BLACK CELL
Protecting critical infrastructures

Vezérléstechnikai Rendszerek Pragmatikus Kiberbiztonsági Praktikái

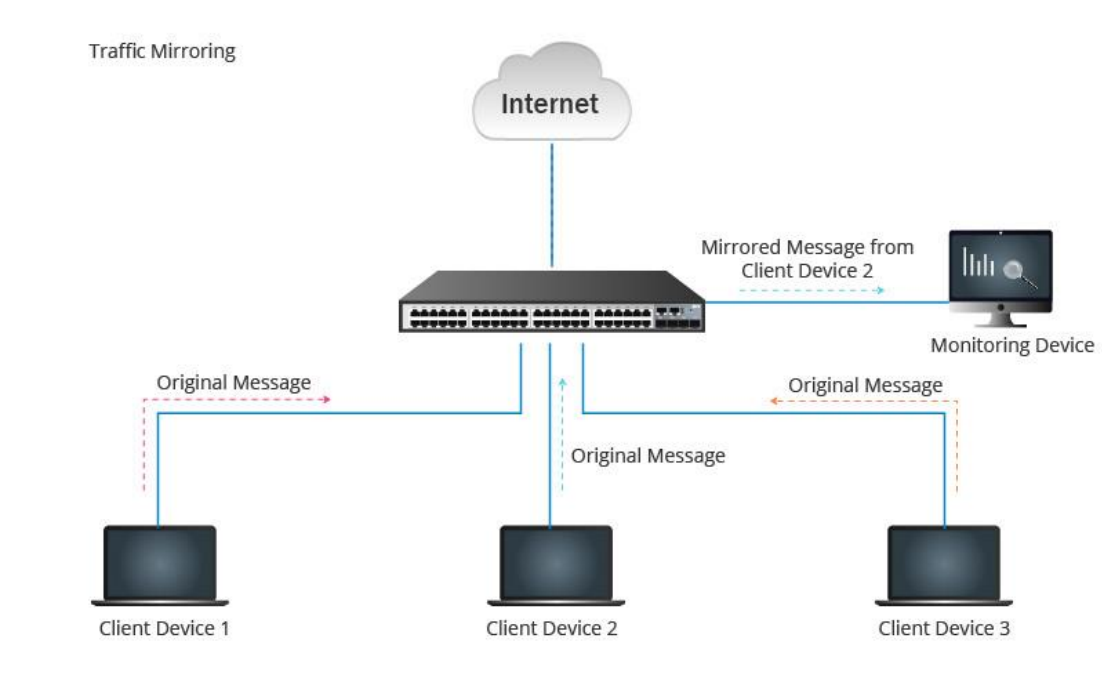
Gyakorlati megoldások

Mit akarunk elérni a vezérléstechinkai kiberbiztonságban?

- Vizibilitás
  - Adatforrások, telemetria
  - Dinamikus leltár
- Kitettség(ek) figyelőztetése
- Központosítás
  - Esemény, eseménysorozat =>? Kockázati tolerancia => riasztás
  - Reaktív eseménykezelés (alacsony fals pozitív számossággal)
  - Szervezetspecifikus baseline felállítása
    - Szektor, lokáció szervezeti érettség
    - "Opportunista" támadások tipizálása
  - Eljárásrendek
    - Operation Manual: OT <=> IT + jog, kommunikáció, vezetőség
    - RACI mátrix
    - Példa: OT AD eseménykezelés
  - Kompetencia

