

ISACA KONFERENCIA 2022

Oroszi Eszter Diána

Időutazás a Social Engineering auditok korában,
avagy mi változott az elmúlt 10 év alatt?

2022.06.16.

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

Bemutakozás

Oroszi Eszter Diána, CISA, CISM, CRISC, ISO 27001 LA

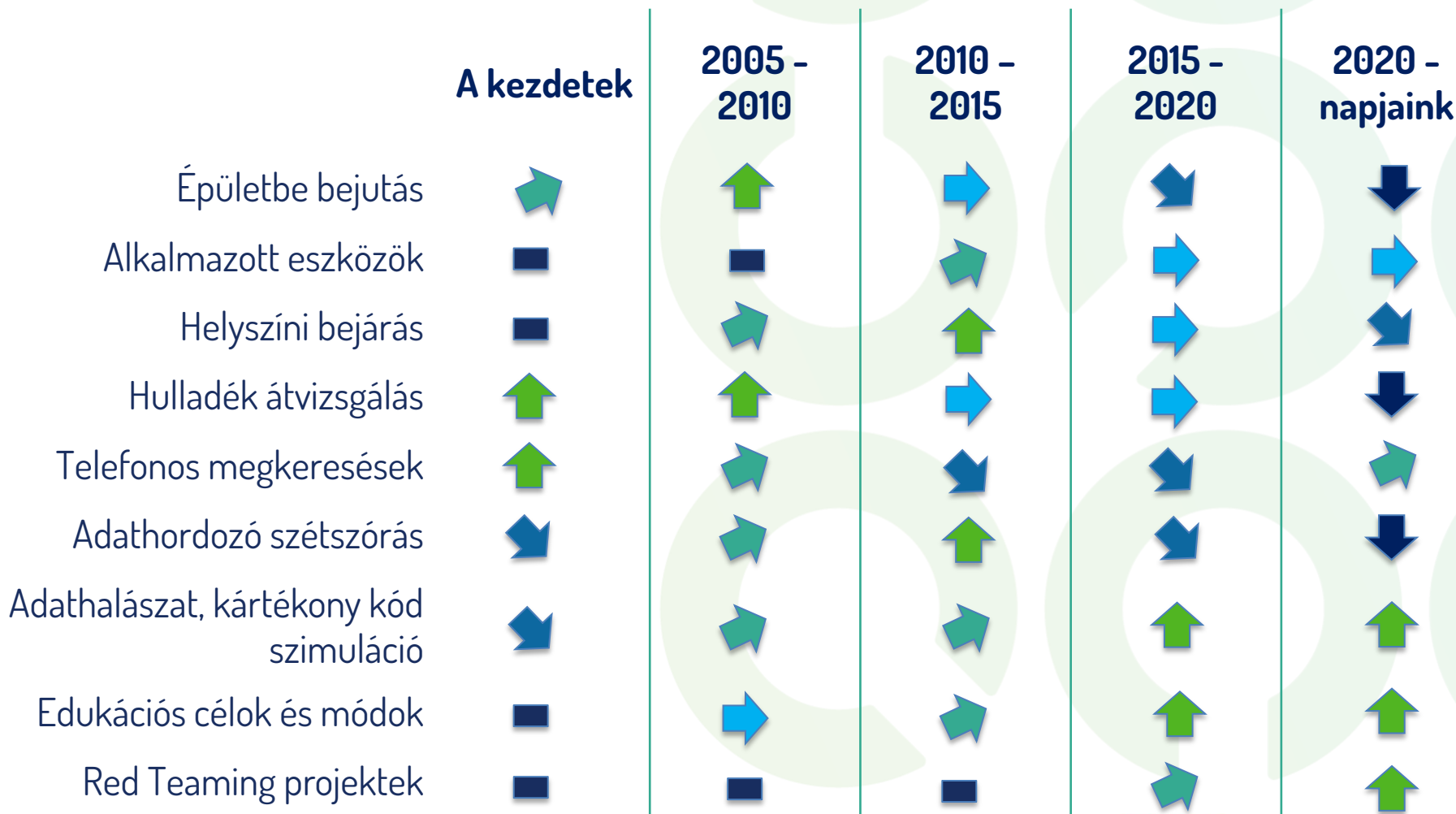
- 12 év szakmai tapasztalat – tanácsadói és ügyfél oldalon egyaránt
- Silent Signal Kft., információbiztonsági tanácsadás üzletágvezető
- Nemzeti Közsolgálati Egyetem, PhD hallgató
- Kutatási terület: Social Engineering, biztonság tudatosság mérése és fejlesztése, gamifikációs lehetőségek
- Biztonságtudatossági szabadulószo
- Biztonságtudatossági társasjáték fejlesztés



FELKÉSZÜLTÜNK AZ IDŐUTAZÁSRA?



