TLP:CLEAR

ALEF

Prevence je ideální, ale detekce je nezbytná:
modelování hrozeb pro oblast security operations

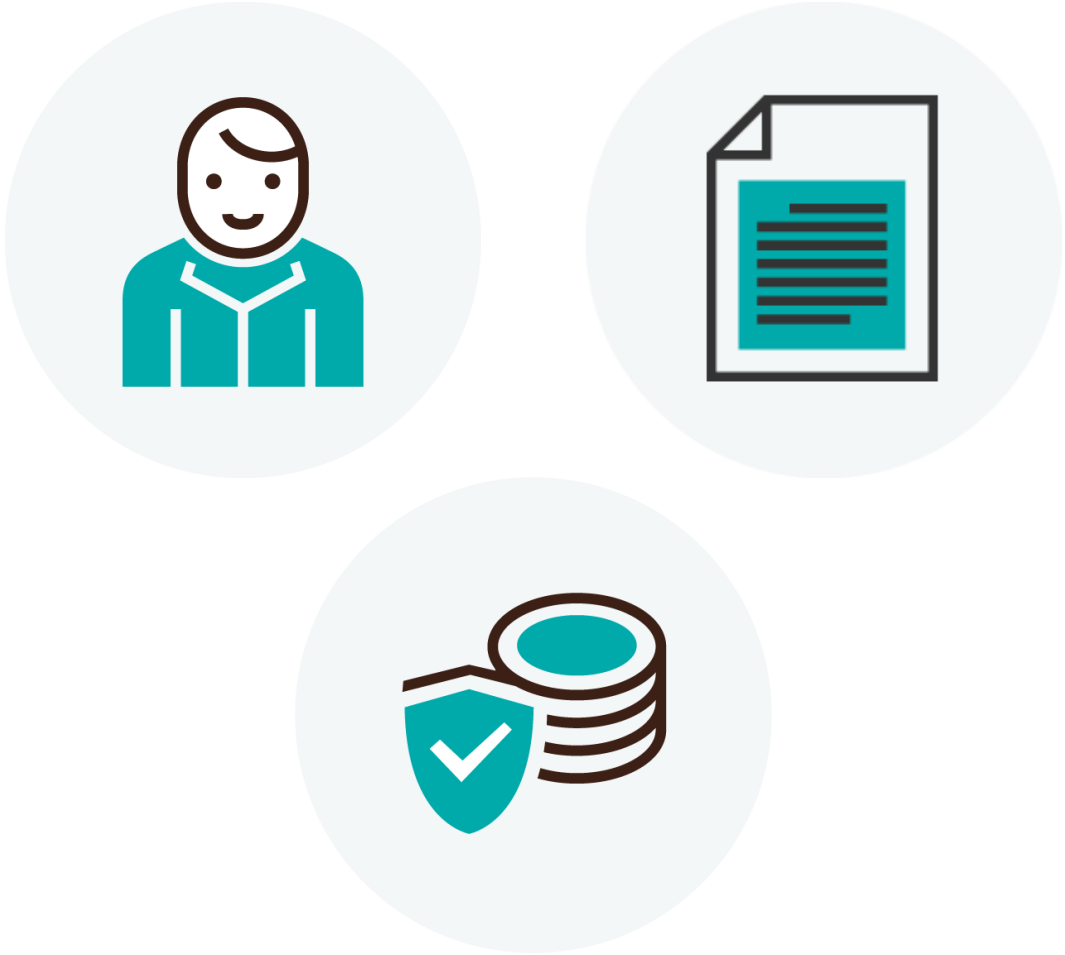
Jan Kopřiva

Senior Security Consultant

jan.kopriva@alef.com @jk0pr

Efektivní (nejen) modrý tým

- 3 hlavní pilíře (PPT)
  - Lidé
  - Procesy
  - Technologie



ALEF

(Ne vždy) historický pohled na SOC

- Hlídáme perimetr a stanice v interní síti
  - Perimetrová IDS/IPS
  - Analýza NetFlow
  - Logy z anti-malware nástrojů
- Vzhledem ke standardnímu fungování mnoha moderních organizací (WFH, BYOD, cloud-first, …) již delší dobu nevyhovující koncepce

