
# Az innováció útja: hogyan lesz a kutatásból valóság?

Orosz Péter Pál

NBSZ Projektiroda

# K&F&I – INFOLAB kutatások és innováció

K+F tevékenység

- Triggerek, folyamat
- Eredmények, eredménytermékek

Innováció

- K+F elsődleges hasznosulás/eredmény alkalmazás
- Másodlagos felhasználás

# Probléma felvetés – igény a megoldására

- A munka során fellépő nehézségek (időigényes, bonyolult, ismétlődő, NINCS RÁ MEGOLDÁS, stb.),
- Önálló ötlet.

?

# Kutatás-fejlesztés

Van már ismert megoldás a problémára?

Ismert e a probléma?

# K+F

- Ismert e a probléma?
- Felismertük e a valódi problér
- Egy összetevős/komplex prob
- Van e folyamatban kapcsolód kutatási program?
- Mely kutatási tudományágat érinti problémánk?
- Kik lehetnek az együttműköd
- Erőforrás szükséget?

# A K+F tevékenység folyamata

K+F tevékenység

- Pontos elérendő célok meghatározása,
- Eredmények, eredménytermékek,
- Kutatási terv

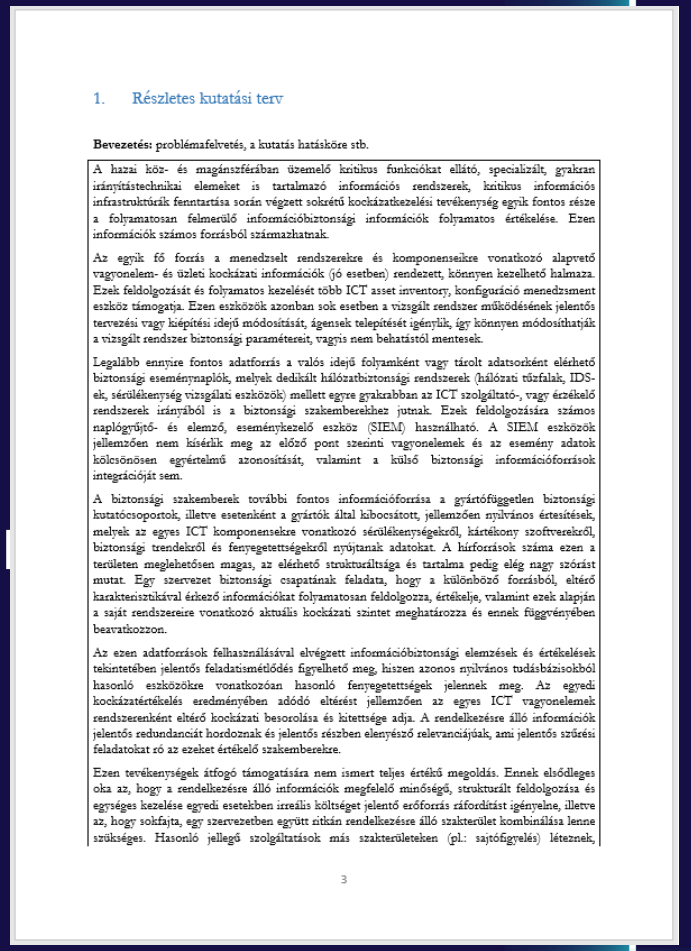
Innováció

- K+F elsődleges hasznosulás/eredmény alkalmazás
- Másodlagos felhasználás

# Kutatási célok

A probléma megoldása érdekében:

- Pontos kutatási célok részletes megfogalm
- Munka és időterv,
- Résztvevők,
- Létesítmények, infrastruktúra,
- Várt eredmények, hasznosulás,
- Költségterv!!!



1. Részletes kutatási terv

**Bevezetés:** problémafelvetés, a kutatás hatásköre stb.

A hazai köz- és magánszférában üzemelő kritikus funkciókat ellátó, specializált, gyakran irányítástechnikai elemeket is tartalmazó információs rendszerek, kritikus információs infrastruktúrák fenntartása során végzett sokrétű kockázatkezelési tevékenység egyik fontos része a folyamatosan felmerülő információbiztonsági információk folyamatos értékelése. Ezen információk számos forrásból származhatnak.

