ANDREWS IT ENGINEERING

Szolgáltatások Technológiák Ügyfél sztori Cégről Kapcsolat HU Beszélgessünk

Cyber-range alapú gyakorlatok támogatásának kérdései és lehetséges megoldásai SOC-ok szempontjából

ELTE

Kiber gyakorlatok komplexitás szerint

Kiber gyakorlatok komplexitás szerint

SERMINAR

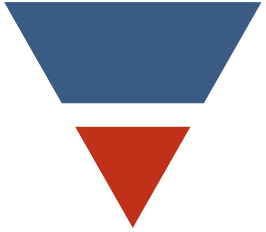
ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

Kiber gyakorlatok komplexitás szerint

WORKSHOP

SERMINAR



ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

Kiber gyakorlatok komplexitás szerint

TABLETOP

WORKSHOP

SERMINAR

ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

Kiber gyakorlatok komplexitás szerint

GAMES

TABLETOP

WORKSHOP

SERMINAR

ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

Kiber gyakorlatok komplexitás szerint

DRILLS

GAMES

TABLETOP

WORKSHOP

SERMINAR

ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

Kiber gyakorlatok komplexitás szerint

FUNCTIONAL

DRILLS

GAMES

TABLETOP

WORKSHOP

SERMINAR

ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

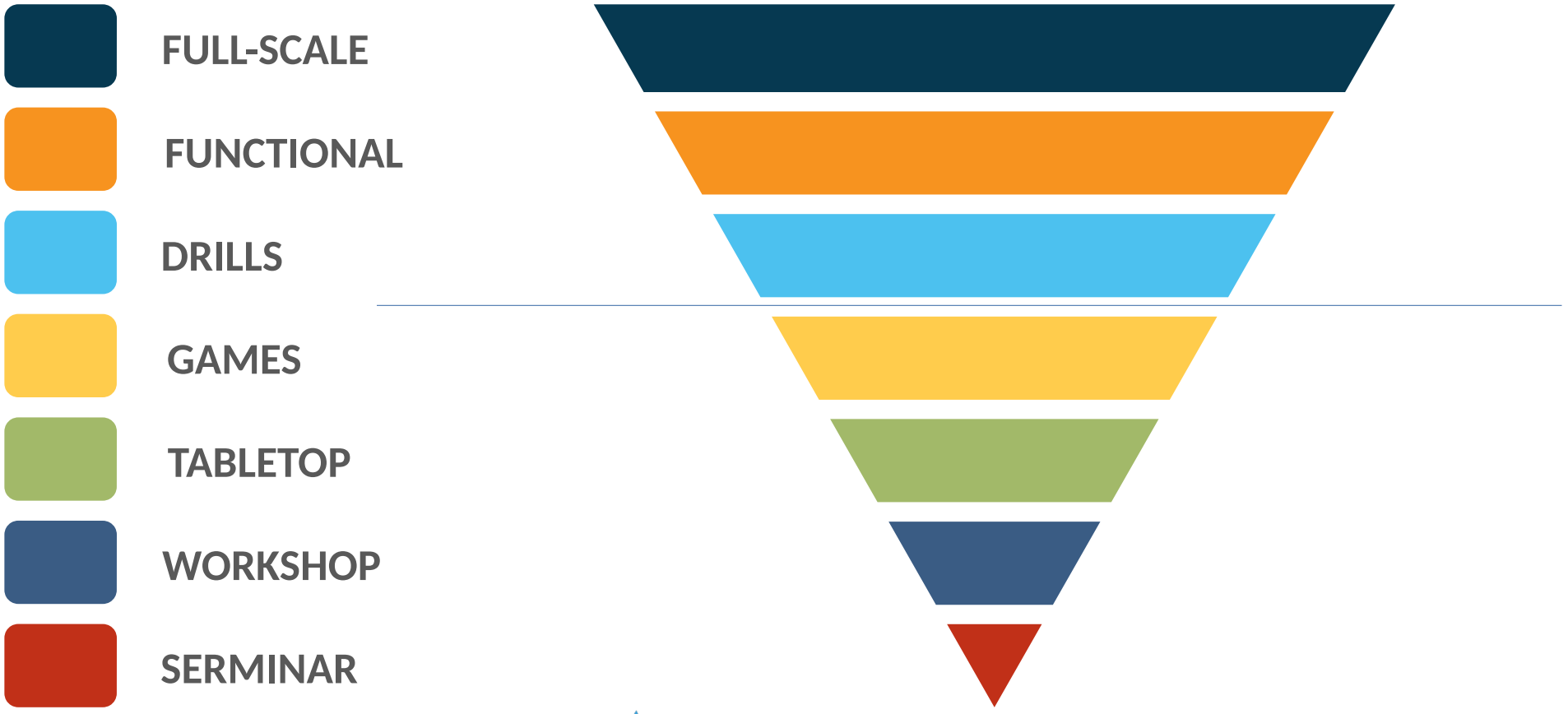
Kiber gyakorlatok komplexitás szerint

- FULL-SCALE
- FUNCTIONAL
- DRILLS
- GAMES
- TABLETOP
- WORKSHOP
- SERMINAR

ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

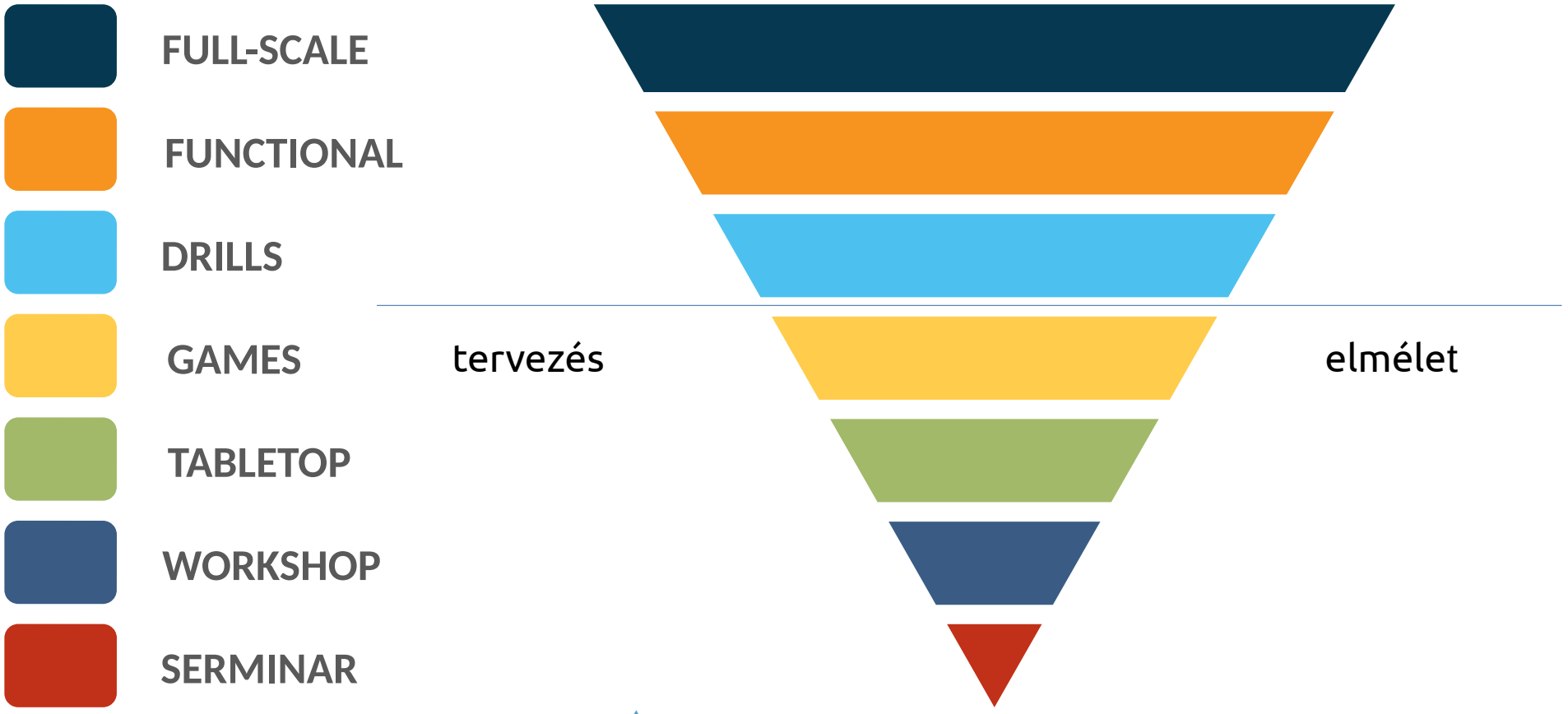
Kiber gyakorlatok komplexitás szerint



ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

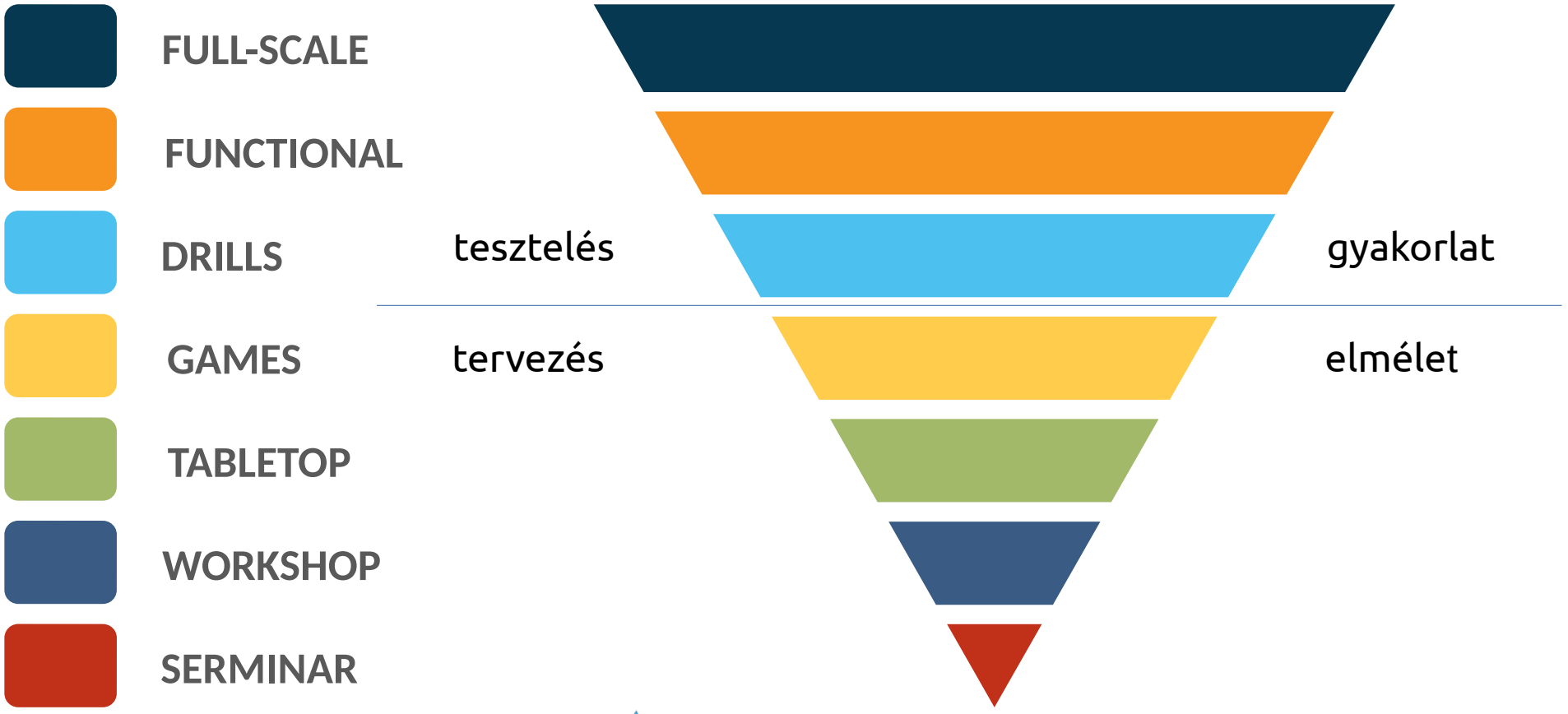
Kiber gyakorlatok komplexitás szerint



ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

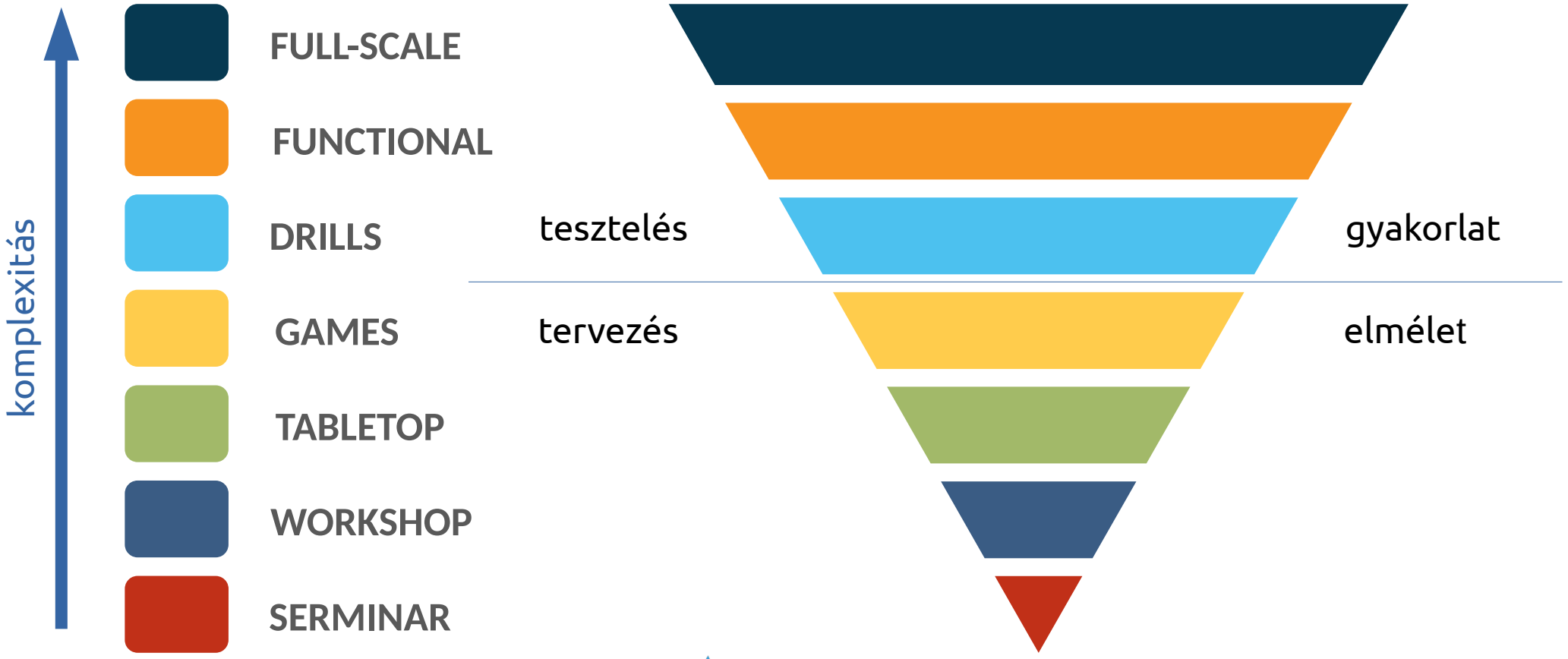
Kiber gyakorlatok komplexitás szerint



ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

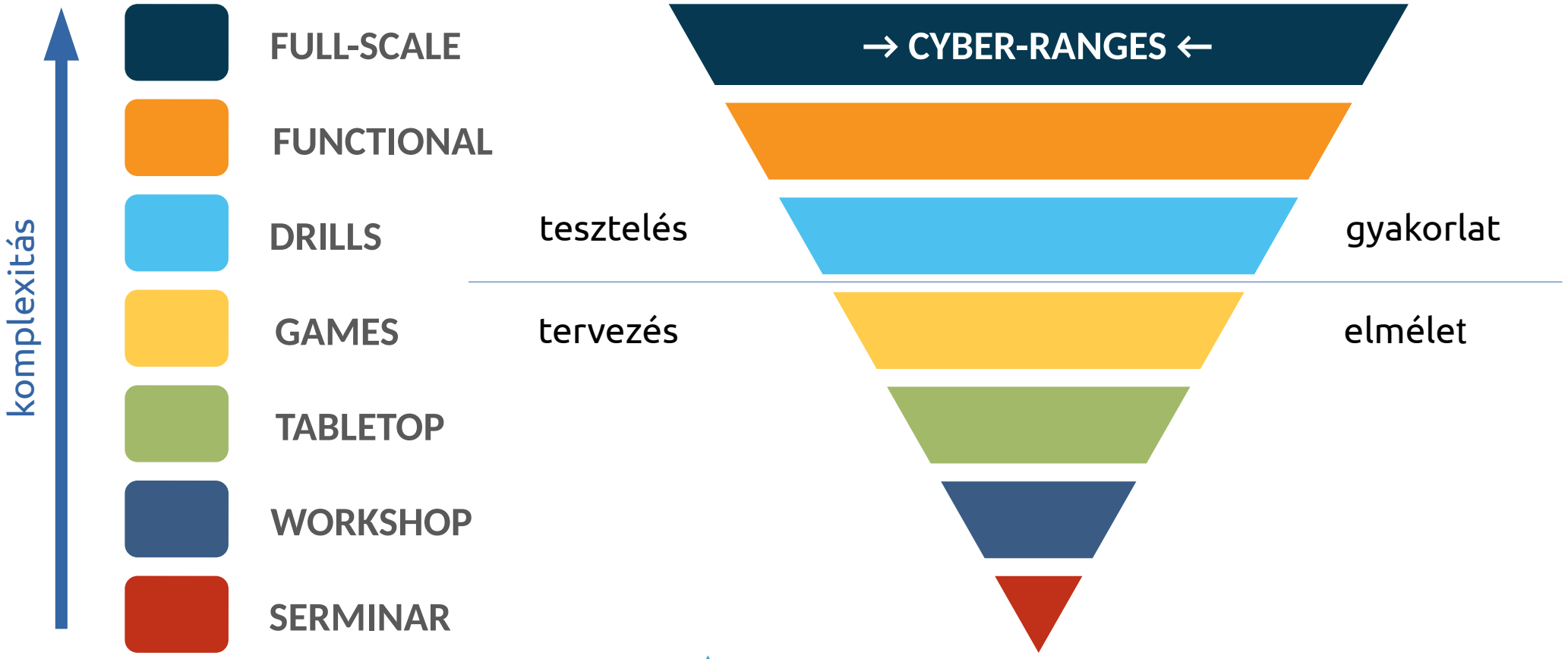
Kiber gyakorlatok komplexitás szerint



ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

Kiber gyakorlatok komplexitás szerint



ANDREWS IT ENGINEERING

Homeland Security Exercise Evaluation Program (HSEEP)

- **Elméleti/Beszélgetős** gyakorlatok:

