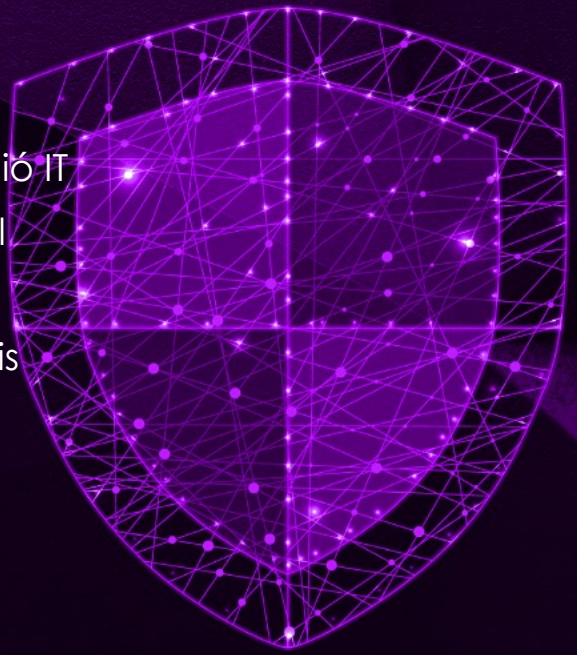
Decloudit Systems

INTERAKTÍV SOC PLATFORM

Menedzselt Security Operation Center szolgáltatás

DecloudIT Systems Kft.

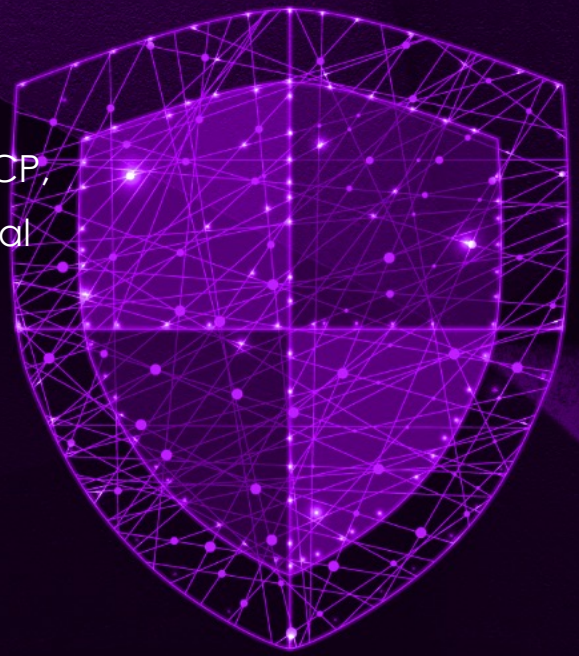
- 2008-ban alapított szervezet vagyunk, mely elsősorban a nagyvállalati tárolási technológiákhoz kapcsolódó tanácsadással foglalkozott. Későbbiekben bővült a portfolió IT Security Audit and Compliance tevékenységekkel. 2017-től kezdve a Cybersecurity együttműködésünket a Fortinettel végezzük. A későbbiekben a Stormshielddel és Penterával is partnerséget alakítottunk ki.



Decloudit Systems

DecloudIT Systems Kft.

- Fő ügyfelek: KKV
- Minősítéseink: CCNA, Fortinet NSE5, PCNSA, CISA, CEH, OSCP, PMI-PMP, GDPR-F, Stormshield CSNA/CSNE, SNIA Professional
- Hivatalos Fortinet Prémium partnerek vagyunk!