Az egyik fő forrás a menedzselt rendszerekre és komponenseikre vonatkozó alapvető vagyonelem- és üzleti kockázati információk (jó esetben) rendezett, könnyen kezelhető halmaza. Ezek feldolgozását és folyamatos kezelését több ICT asset inventory, konfiguráció menedzsment eszköz támogatja. Ezen eszközök azonban sok esetben a vizsgált rendszer működésének jelentős tervezési vagy kiépítési idejű módosítását, ágensek telepítését igénylik, így könnyen módosíthatják a vizsgált rendszer biztonsági paramétereit, vagyis nem behatástól mentesek.

Legalább ennyire fontos adatforrás a valós idejű folyamként vagy tárolt adatsorként elérhető biztonsági eseménynaplók, melyek dedikált hálózatbiztonsági rendszerek (hálózati tűzfalak, IDS-ek, sérülékenység vizsgálati eszközök) mellett egyre gyakrabban az ICT szolgáltató-, vagy érzékelő rendszerek irányából is a biztonsági szakemberekhez jutnak. Ezek feldolgozására számos naplógyűjtő- és elemző, eseménykezelő eszköz (SIEM) használható. A SIEM eszközök jellemzően nem kísérlik meg az előző pont szerinti vagyonelemek és az esemény adatok kölcsönösen egyértelmű azonosítását, valamint a külső biztonsági információforrások integrációját sem.

A biztonsági szakemberek további fontos információforrása a gyártófüggetlen biztonsági kutatócsoportok, illetve esetenként a gyártók által kibocsátott, jellemzően nyilvános értesítések, melyek az egyes ICT komponensekre vonatkozó sérülékenységekről, kártékony szoftverekről, biztonsági trendekről és fenyegetettségekről nyújtanak adatokat. A hírforrások száma ezen a területen meglehetősen magas, az elérhető struktúráltsága és tartalma pedig elég nagy szórást mutat. Egy szervezet biztonsági csapatának feladata, hogy a különböző forrásból, eltérő karakterisztikával érkező információkat folyamatosan feldolgozza, értékelje, valamint ezek alapján a saját rendszereire vonatkozó aktuális kockázati szintet meghatározza és ennek függvényében beavatkozzon.

Az ezen adatforrások felhasználásával elvégzett információbiztonsági elemzések és értékelések tekintetében jelentős feladatismétlődés figyelhető meg, hiszen azonos nyilvános tudásbázisokból hasonló eszközökre vonatkozóan hasonló fenyegetettségek jelennek meg. Az egyedi kockázatértékelés eredményében adódó eltérést jellemzően az egyes ICT vagyonelemek rendszerenként eltérő kockázati besorolása és kitettsége adja. A rendelkezésre álló információk jelentős redundanciát hordoznak és jelentős részben elenyésző relevanciájúak, ami jelentős szűrési feladatokat ró az ezeket értékelő szakemberekre.

Ezen tevékenységek átfogó támogatására nem ismert teljes értékű megoldás. Ennek elsődleges oka az, hogy a rendelkezésre álló információk megfelelő minőségű, strukturált feldolgozása és egységes kezelése egyedi esetekben irreális költséget jelentő erőforrás ráfordítást igényelne, illetve az, hogy sokfajta, egy szervezetben együtt ritkán rendelkezésre álló szakterület kombinálása lenne szükséges. Hasonló jellegű szolgáltatások más szakterületeken (pl.: sajtófigyelés) léteznek,