  A résztvevőket megismerik a jelenlegi tervekkel, szabályzatokkal, megállapodásokkal és eljárásokkal, vagy új terveket, szabályzatokat, megállapodásokat és eljárásokat fejlesztenek. A beszélgetés alapú gyakorlatok típusai:

  - **Seminar**: Egy informális beszélgetés, amelynek célja az új vagy frissített tervekkel, szabályzatokkal vagy eljárásokkal való megismerkedés
  - **Workshop**: A műhelymunka hasonlít a szemináriumhoz, de konkrét termékek létrehozására szolgál, például vázlatos terv vagy szabályzat készítésére.
  - **Tabletop:** A táblagyakorlat során a kulcsfontosságú személyzet informális környezetben tárgyal szimulált forgatókönyvekről. A táblagyakorlatok használhatók tervek, szabályzatok és eljárások értékelésére.
  - **Game:** Egy műveletet szimuláló játék, amelyben általában két vagy több csapat vesz részt versenyszerű környezetben. A játék során szabályokat, adatokat és eljárásokat alkalmaznak, hogy egy valós vagy feltételezett valós helyzetet ábrázoljanak.

- **Elméleti/Beszélgetős** gyakorlatok:

  A résztvevőket megismerik a jelenlegi tervekkel, szabályzatokkal, megállapodásokkal és eljárásokkal, vagy új terveket, szabályzatokat, megállapodásokat és eljárásokat fejlesztenek. A beszélgetés alapú gyakorlatok típusai:

  - **Seminar**: Egy informális beszélgetés, amelynek célja az új vagy frissített tervekkel, szabályzatokkal vagy eljárásokkal való megismerkedés
  - **Workshop**: A műhelymunka hasonlít a szemináriumhoz, de konkrét termékek létrehozására szolgál, például vázlatos terv vagy szabályzat készítésére.
  - **Tabletop:** A táblagyakorlat során a kulcsfontosságú személyzet informális környezetben tárgyal szimulált forgatókönyvekről. A táblagyakorlatok használhatók tervek, szabályzatok és eljárások értékelésére.
  - **Game:** Egy műveletet szimuláló játék, amelyben általában két vagy több csapat vesz részt versenyszerű környezetben. A játék során szabályokat, adatokat és eljárásokat alkalmaznak, hogy egy valós vagy feltételezett valós helyzetet ábrázoljanak.

- **Műveleti/gyakorlati** gyakorlatok:

  Ezek a gyakorlatok validálják a terveket, szabályzatokat, megállapodásokat és eljárásokat, tisztázzák a szerepeket és felelősségeket, valamint az erőforrás-hiányokat az operatív környezetben. A műveleti gyakorlatok típusai:

  - **Drill**: A gyakorlat egy koordinált, felügyelt tevékenység, amelyet általában egyetlen, konkrét művelet vagy funkció tesztelésére használnak egyetlen entitáson belül (például tömeges jelszócsere kompromittált környezetben).
  - **Functional**: A funkcionális gyakorlat az együttműködés, irányítás és irányítás vizsgálatát és/vagy érvényesítését célozza különböző többszereplős koordinációs központok között. A funkcionális gyakorlat nem magában foglalja a "téren lévő" szereplőket (azaz a első válaszadókat vagy vészhelyzeti tisztviselőket, akik valós időben reagálnak egy eseményre).
  - **Full-scale**: A teljes körű gyakorlat melyben valamennyi érintett részt vesz, valamennyi fontosabb elem szimulációra kerül és gyakorlat során minden releváns elem kipróbálásra és kiértékelésre kerül.

