhasználói dokumentumok. Az ismert ikonok megváltoztak, a dokumentumok és táblázatok nem nyithatóak meg, elérhetetlenné váltak a pénzügyi, marketing osztályokon és a vezérigazgatói titkárságon.

1. nap

Döntéshozók számára tartott általános összefoglaló és table top stratégiai gyakorlat

- Globális kiberbiztonsági helyzet áttekintése
- Kiberbiztonsági gyakorlatok szerepe az integrációs szervezetekben (EU, NATO)
- Table top és műszaki szimulációs gyakorlatok módszertana
- 3+1 éves program bemutatása
- Vezetői szintű, stratégiai kiberbiztonsági döntéshozatali gyakorlat

2-3. nap

Technikai emberek számára tartott műszaki gyakorlat előkészített műszaki feladatokkal, de nem teljes gyakorlópálya rendszeren és nem teljesen valós időben

- Áttekintés és összefoglalók
- Technikai gyakorlat: 4 szakasz, egységes story-line
  - 1. szakasz: ransomware támadás érzékelése, kezelése
  - 2. szakasz: kompromittált Linux szerver forensic elemzése
  - 3. szakasz: hálózati logok elemzése
  - 4. szakasz: malware bináris visszafejtés és elemzés

Köszönetnyilvánítás