BLACK CELL
Protecting critical infrastructures

Átfogó technikai CISO képességek

Készítette:
Dörmő Richárd

23.04.2026

Aktualitás

Miért kell a security vezetőnek hidat képeznie a technikai állomány és a vezetőség között?

73%
CISO stratégiai bevonásának növekedése

94%
AI, mint a kiberbiztonság mozgatórugója

NIS2
Felsővezetői felelősség erősítése

TLP:GREEN

23.04.2026

Eszköz vs Képesség

A gyakorlatban nem csak eszközt veszünk, hanem képességet építünk!

VIZIBILITÁS

- Mit naplózzunk?
- Miből lesz valódi láthatóság?

DETEKCIÓS LEFEDETTSÉG

- SIEM/EDR, mint platform
- Detection engineering, mint képesség

KIEGÉSZÍTŐ INTELLIGENCIA

- Elemzői, mérnöki munka
- Anomáliadetekció, ML, local AI

23.04.2026

Vizibilitás

Mit látunk, és mit nem?

CÉL

Ahelyett, hogy mindent logolnánk, döntsünk annak köréről, amelyből vizsgálat és detekció következik.

APPLOG

Sok helyen alulhasználják, miközben rengeteg üzletileg releváns információ innen származtatható.

OT, IT(L2)

A network mirror ebben az esetben nem extra, hanem alapvető feltétel.

TELEMETRIA MEGVÁLASZTÁSA

Rosszul megválasztva zajt termel, jól megválasztva pedig képességet ad.

- **Azonosítás/hozzáférés-kezelés**
- **Végpont/EDR**
- **Network mirror/east-west**
- **Application logs**
- **OT/Ipari protokollok**

23.04.2026

SIEM/EDR

Önmagában nem képesség, beszerzése könnyű, a használható detekciós képesség felépítése nehezebb.

SIEM/EDR
Alap, de önmagában csak platform.

VALÓDI ÉRTÉK
Szükséges a jó use case, telemetria és üzemeltetés.

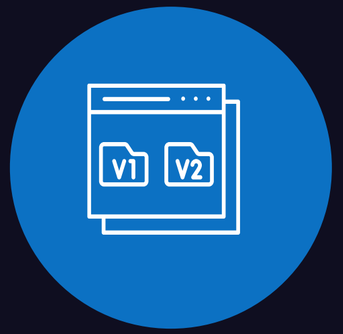
DETEKCIÓ MINŐSÉGE
A rossz minőségű detekció pontatlan, és az elemzők számára is kimerítő.

SECURITY ÉRETTSÉG
Nem a tool megléte, hanem a detekciós képesség a meghatározó.

23.04.2026

Detection Engineering

Detection-as-Code szemlélet lehetőségei.



Verziókezelés & Kollaboráció

Gyorsabb reakció az új fenyegetésekre

Automatizálás & CI/CD

Skálázhatóság & Konzisztencia

Teszt & Validáció

23.04.2026

Anomáliadetektálás és AI

Nem az alapot váltja ki, hanem a szabályokon túli eltérés észlelését támogatja.

NEM CSODASZER

Akkor működik jól, ha stabil telemetriára és jó alapokra épül.

FŐ ÉRTÉK

Eltérés észlelése: nem csak ismert mintát keres, hanem szokatlan viselkedést is.

OT/SPECIÁLIS KÖRNYEZET

Különösen hasznos, ahol a normalitás jobban modellezhető.

ALAP

Szabályalapú detekció, ML kiegészít és priorizál.

23.04.2026

Local AI

Napjainkban az információk sűrítése és a gyors reagálás a legnagyobb értéke, nem az autonóm döntéshozatal.

- Elemzői munka gyorsítása
- Rule/detekció draftolása
- Dokumentáció, tudásmegosztás
- Guardrail

23.04.2026

Összegzés

A technikai tudás nem öncél, hanem hitelességi és döntéstámogatási képesség.

TECHNIKAI HITELESSÉG
Partner a mérnök kollégáknak.

DÖNTÉSHOZATAL
Különbségtétel képesség és tool között.

PRIORIZÁLÁS
A valódi kockázatra tud fókuszálni.

FORDÍTÁS
Technikai paraméterek “board kompatibilis” nyelvre fordítása.

BLACK CELL
Protecting critical infrastructures

Köszönöm a figyelmet!

richard.dormo@blackcell.io

www.blackcell.io