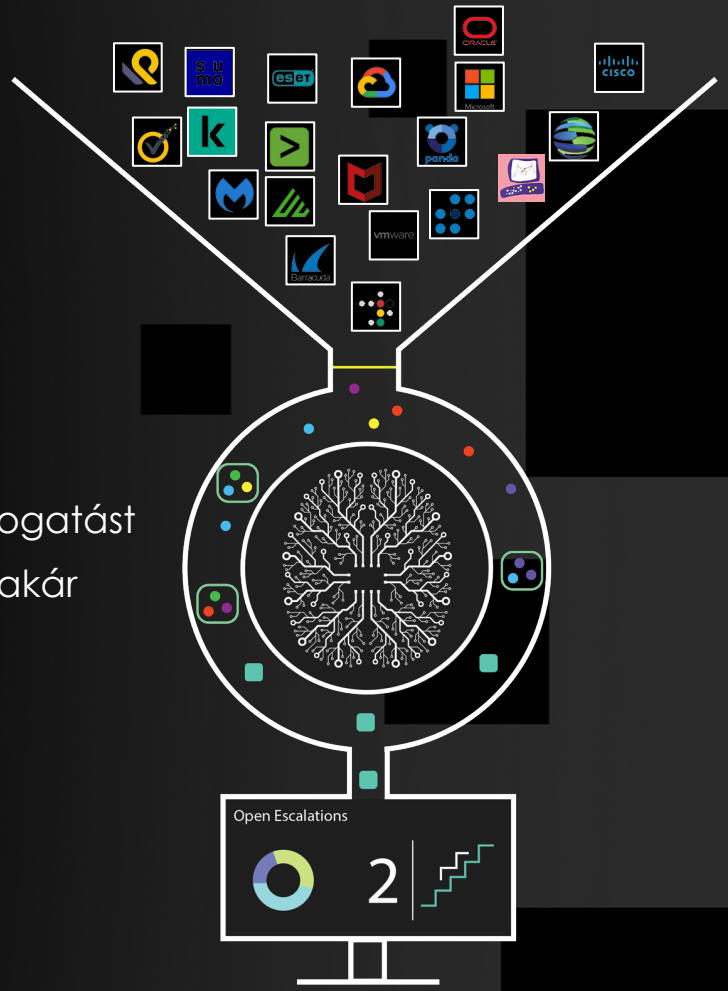
Decloudit Systems

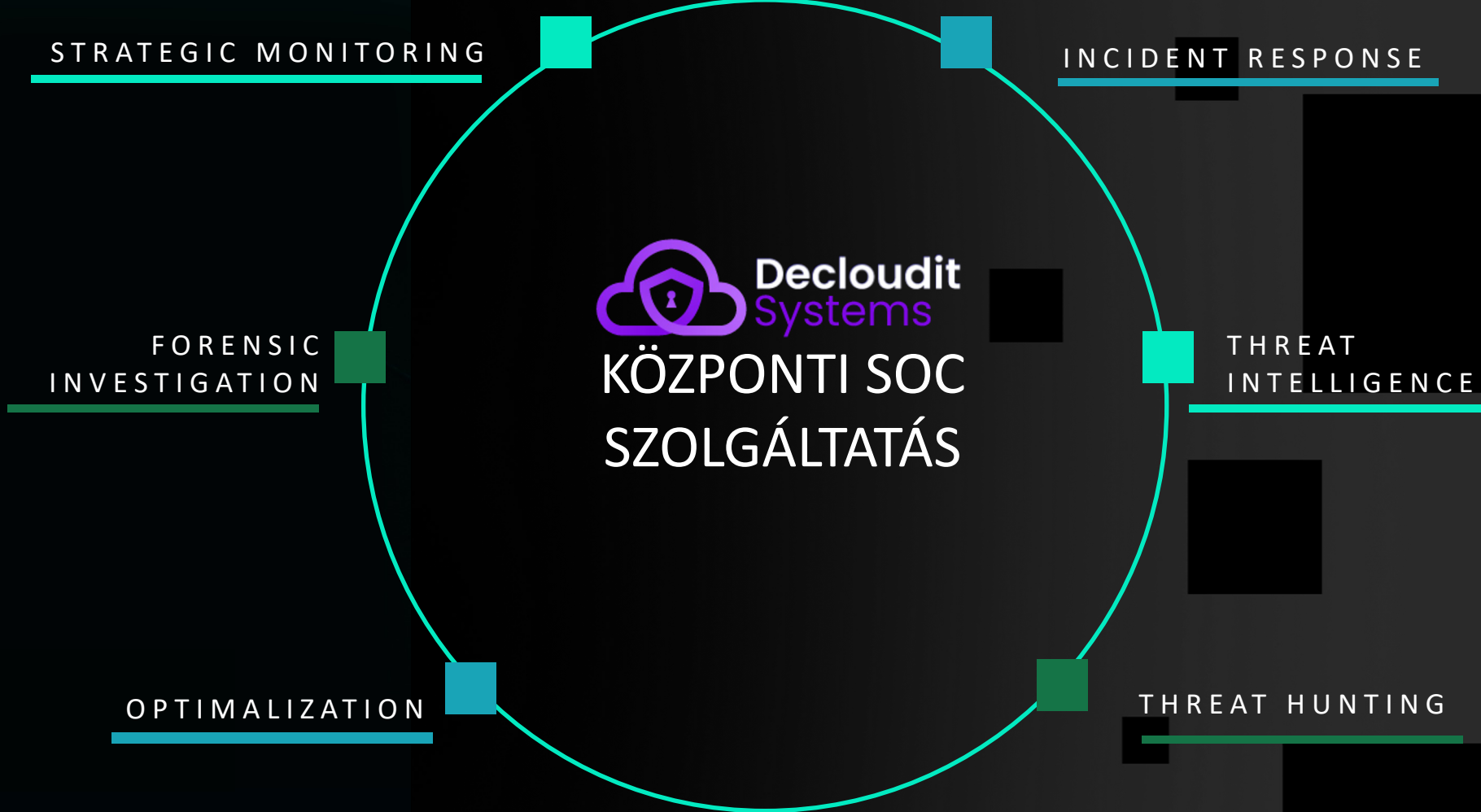
Interaktív SOC platform

- **Hány IT védelmi megoldást alkalmaz?** A kisebb cégek átlagosan 15-20-at, a közepesek 50-60-at, a nagyvállalatok 130-nál is többet.
- **Túl sok az információ?** Egy átlagos cég naponta több, mint 10.000 kiberbiztonsági riasztást kap, ez már önmagában is kezelhetetlen, túl sok erőforrást igényel a menedzselése.
- **A megoldásunk:** Egyetlen központi platform, ami az összes kiberbiztonsági információt összegyűjti és elemzi, valamint megoldási javaslatokat tesz a védelem fenntartására.

Interaktív SOC platform

- Integrálja a felhasználó meglévő rendszerének összes értesítését és adatforrását
- Segít értelmezni, mi történik a rendszerben; az AI összefüggéseket keres az adathalmazokban
- Felhívja a figyelmet a veszélyforrásokra, valamint támogatást nyújt a védekezéshez és a támadások elhárításához, akár szakértők bevonásával
- Felhő alapú modell, valós idejű működéssel
- Az adatközpont EU-n belül, Frankfurtban található




STRATEGIC MONITORING
INCIDENT RESPONSE
FORENSIC INVESTIGATION
Decloudit Systems
KÖZPONTI SOC SZOLGÁLTATÁS
THREAT INTELLIGENCE
OPTIMALIZATION
THREAT HUNTING

Célközönség

A DECLOUDIT SYSTEMS interaktív SOC megoldása ideális minden vállalat mérethez.

NAGY ÉS KÖZEPES VÁLLALATOK

KKV

NAGY ÉS KÖZEPES VÁLLALATOK

Optimalizálja az Ön kiberbiztonsági befektetéseit egy okos, központi platformmal.

Technológiafüggetlen

Bármilyen megoldás, technológia, naplóforrás és végpont integrálva a SIEM-ünkbe; automatikusan hozzáadott új szabályok és összefüggések a képességek optimalizálása érdekében az összes kiberművelet során.