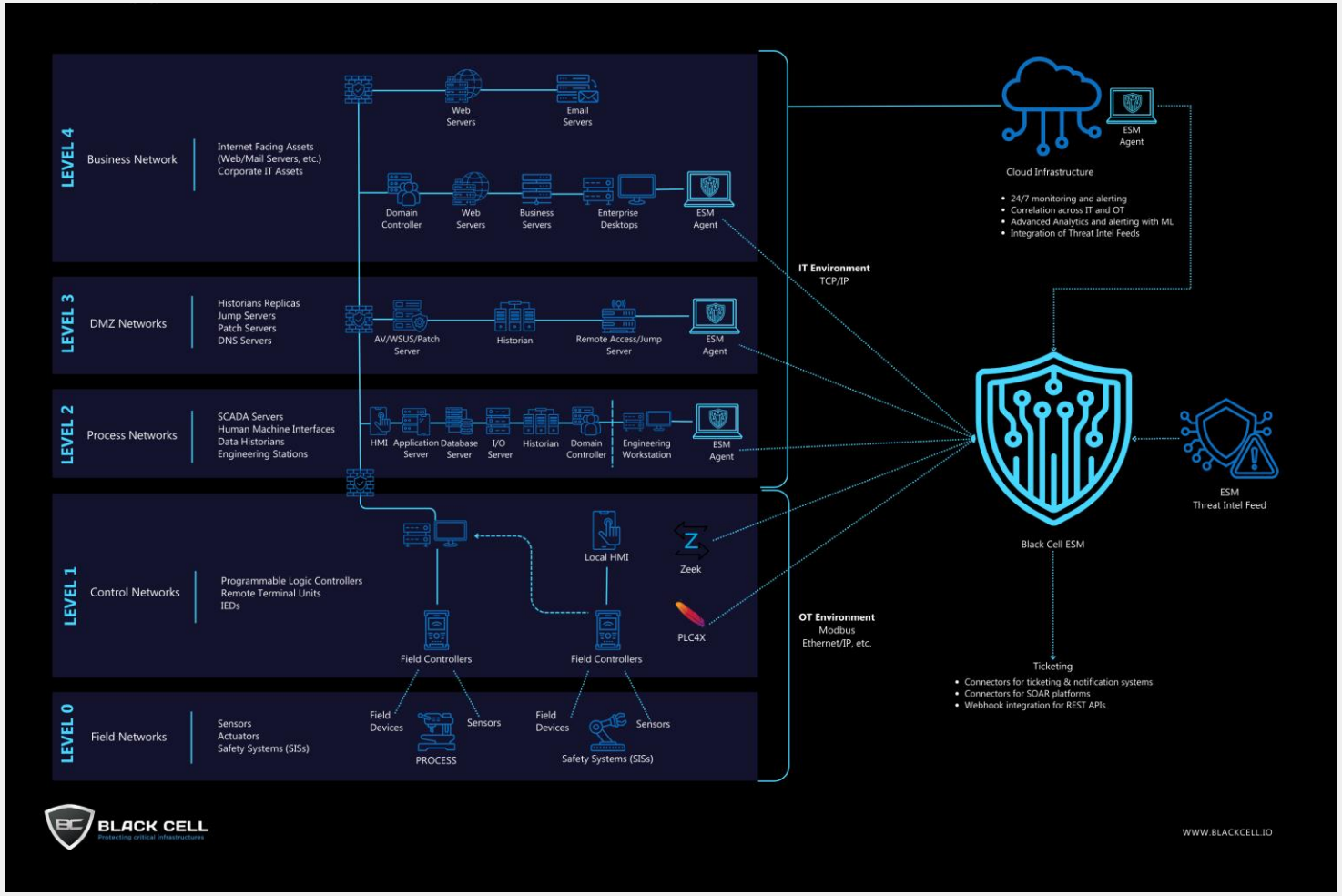
Kitükrözött hálózat | Koncepció

- Mivel?
  - Mirror port
  - Network TAP
  - Packet Broker
- Miért?
  - Dinamikus leltár (hardware, software)
  - Sérülkenységek
  - Szignatúra és anomália alapú riasztások (port, protokoll, üzleti logika)



Kitükrözött hálózat | Gyakorlat

- Suricata: Intrusion Detection System
- Zeek: Protokollok értelmezése: *Modbus, DNP3, Ethernet/IP és CIP, BACnet, BSAP, Ethercat Genisys OPCUA, Profinet IO CM, S7Comm MQTT, MMS, Goose*
- Fájlok vizsgálata
- Elastic: Log aggregációs és adatmanipulációs platform