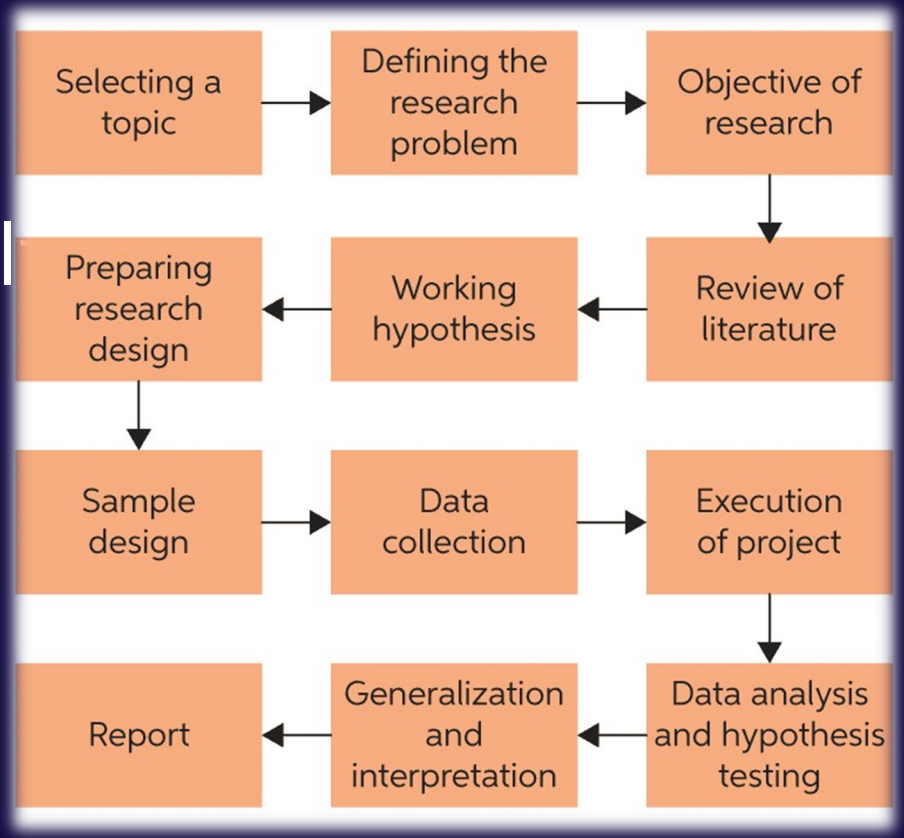
3

# K+F folyamat

- Definiált folyamat,
- Ismétlődhet,
- Cél- és eredmény orientál
- Folyamatos kontroll,

Eredmények alapján:

- Célok pontosítása,
- Munkaterv átdolgozása,
- Egyéb változás kezelések.



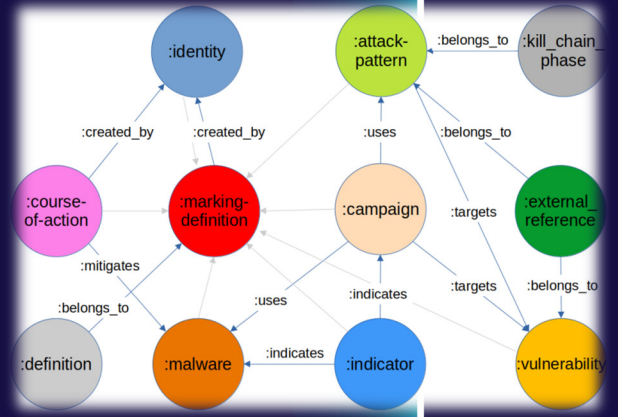
# INFOLAB – RIVET kutatás és eredményei

Sérülékenységi szint megítéléséhez szükséges információk összegyűjthetősége:

- Melyek a releváns információk,
- Hol találhatók, hogyan érhetők el,
- További relevanciák,
- Hogyan értelmezhetők egységesen a fentiek,
- Hogyan viselkedhet a modellezett környezetben egy támadó?