Vhodný moderní „modrý“ technický základ

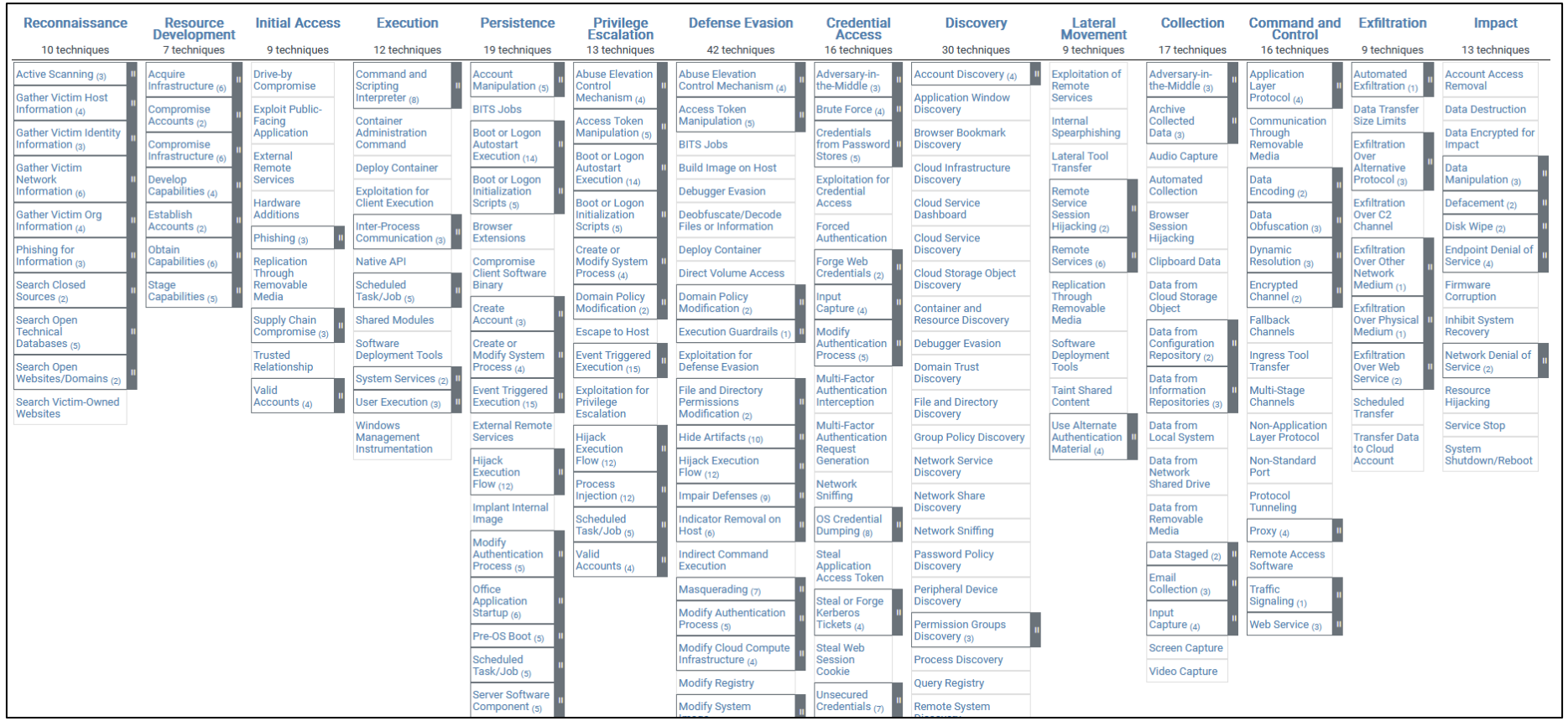
- Pokrytí 3 domén
  - Síť
    - IPS, NetFlow/IPFIX/Service-level analytika, „always on“ web proxy
  - Koncové body
    - AV/EPP, EDR
  - Aplikace
    - Nativní logy aplikací, reverse-proxy, …
- On-premise, mobilní i cloudové systémy

Postačuje takový přístup?