Mi az a cyber-range?

Ez egy olyan full-scale kiber/cyber gyakorlati forma illetve speciális környezet vagy platform, amelyet a kiberbiztonsági képzések és gyakorlatok számára hoznak létre. A cyber-range lehetőséget nyújt a résztvevőknek, hogy valós időben és ellenőrzött környezetben gyakorolják és teszteljék a kiberbiztonsági képességeiket, válaszreakcióikat és eszközeiket.


ANDREWS
IT ENGINEERING

Cyber-range != Tesztrendszer

Cyber-range != Tesztrendszer
Cyber-range != Digital Twins

Cyber-range != Tesztrendszer
Cyber-range != Digital Twins
Cyber-range != Éles környezet

Mi a SOC? B.Zs©

ANDREWS
IT ENGINEERING

Mi a SOC? B.Zs©

Mi a SOC? B.Zs©

Napló gyűjtés

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

- Kockázatok feltárásához szükséges (statikus vagy ML alapú) logikai szabályok, melyek a naplókban felfedezhető logikai együttállásokat képeseket feltárni

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

- Kockázatok feltárásához szükséges (statikus vagy ML alapú) logikai szabályok, melyek a naplókban felfedezhető logikai együttállásokat képeseket feltárni

Triage

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

- Kockázatok feltárásához szükséges (statikus vagy ML alapú) logikai szabályok, melyek a naplókban felfedezhető logikai együttállásokat képeseket feltárni

Triage

- Validáció
  - T+ v F+?
- Priorizálás
  - Fontos v sürgős
- Szükséges ”gyógykezelés” meghatározása

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

- Kockázatok feltárásához szükséges (statikus vagy ML alapú) logikai szabályok, melyek a naplókban felfedezhető logikai együttállásokat képeseket feltárni

Triage

- Validáció
  - T+ v F+?
- Priorizálás
  - Fontos v sürgős
- Szükséges ”gyógykezelés” meghatározása

DFIR

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

- Kockázatok feltárásához szükséges (statikus vagy ML alapú) logikai szabályok, melyek a naplókban felfedezhető logikai együttállásokat képeseket feltárni

Triage

- Validáció
  - T+ v F+?
- Priorizálás
  - Fontos v sürgős
- Szükséges ”gyógykezelés” meghatározása

DFIR

- T+ esetén az incidens nyomainak biztosítása
- Hatások mérséklése, visszaállítás támogatása
- **Tafe**

ANDREWS IT ENGINEERING

Mi a SOC? B.Zs©

Napló gyűjtés

- Naplóforrások feltárása
- Naplóforrások integrációja a naplógyűjtő rendszerbe

Feldolgozás

- Gyűjtött naplók egységes elemezésének biztosítása
- Naplók gazdagítása
- Korrelációs képesség biztosítása

Elemzés

- Kockázatok feltárásához szükséges (statikus vagy ML alapú) logikai szabályok, melyek a naplókban felfedezhető logikai együttállásokat képeseket feltárni

Triage

- Validáció
  - T+ v F+?
- Priorizálás
  - Fontos v sürgős
- Szükséges ”gyógykezelés” meghatározása

DFIR

- T+ esetén az incidens nyomainak biztosítása
- Hatások mérséklése, visszaállítás támogatása
- **Tafe**

ANDREWS IT ENGINEERING

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Milyen kihívásokat jelent a gyakorlat a SOC számára?

- Azonos technológiát tudunk használni a gyakorlaton és az éles környezetben?
  - SOC platform licenc kérdései
  - Elkülönítés: Tenant, új példány, cloud/virtuális megoldás?
  - Milyen eltérések származnak a range sajátosságaiból? (A rendszereken megjelenik alkalmazás szinten a pontozási alrendszer?)

Milyen kihívásokat jelent a gyakorlat a SOC számára?

- Azonos technológiát tudunk használni a gyakorlaton és az éles környezetben?
  - SOC platform licenc kérdései
  - Elkülönítés: Tenant, új példány, cloud/virtuális megoldás?
  - Milyen eltérések származnak a range sajátosságaiból? (A rendszereken megjelenik alkalmazás szinten a pontozási alrendszer?)
- Rendszerkapacitás
  - Elérhető infrastruktúra és erőforrások
  - Skálázhatóság és rugalmasság kérdései

Milyen kihívásokat jelent a gyakorlat a SOC számára?