A kezdetektől napjainkig



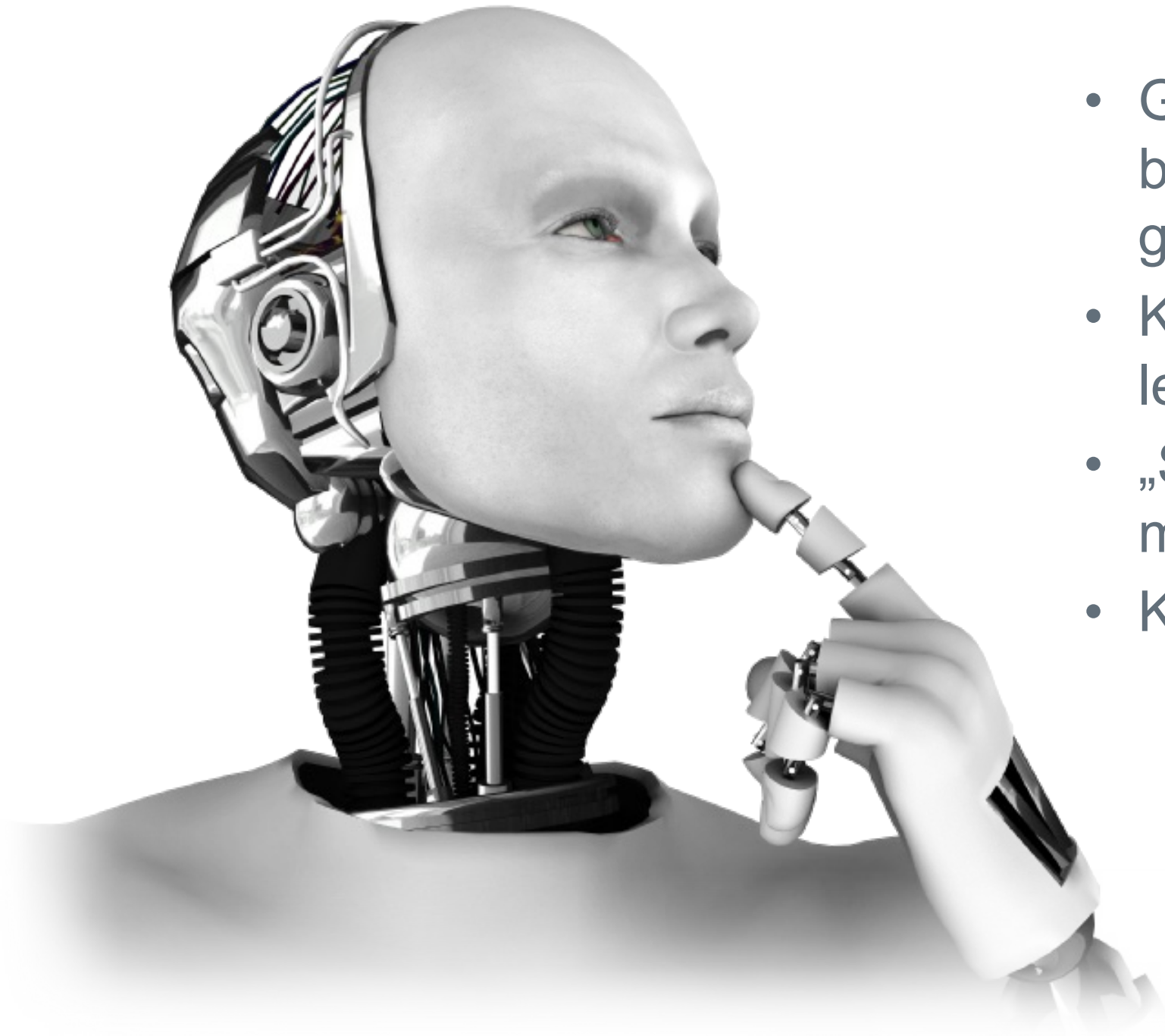
ISACA
Budapest Chapter

NEHEZÍTETT PÁLYA?



- Végpontvédelem
- Spamszűrő
- MFA
- Felhasználói interakció szükségé (makró, biztonsági beállítások, stb.)

VÉDELEM ÉS KÉNYELEM?



- Gyanús tartalom bejelentése gombnyomásra
- Külső feladótól érkező levelek jelölése
- „Secure by default” megközelítés
- Központi cloud előnyei

A LEGGYENGÉBB LÁNCSZEM TOVÁBBRA IS AZ EMBERI TÉNYEZŐ!



- „Ez biztos csak a biztonsági terület újabb tesztje...”
- Megszokott anomáliák
- Alternatív megoldások, kerülőutak
- Szándékos/tudatos szabályszegés
- Utasítások és többletinformációk
- Hogyan mérjük helyesen?

KATTINTÁSI ARÁNY

MÉRÉSI TALÁNY?

Levelet megkapta



99%

Levelet megnyitotta



85%

Linket/fájlt megnyitotta



40%

Tartalmat aktiválta



15%

Hány % és
mikor
jelentette?



ISACA

Budapest Chapter

**„ÉS TÉNYLEG KIADNAK MÉG NEKED
JELSZÓT?”**



TUDATOS TUDATOSÍTÁS!



- Szervezetre és célközönségre szabott módszerek!
- Megfelelő mérések
- Biztonsági események és incidensek észlelése, jelentése, kezelése kiemelt témajavaslat...
- Szemléletváltás

Összefoglalás

- A Social Engineering soha nem megy ki a divatból...
- Megfelelő védelmi intézkedések, technológiai kontrollok alkalmazásával a **támadók dolga jelentősen megnehezíthető...**
- ...de **soha nem zárható ki** a sikeres támadás lehetősége!
- Kiemelten fontos a **megfelelő tudatosítás...**
- ...és ahhoz **megfelelő mérések, auditok** szükségesek!





KÖSZÖNÖM A FIGYELMET!