CTI lehetőségei és kihívásai

Gábriel Gábor

Senior architect

CTI – „Kiberfenyegetettségi hírszerzés”

- Régióval/Országgal/szektorral/szervezettel szembeni potenciális fenyegetésekkel kapcsolatos információk felderítése és analizálása
- Sérülékenységek felderítése
- Reputáció (brand, domain) rombolási kísérletek felderítése
- Elveszett hozzáférések felderítése
- Kiszivárgott adatok felderítése

Lefedett képességek

- Hírforrások felderítése
- Hírszerzéshez szükséges fedés biztosítása
- Beszerzett információk begyűjtése
- Begyűjtött információk osztályozása és több szintű feldolgozása
- Feldolgozott adatokból információk kinyerése és kontextusba helyezése
- Releváns információk operatív csapathoz juttatása (IoC, IoA, Reports by STIX/TAXII, Rest API, email, stb.)

Szükséges képességek (Kihívások 1.)

- Releváns információk befogadása
- Megkapott információk hitelességének ellenőrzése
- Operatív csapatok (SOC/CSIRT) offenzív és defenzív kollégák által történő kiértékelése
- Megkapott információk esetleges hibáinak ellenőrzése
- Védelem elemeinek (use-case, runbook, playbook, stb.) vagy stratégiájának átszervezése

Felderítés módszertanának összetevői

- Magas szintű régió/ország/szektor/szervezet specifikus információk keresése
- Alacsony szintű régió/ország/szektor/szervezet specifikus információk keresése
- Kulcsszavak alapján történő keresések
- Intenció alapú keresése
- Reputáció alapú keresések
- Komplex mesterséges intelligencia alapú keresések (LLM, etc)
- TovábbiAI alapú keresések

Előnyök

- Olyan dolgokat kaphatunk, amivel nem rendelkezünk
  - Képességek
  - Információk
  - Folyamatok
  - Irányítás, szugesszió

Lehetőségek

- Olyan információk beszerzése, amit önerőből nem tudunk előállítani
- Olyan együttműködések, amik korábban nem voltak
  - Gyártói
  - Nemzeti
  - Szektor specifikus
  - Szabadon választott
- Zaj mentes információ elérése végre

Kihívások 2.

- Releváns információforrások megtalálása és megtartása
- Beszerzett információk hitelességének ellenőrzése
- Megfelelő kompetenciák beszerzése és fenntartása
- Relevancia alapján információforrások számának drasztikus lecsökkentése
- Felesleges zaj kiszűrése
- Hatékony folyamatok kialakítása és üzemeltetése
- Új fenyegetettségekkel szembeni védelem megteremtése és naprakészen tartása

KÖSZÖNÖM A FIGYELMET!

Gábriel Gábor

Senior architect

gabor.gabriel@4ig.hu