# INFOLAB – RIVET kutatás és eredményei

- Netflow adatok → Neo4j adatbázis → gráf adatbázis
  Adat modellezés + gráf elemzés → sérülékeny csomópontok
  Csomópontok + sérülékenységi jellemzőik → TÁMADÁSI GRÁF
- Anomália detekciók → további sérülékenységi információk
- Architektúra tudásgráf + klaszterezési algoritmusok (**Louvain algoritmus és a KNN**) → node-ok csoportosítása: hasonló tulajdonságok, vagy kapcsolatok alapján →



# INFOLAB – RIVET kutatás és eredményei

- Módosított pagerank (RISKRANK) algoritmus → testbed implementáció → TÁMADÁSI GRAF generáló/kiegészítő, egyszerűsítő
- A támadó viselkedését és az egyes állapotok bekövetkezési valószínűségét szimulálja Markov-lánc alapú módszerrel

- Meghatározhatók az integrity, confidentiality és availability értékek → kockázatértékelés

- Támadási gráf vizualizáció, lekérdezési lehetőségek

# INFOLAB – RIVET kutatás és eredményei

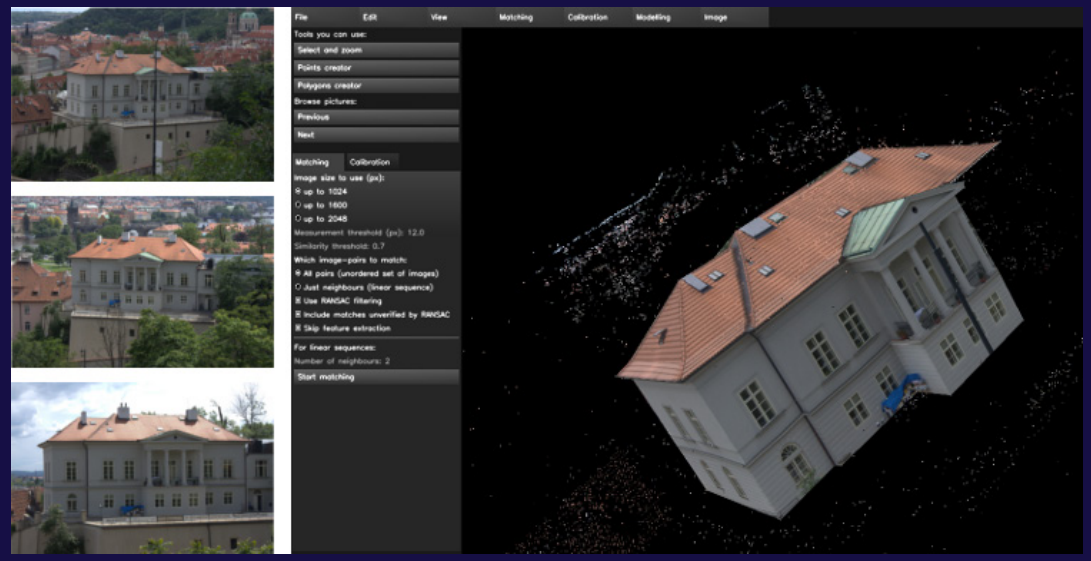
- A prototípus működőképes a SZTAKI openstack felhőjében
- Limitációk (skálázhatóság), további fejlesztési lehetőségek

Innovációs lehetőségek:

- Továbbfejlesztéssel/implementációval valós környezetekben történő alkalmazhatóság,
- Akár „dobozos” termék potenciális előállítása.

# INFOLAB – további innovációk

## Digitális helyszínelés, fotó alapú 3D modell készítés




Események helyszínének felmérése rövid idő alatt

Nagypontosságú, méretarányos 3D modell – digital twin

# INFOLAB – további innovációk

**IT rendszerek üzemeltetés támogatása – anomália detekció**

- INFOLAB közigazgatási/nemzeti adatvagyon védelme kutatások
- AI alapú technológia alkalmazásával va anomália érzékelése
- Meghibásodások előre jelezhetősége
- Megszokottól eltérő működés kimutatása

PREVENCIÓ lehetősége, hatékony üzemeltetés, stb. Közigazgatási szakrendszerekben bizonyított működése

# Köszönöm a figyelmet!

Orosz Péter Pál

orosz.peter@nbsz.gov.hu

+36305630616

INFOKOMMUNIKÁCIÓS ÉS INFORMÁCIÓTECHNOLÓGIAI
Nemzeti Laboratórium

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

CYBERSEC