- „Nástroje X, Y a Z nám zajišťují detekci…“
  - Žádný nástroj nedokáže zachytit vše
  - Týmy, které se omezují výhradně na využívání out-of-the-box funkcionalit bezpečnostních nástrojů si samy svazují ruce
  - Je nezbytné využívat bezpečnostní nástroje, ale i **další zdroje dat** (ne nezbytně bezpečnostní) pro bezpečnostní dohled

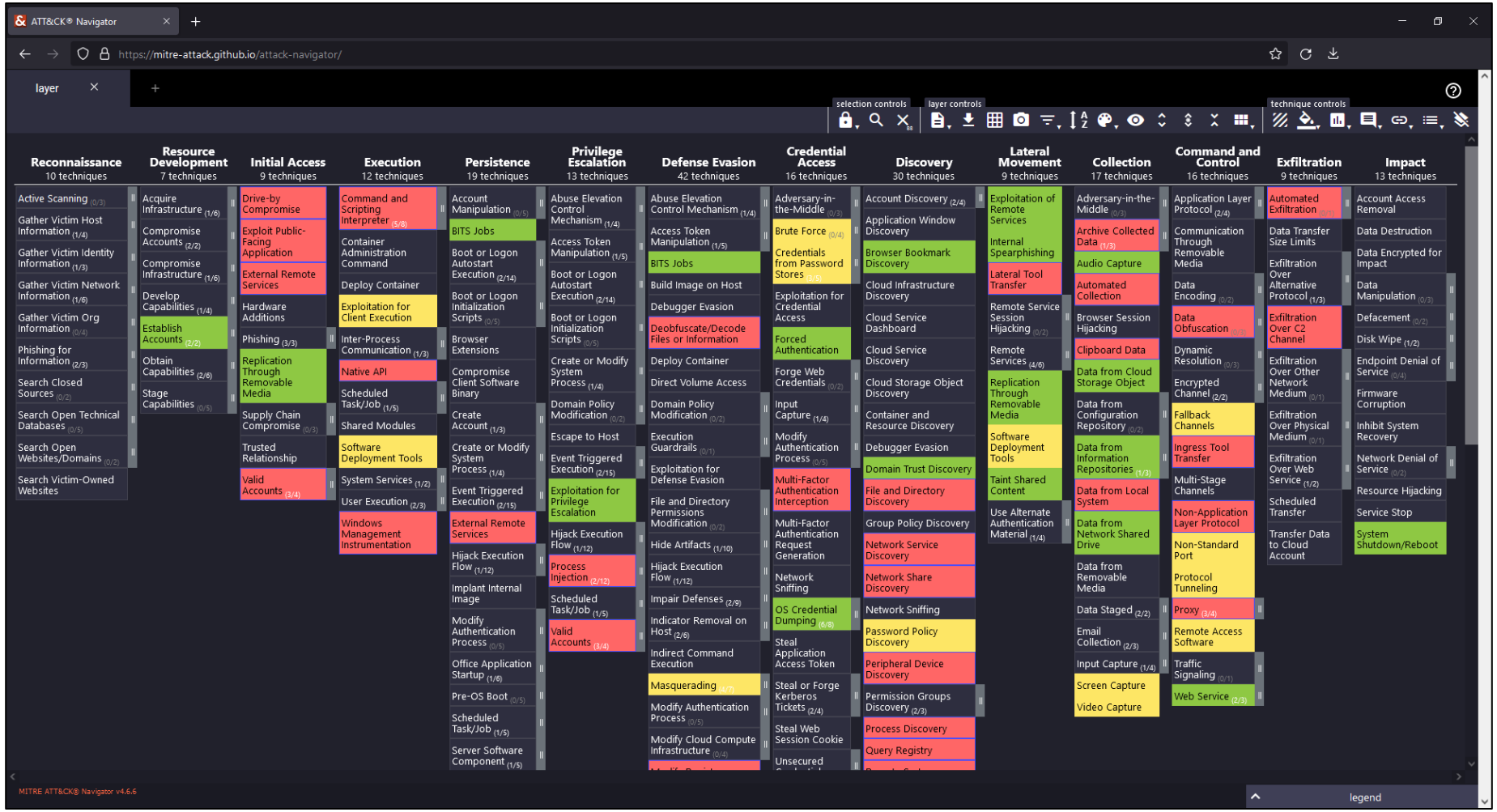
Oblast hrozeb je extrémně široká

- Reálně nelze pokrýt vše…



Zdroj: MITRE

Modelování hrozeb na vhodné úrovni



ALEF

Optimální stav

- Pokrytí (nejen) relevantního modelu hrozeb
  - Z pohledu prevence
  - Z pohledu detekce
  - Z pohledu reakce
- Vhodné vytvoření samostatných modelů pro jednotlivé oblasti

→ Pro efektivní defenzivu platí, že prevence je ideální, detekce je nezbytná

Jak na nepokryté oblasti modelu hrozeb?

- Vlastní analytické mechanismy
  - Korelační pravidla a signatury „na míru“
- Méně obvyklé zdroje dat