- Azonos technológiát tudunk használni a gyakorlaton és az éles környezetben?
  - SOC platform licenc kérdései
  - Elkülönítés: Tenant, új példány, cloud/virtuális megoldás?
  - Milyen eltérések származnak a range sajátosságaiból? (A rendszereken megjelenik alkalmazás szinten a pontozási alrendszer?)
- Rendszerkapacitás
  - Elérhető infrastruktúra és erőforrások
  - Skálázhatóság és rugalmasság kérdései
- Szimulációs környezetek
  - Valósághűség és komplexitás
  - Támadói technikák és eszközök reprodukálása

ANDREWS IT ENGINEERING

Milyen kihívásokat jelent a gyakorlat a SOC számára?

- Azonos technológiát tudunk használni a gyakorlaton és az éles környezetben?
  - SOC platform licenc kérdései
  - Elkülönítés: Tenant, új példány, cloud/virtuális megoldás?
  - Milyen eltérések származnak a range sajátosságaiból? (A rendszereken megjelenik alkalmazás szinten a pontozási alrendszer?)
- Rendszerkapacitás
  - Elérhető infrastruktúra és erőforrások
  - Skálázhatóság és rugalmasság kérdései
- Szimulációs környezetek
  - Valósághűség és komplexitás
  - Támadói technikák és eszközök reprodukálása
- Adatgyűjtés és elemzés
  - Események és naplóbejegyzések monitorozása
  - Biztonsági információk gyűjtése és kiértékelése

Milyen kihívásokat jelent a gyakorlat a SOC számára?

- Azonos technológiát tudunk használni a gyakorlaton és az éles környezetben?
  - SOC platform licenc kérdései
  - Elkülönítés: Tenant, új példány, cloud/virtuális megoldás?
  - Milyen eltérések származnak a range sajátosságaiból? (A rendszereken megjelenik alkalmazás szinten a pontozási alrendszer?)
- Rendszerkapacitás
  - Elérhető infrastruktúra és erőforrások
  - Skálázhatóság és rugalmasság kérdései
- Szimulációs környezetek
  - Valósághűség és komplexitás
  - Támadói technikák és eszközök reprodukálása
- Adatgyűjtés és elemzés
  - Események és naplóbejegyzések monitorozása
  - Biztonsági információk gyűjtése és kiértékelése
- Gyakorlatok tervezése és végrehajtása
  - Célok és forgatókönyvek kidolgozása
  - Csapatok és szerepek meghatározása
  - Visszajelzések és utólagos értékelés

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Napló gyűjtés

- Hogyan hozzuk el a logot? (agent vs agentless)
- Titkosított / titkosítatlan?
- Milyen logot hozunk el? (OS, appl, infra?)

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Napló gyűjtés

- Hogyan hozzuk el a logot? (agent vs agentless)
- Titkosított / titkosítatlan?
- Milyen logot hozunk el? (OS, appl, infra?)

Feldolgozás

- Standard, struktúrált logok lesznek kizárólag?
- Egyedi alkalmazások/eltérő verziók lesznek?
- Milyen egyedi korrelációs igények merülnek fel?

ANDREWS IT ENGINEERING

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Napló gyűjtés

- Hogyan hozzuk el a logot? (agent vs agentless)
- Titkosított / titkosítatlan?
- Milyen logot hozunk el? (OS, appl, infra?)

Feldolgozás

- Standard, struktúrált logok lesznek kizárólag?
- Egyedi alkalmazások/eltérő verziók lesznek?
- Milyen egyedi korrelációs igények merülnek fel?

Elemzés

- Milyen sajátosságai vannak a környezetnek?
- Kellenek kivételek, új szabályok?
- Mi a gyakorlat célja SOC szempontjából?

ANDREWS IT ENGINEERING

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Napló gyűjtés

- Hogyan hozzuk el a logot? (agent vs agentless)
- Titkosított / titkosítatlan?
- Milyen logot hozunk el? (OS, appl, infra?)

Feldolgozás

- Standard, struktúrált logok lesznek kizárólag?
- Egyedi alkalmazások/eltérő verziók lesznek?
- Milyen egyedi korrelációs igények merülnek fel?

Elemzés

- Milyen sajátosságai vannak a környezetnek?
- Kellenek kivételek, új szabályok?
- Mi a gyakorlat célja SOC szempontjából?