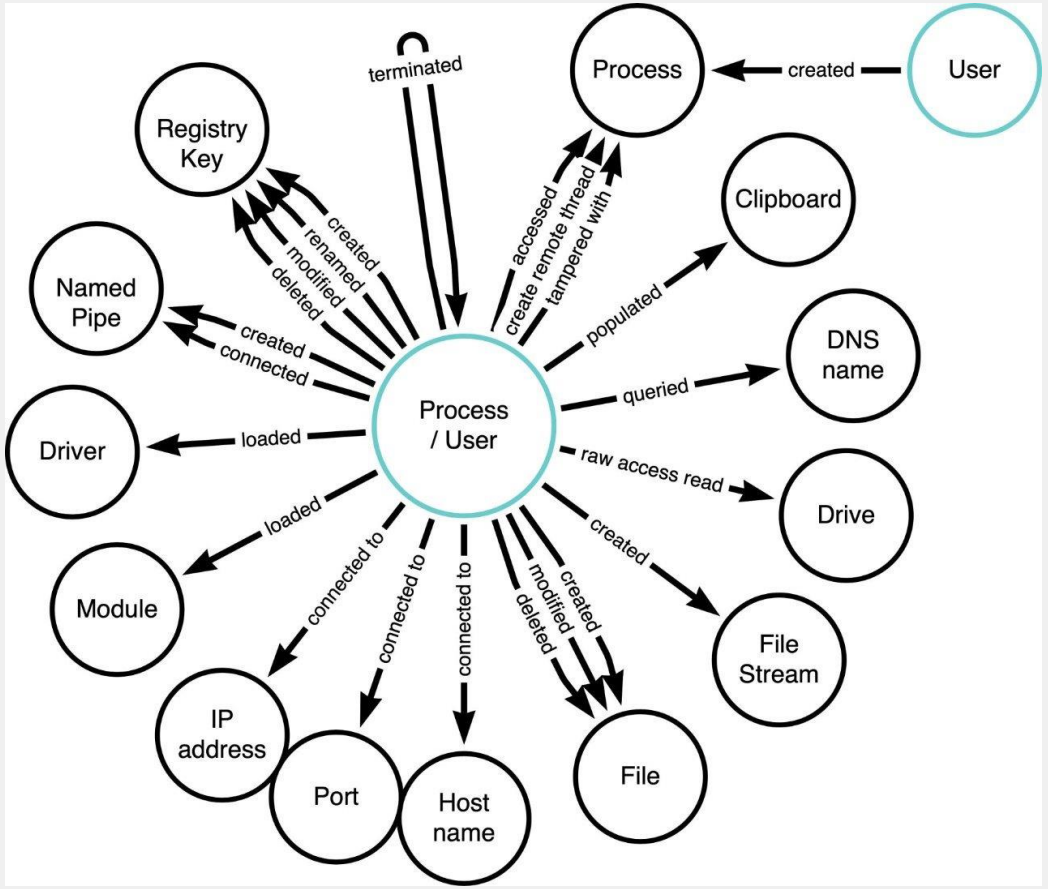


Végpont telemetria | Elmélet

- *nix naplók
- Windows naplók
- Egyedi OT eszközök logolása
- Hozzáférések naplói
- Alkalmazások
- Rendelkezésre állás

Végpont telemetria | Gyakorlat

- Sysmon
- Auditd
- Sigma szabályok 3000+ riasztási szabály
  - application
  - cloud
  - compliance
  - linux
  - macos
  - network
  - web
  - windows

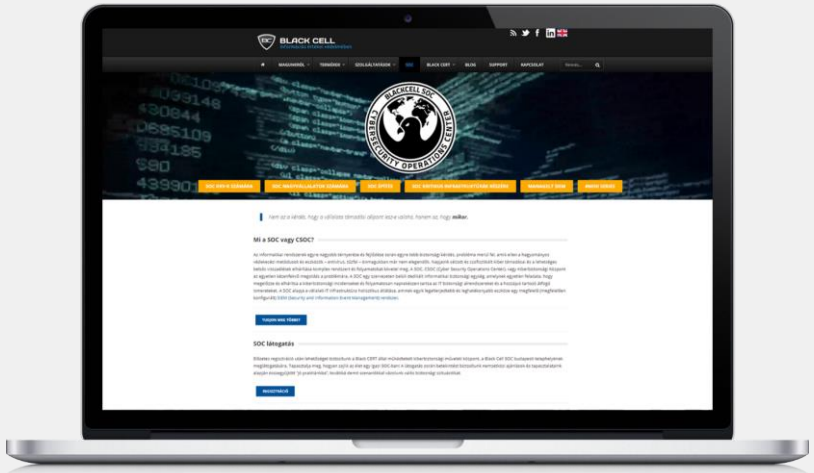


Honeypot-ok

- A hálózaton belül telepített, valódi eszközöket imitáló, a támadókat a tényleges célpontokról elterelő rendszerek.
- A támadók bevonására és megtévesztésére tervezték, korai észlelést és fenyegetés-felderítést biztosítva.
- Szimulált sebezhetőségek és szolgáltatások, lehetővé téve a taktikáik és technikáik tanulmányozását.
- Növeli az újonnan megjelenő fenyegetések és sebezhetőségek megértését.
- Stratégiailag elhelyezett honeypot-ok, amelyek a támadókat jelenlétük felfedésére csábítják.
- Megtévesztő adatbázisok: Fiktív adattárak, amelyek a támadó számára hitelesnek tűnnek.

Tesztelni, gyakorlatozni

Köszönöm a figyelmet.



https://blackcell.io/

info@blackcell.io

TLP: GREEN

Források:

- Zeek: https://github.com/zeek/zeek
- Industrial Control Systems Network Protocol Parsers (ICSNPP): https://github.com/cisagov/icsnpp
- Suricata: https://github.com/OISF/suricata
- Sigma: https://github.com/SigmaHQ/sigma
- Elastic: https://www.elastic.co/
- Opencanary: https://github.com/thinkst/opencanary
- SecurityOnion: https://securityonionsolutions.com/