  - Specifické logy z OS, pokročilé nástroje (Sysmon, eBPF, …)
- „Kompenzační“ datové zdroje pro chybějící vstupy (nejen) na úrovni aplikací
- Silná automatizace s pomocí SIEM, SOAR a/nebo skriptů
  - Externí vstupy pro obohacení dat

Jak postupovat?

- Začínat s „out-of-the-box“ funkcemi bezpečnostních nástrojů je v pořádku
- Je však nezbytné u nich neskončit
  - Vedle technických detekčních mechanismů vhodné zhodnotit i možnosti využívání threat huntingu
- Prostor pro rozšíření (nejen) detekčních kapacit „modrých“ týmů je téměř neomezený
  - Rozvoj nezbytné (alespoň do jisté míry) řídit

Jak postupovat?

ALEF

Periodické ověřování stavu

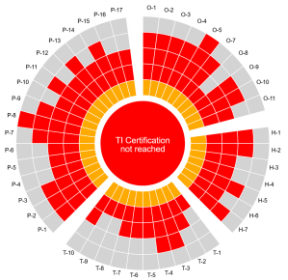
- Audity a (sebe)hodnocení
  - SIM3
  - SOC-CMM (a 4CERT)
  - MITRE ATT&CK a D3FEND
- Praktické testy
  - Red teaming
  - Purple teaming

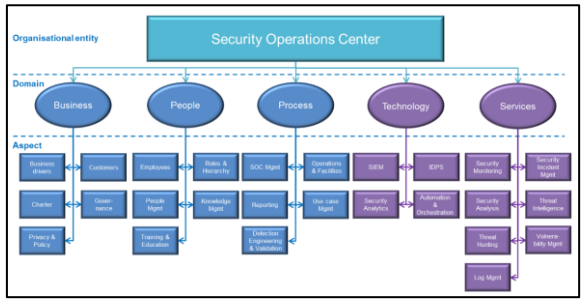
Metodiky nejen pro audity a (sebe)hodnocení