Skálázható

A Cyber-brain-hez csatlakoztatott több mint 350 000 gép több mint 1000 szabadalmaztatott észlelési algoritmust futtat, és több mint 200 millió naplóforrást dolgoz fel és elemez.

Központosított

A központi Cyber-brain (MI) a gyanús tevékenységek kifinomult, többfunkciós észlelésével azonosítja a rendszerek és folyamatok elleni támadásokat a szervezetben.

Transzparens

Egyszerűség és elszámoltathatóság, hogy mindig tudja, mely fenyegetések érinthetik az üzletet vagy igényelnek figyelmet, és hogyan lehet ezeket valós időben mérsékelni.

KKV

Kiberbiztonság végre megfizethető, és érthető formában.

Egyszerűsített kibervédelem

Egyetlen interfész teljes átláthatósággal és jól érthető angol nyelven.

Házon belüli szakértők

Világszínvonalú technológia és tapasztalat, 24/7. L1 támogatás magyarul, igény esetén azonnali beavatkozással.

Költséghatékonyság

A fejlett kiberbiztonság ma már megfizethető az eszközök és ügyfelek hatékony védelme érdekében.

Központi irányítás

Minden eszközt, figyelmeztetést, jelzést és utasítást integrál egy intelligens központi felületre.

Bemutatkozik a Dashboard

- Teljes átláthatóság: az összes vizsgálati eset típus, súlyosság és állapot szerint, valós időben

- Incidens eszkaláció magasan képzett kibervédelmi szakértő bevonásával, amely azonosítja, kivizsgálja és helyreállítja a kiberbiztonsági eseményeket

Bemutatkozik a Dashboard

Analizált események száma az utolsó 24 órából

A rendszer által ismert veszély/támadás korrelációk száma

A felső sor a nyitott vizsgálatokat mutatja típusok szerint

Az alsó sor a nyitott és lezárt vizsgálatok veszélyszintjét mutatja

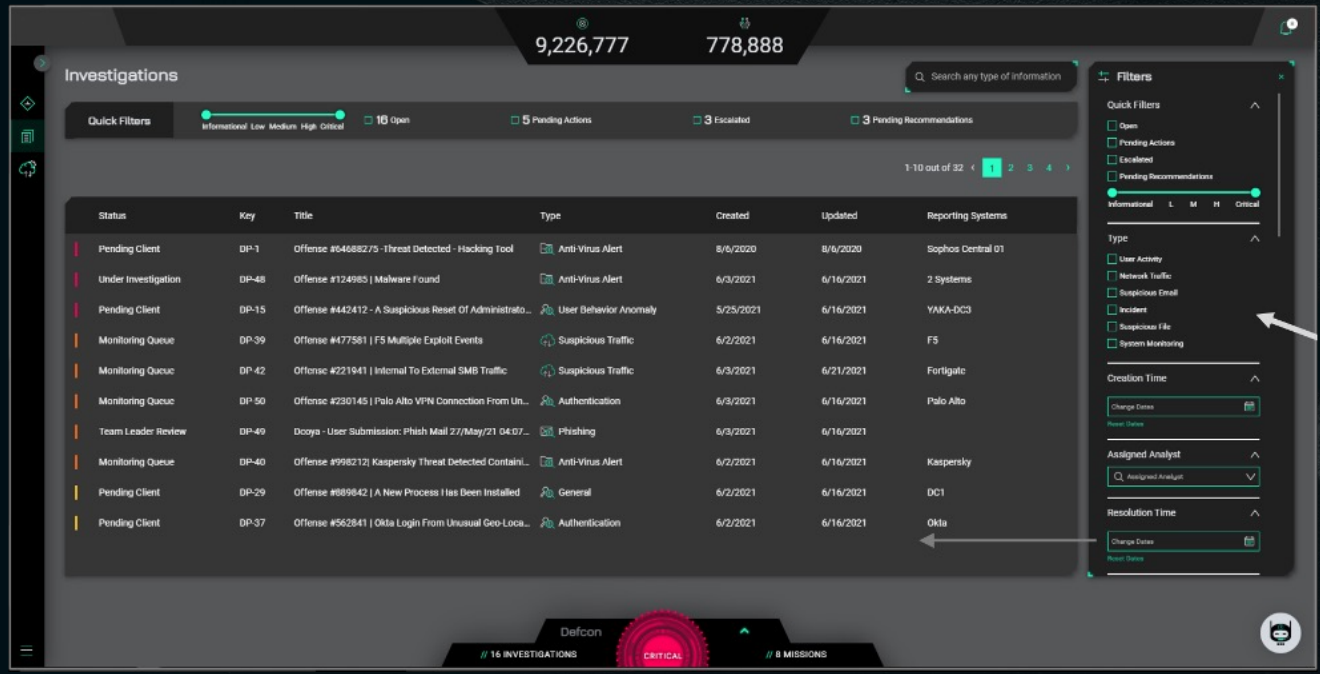
A DEFCON az aktuális fenyegetettségi szintet mutatja

