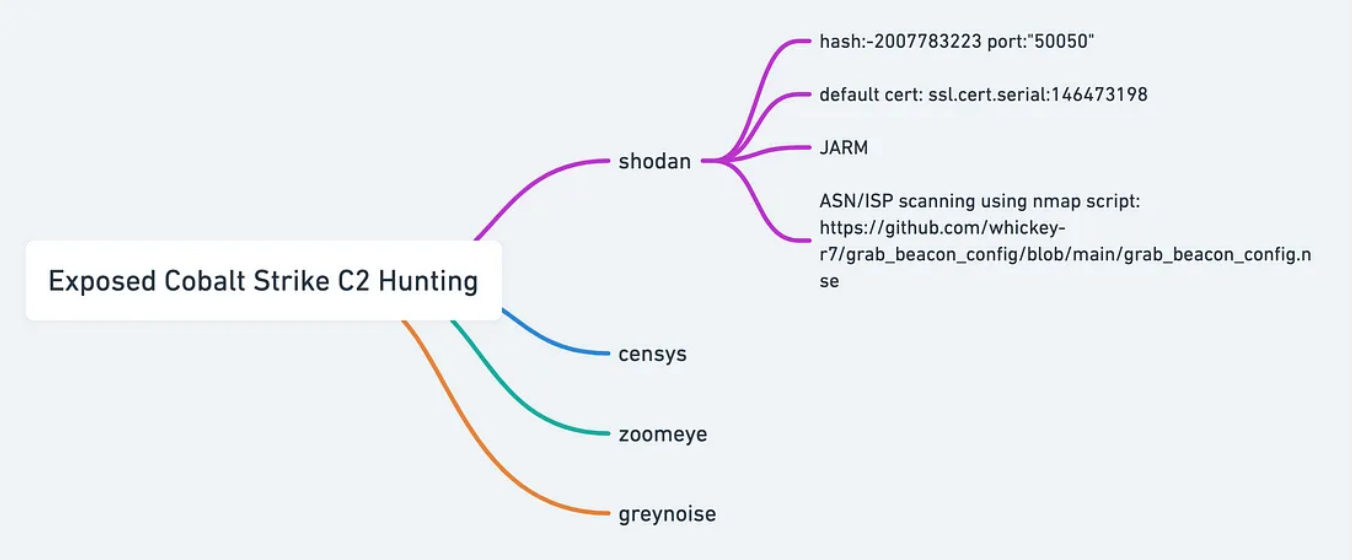
BLACK CELL
Protecting critical infrastructures

Technikai indikátorok fogyasztása és feltételeik

EIVOK-47 Cyber Threat Intelligence
(CTI) aktuális kérdései Tudományos - Szakmai Konferencia

Határvédelem

- C2 infrastruktúra query-k Shodan-al és/vagy Censys-el:
  - Cobalt Strike,
  - Silver,
  - Mythic,
  - Pochc2,
- DNS:
  - DGA,
    - Entrópia?
  - Tunnel (TXT rekordok)
  - => Sinkhole
- MISP
  - ISAC-ek
  - TOR Exit node-ok



Kitükrözött forgalom

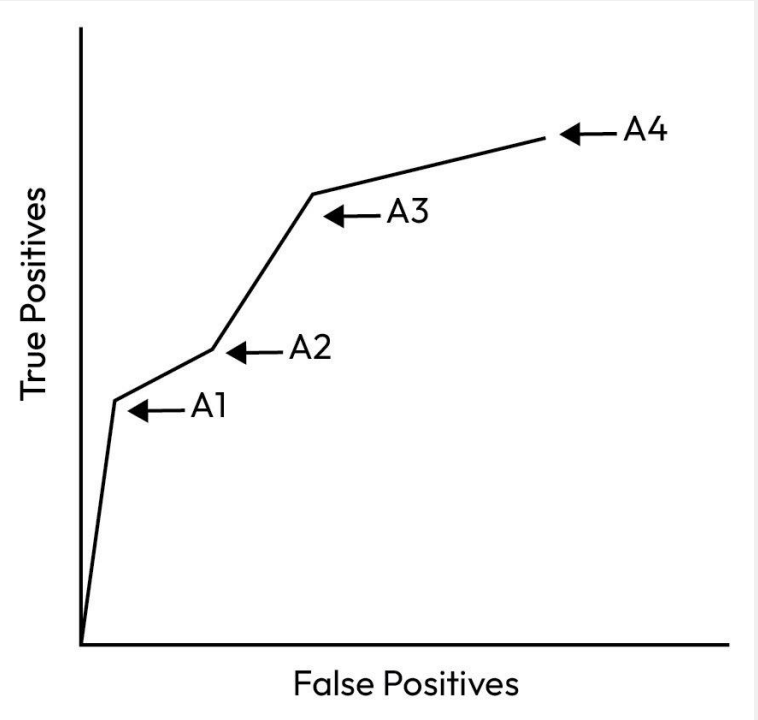
- Suricata as an IDS
  - Network rules
    - SNORT syntax
    - Detection Engineering
- Zeek
  - Protokoll stack bővítésre
    - BACNet
  - YARA rule-ok
- p0f
  - Leltár
  - NVD?

SIEM rule-ok

- High level IoC-k
  - Lookup táblák készítése
  - Retrospektív elemzés
- Cybersquatting
  - Index.hu (kis L-el)
  - Védett beszállítók listája <=> message trace log-ok
- Tunneling
  - DNS TXT, CNAME, NULL rekordok
  - Rövid TTL-ek
- ATO
  - Ldap query
- Detection as Code

Detection as Code

- SIEM riasztások threat feed-ként
- Többszörösen tesztelve
  - Linting
  - RTA
  - Peer review
- Tag-elve
- Minimális emberi hibalehetőség
- MITRE Heatmap-ek
  https://github.com/blackcellltd/Heatmaps
- Detection engineering
  lifecycle alapján folyamatosan fejlesztve



Kérdések

Cybersecurity today is a race between defenders striving to build bigger and better idiot-proof programs and the universe trying to produce bigger and better idiots. So far, the universe is winning. (Orig.:Robert Cook)

Elérhetőségeink

https://blackcell.io/

info@blackcell.io