SIM3

SOC-CMM
4CERT

MITRE ATT&CK



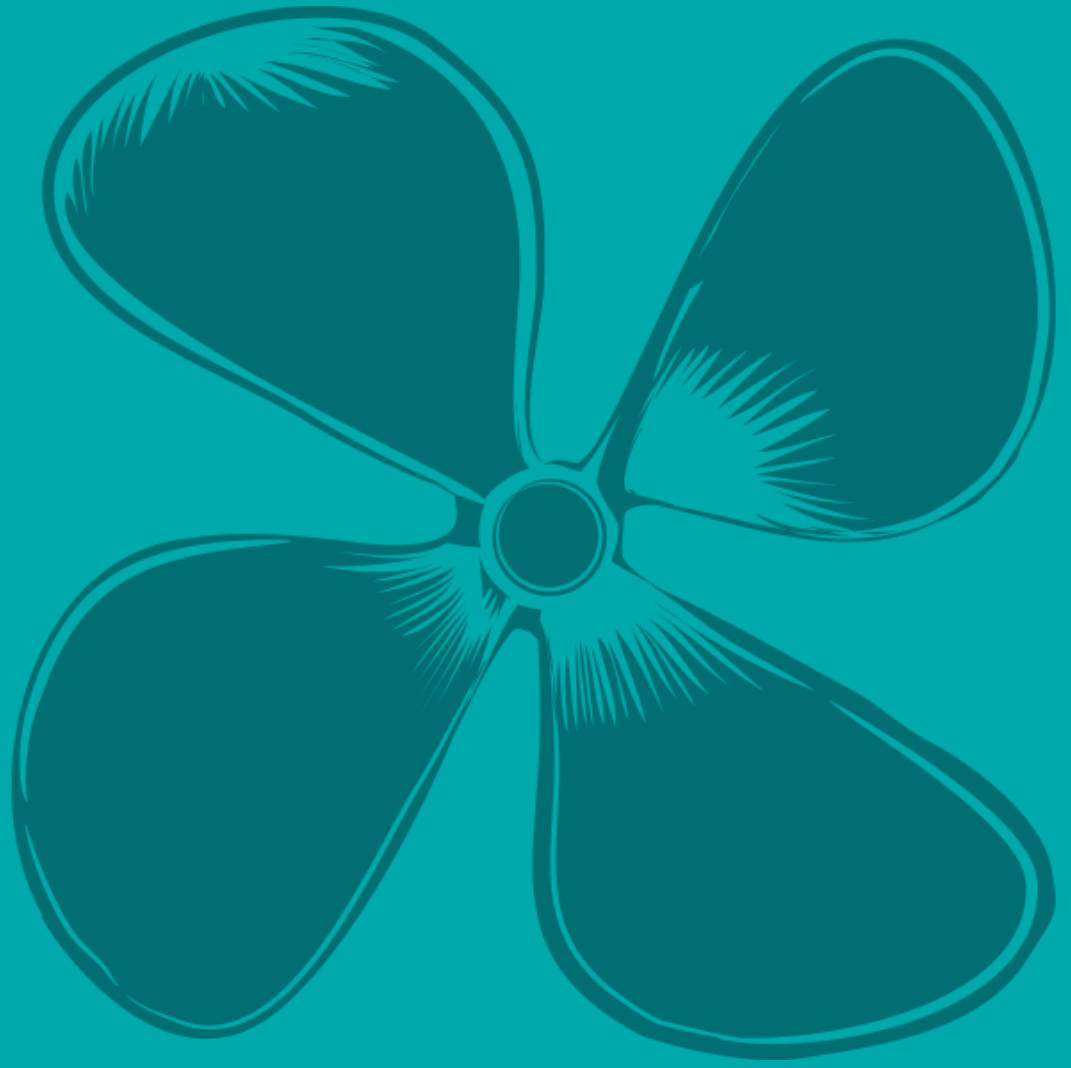


ALEF

Zdroj: OCF, SOC-CMM, MITRE

ALEF

Prostor pro Vaše dotazy



TLP:CLEAR

ALEF

Děkuji Vám za pozornost