Triage

- Meglevő eljárásrend elégséges?
- Vannak speciális szempontok melyeket figyelembe kell venni a gyakorlag jellege miatt?

ANDREWS IT ENGINEERING

Milyen kihívásokat jelent a gyakorlat a SOC számára?

Napló gyűjtés

- Hogyan hozzuk el a logot? (agent vs agentless)
- Titkosított / titkosítatlan?
- Milyen logot hozunk el? (OS, appl, infra?)

Feldolgozás

- Standard, struktúrált logok lesznek kizárólag?
- Egyedi alkalmazások/eltérő verziók lesznek?
- Milyen egyedi korrelációs igények merülnek fel?

Elemzés

- Milyen sajátosságai vannak a környezetnek?
- Kellenek kivételek, új szabályok?
- Mi a gyakorlat célja SOC szempontjából?

Triage

- Meglevő eljárásrend elégséges?
- Vannak speciális szempontok melyeket figyelembe kell venni a gyakorlag jellege miatt?

DFIR

- Része egyáltalán a gyakorlatnak?
- Mely csapat végzi? (Blue/Purple)
- Jelentések készítése feladat?

ANDREWS IT ENGINEERING

Lehetséges megoldások a cyber-range alapú gyakorlatok támogatására

ANDREWS
IT ENGINEERING

Lehetséges megoldások a cyber-range alapú gyakorlatok támogatására

- Infrastrukturális fejlesztések
  - Kiterjesztett kapacitás és erőforrások biztosítása
  - Felhőalapú megoldások alkalmazása

Lehetséges megoldások a cyber-range alapú gyakorlatok támogatására

- Infrastrukturális fejlesztések
  - Kiterjesztett kapacitás és erőforrások biztosítása
  - Felhőalapú megoldások alkalmazása
- Szimulációs eszközök és technológiák
  - Komplex támadói eszközök és technikák integrálása
  - Hálózati és rendszereszközök szimulációja

ANDREWS IT ENGINEERING

Lehetséges megoldások a cyber-range alapú gyakorlatok támogatására

- Infrastrukturális fejlesztések
  - Kiterjesztett kapacitás és erőforrások biztosítása
  - Felhőalapú megoldások alkalmazása
- Szimulációs eszközök és technológiák
  - Komplex támadói eszközök és technikák integrálása
  - Hálózati és rendszereszközök szimulációja
- Adatgyűjtés és elemzés automatizálása
  - Események és naplóbejegyzések automatikus monitorozása
  - Intelligens elemzőrendszer alkalmazása

ANDREWS IT ENGINEERING

Lehetséges megoldások a cyber-range alapú gyakorlatok támogatására

- Infrastrukturális fejlesztések
  - Kiterjesztett kapacitás és erőforrások biztosítása
  - Felhőalapú megoldások alkalmazása
- Szimulációs eszközök és technológiák
  - Komplex támadói eszközök és technikák integrálása
  - Hálózati és rendszereszközök szimulációja
- Adatgyűjtés és elemzés automatizálása
  - Események és naplóbejegyzések automatikus monitorozása
  - Intelligens elemzőrendszer alkalmazása
- Gyakorlatok tervezésének és végrehajtásának támogatása
  - Forgatókönyv- és célgenerátorok alkalmazása
  - Csapatmenedzsment és együttműködési eszközök használata

ANDREWS IT ENGINEERING

Összegzés - Trendek

Összegzés - Trendek

Összefoglalás és következtetés

- A cyber-range alapú gyakorlatok jelentősége a SOC számára
- Lehetséges megoldások a gyakorlatok támogatás
- Kihívások és továbbfejlesztési lehetőségek
  - Komplexebb és realisztikusabb támadói szcenáriók kidolgozása
  - Intelligens elemzési és válaszadási mechanizmusok fejlesztése

Összegzés - Trendek

Összefoglalás és következtetés

- A cyber-range alapú gyakorlatok jelentősége a SOC számára
- Lehetséges megoldások a gyakorlatok támogatás
- Kihívások és továbbfejlesztési lehetőségek
  - Komplexebb és realisztikusabb támadói szcenáriók kidolgozása
  - Intelligens elemzési és válaszadási mechanizmusok fejlesztése

Jövőbeli trendek és fejlesztési irányok

- Mesterséges intelligencia és gépi tanulás alkalmazása a cyber-range gyakorlatokban
- Threat intelligence, CTI reporting integrációja a gyakorlatokba
- Automatizált sebezhetőségértékelés és sebezhetőségkezelés támogatása