Bemutatkozik a Dashboard

Investigations' képernyő:

Gyanús esemény azonosítását követően vizsgálatot indít a rendszer és figyelmeztetést küld. A listában a jelenleg futó és a lezárt vizsgálatokat látjuk, veszélyességi szint szerint színkódolva. A jobb oldalon szűrési lehetőségeket találunk.

Minden vizsgálatnál részletes információkhoz juthatunk, kiegészítve konkrét megoldási javaslatokkal.



Kérdések és válaszok 1.

- **Kell az ügyfélnek saját SIEM megoldással rendelkeznie?** A kínált megoldásunk tartalmaz felhő alapú SIEM szolgáltatást (IBM QRadar), ezzel rengeteg költség és erőforrás takarítható meg.

- **Biztonságban lesznek az adataim a felhőben?** A felhőbe kizárólag a feltöltéskor titkosított log file-ok továbbítódnak, a felhős megoldás szervereire semmilyen adat nem kerül. A naplófile-ok tárolása 90 napig történik, hosszabbítás kérhető.

Kérdések és válaszok 2.

- **Milyen tanúsítványokkal, megfelelőségekkel rendelkezik a szolgáltatás?** SOC2, ISO 27001, ISO 22301, GDPR megfelelősség, PCI Service Provider level 2.

- **Milyen technológiákkal integrálható a platform?** Bármilyen biztonsági megoldással, technológiával, napló forrással és végponttal zökkenőmentesen együttműködik. Adatközlés „pull” és „push” módszerekkel történhet.

Kérdések és válaszok 3.

- **Mennyi időbe telik a rendszer bevezetése?** A felhasználó rendelkezésre állásától függően átlagosan pár hét.

- **Amennyiben kritikus helyzet áll elő, hogyan avatkoznak be?** Az L2 szakértő (level2) csapat minden információval el fogja látni az ügyfelet a kialakult helyzetről és annak rendezéséről (forródrót telefonon és emailen). L2 szakértő csapat semmilyen körülmények között sem veszi át az irányítást a felhasználó rendszere felett, beavatkozást nem végez! Ugyanakkor a DECLOUDIT SYSTEMS L1 (level1) szakértő csapata átveheti az irányítást az ügyfél rendszerén, amennyiben külön megállapodás van érvényben a napi IT biztonsági műveletek és támogatás területén.

Decloudit Systems

Központilag menedzselt online megoldás világszínvonalú kibervédelmi képességekkel és technológiával:

MEGFIZETHETŐ

SKÁLÁZHATÓ

ÉRTHETŐ

ONLINE 24/7

Kiküszöböli a biztonsági események egymástól elválasztott elemzését,
drasztikusan lecsökkenti a problémamegoldás idejét,
ezáltal elkerülve a költséges károkat és kritikus rendszerleállásokat.

Szívesen megtekintene egy élő demót?

Kérem, jelezze felénk: lajos.bogdan@decloudit.com