Üdvözlöm!

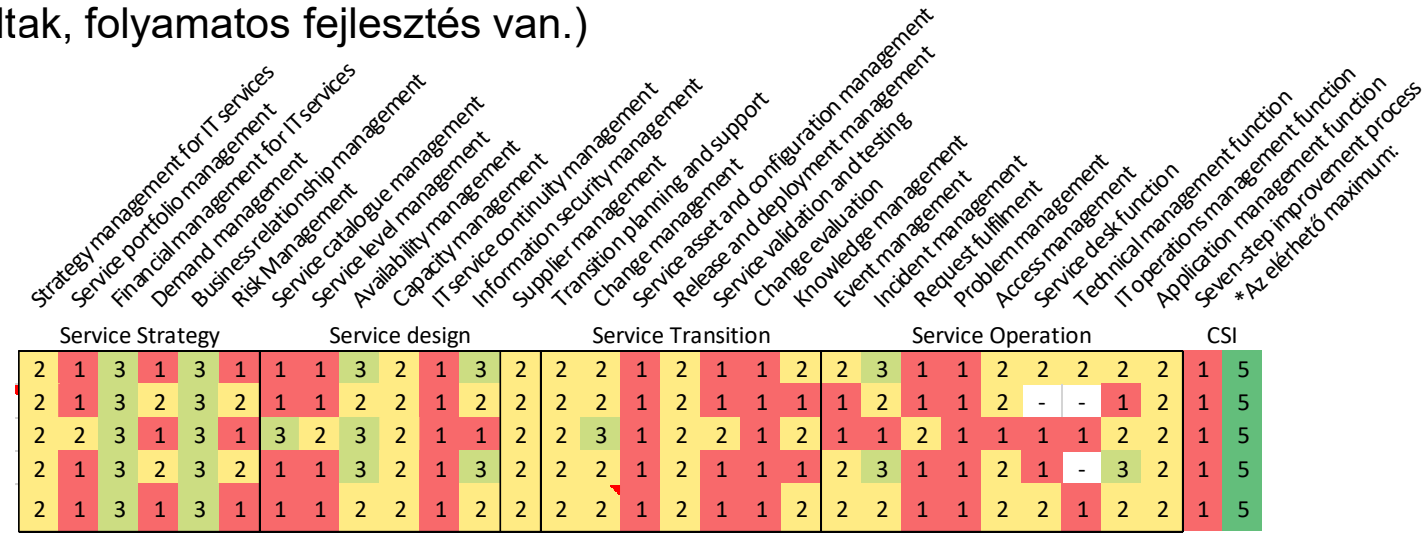
SOC bevezetési Stratégiák

HTE EIVOK 36 Konferencia

Lázár Tamás

Érettség

- Mi a szervezet érettségi szintje? (Egy ITIL alapú érettségi heatmap a lenti ábrán)
- CMM (Capability Maturity Model) 5 szintű skála
  - Initial (Kezdeti szint, a folyamatok nem szervezettek)
  - Repeatable (A főbb folyamatok dokumentáltak, megismételhetők)
  - Defined (A folyamatok pontosan definiáltak, belső szabványok megjelennek)
  - Managed (A folyamatok mértek, felügyeltek)
  - Optimizing (A folyamatok visszacsatoltak, folyamatos fejlesztés van.)
- A szervezet ≥ 3?
- Fontos a dokumentáltság is:
  - (Karbantartott) asset leltár, CMDB, Hálózati térkép, stb.



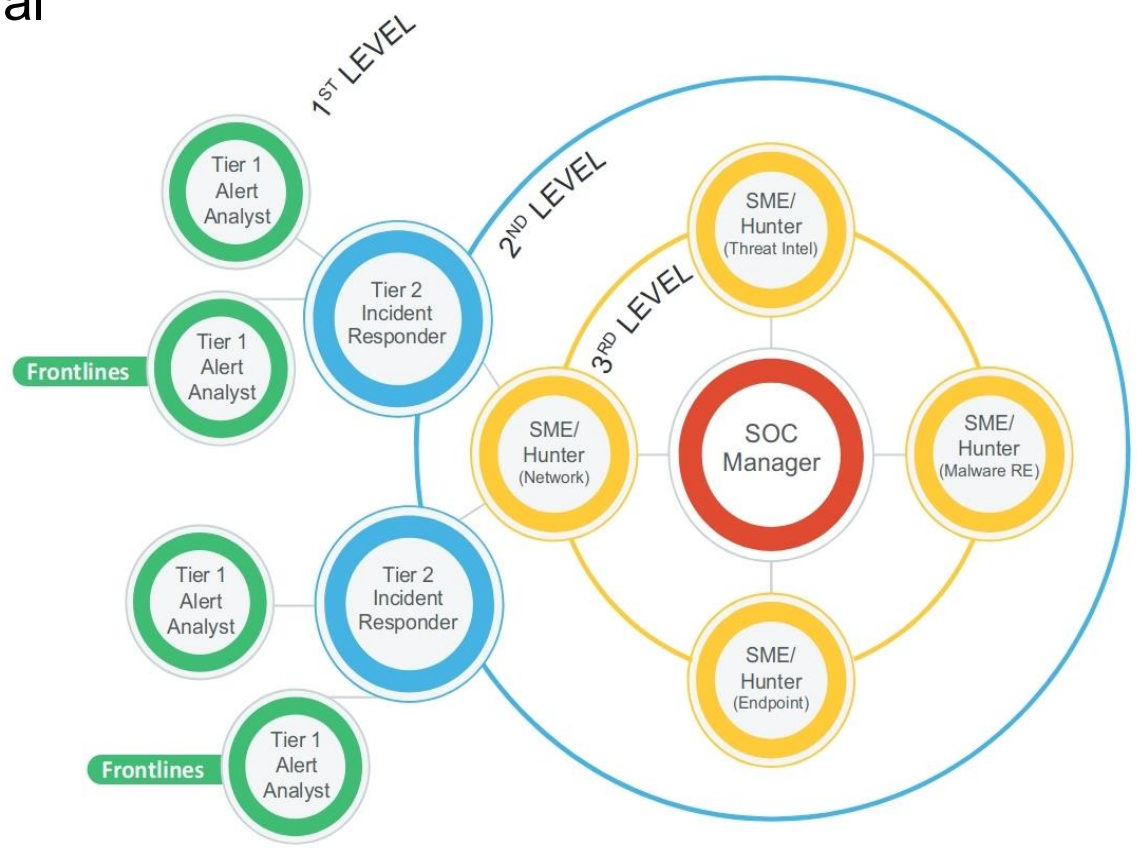
Adminisztratív feladatok 1

- (Megvalósíthatósági tanulmány, tool-ok kiválasztása)
- Stratégia – Vezetői elkötelezettség
- SOC szabályzat – SOC működési szabályai
- SZMSZ + IBSZ – SOC helye a szervezetben
  - IT
  - ITB
  - Bankbiztonság
- Szakmai szabályzatok
  - Incident Response
  - Threat Intelligence
  - (Vulnerability Management)

Adminisztratív feladatok 2

- Pozíciók – a szokásos elvárt dokumentációval
  - SOC Manager
  - L1 analyst
  - L2 analyst (Incident Responder)
  - L3 analyst (Threat Hunter)

- Playbook-ok elkészítése
  - Kategorizálás
  - Step-by-step útmutató a riasztás kezelésére
  - Eszkalációs terv
  - Incidens válaszlépések
  - Incidens kommunikációs terv

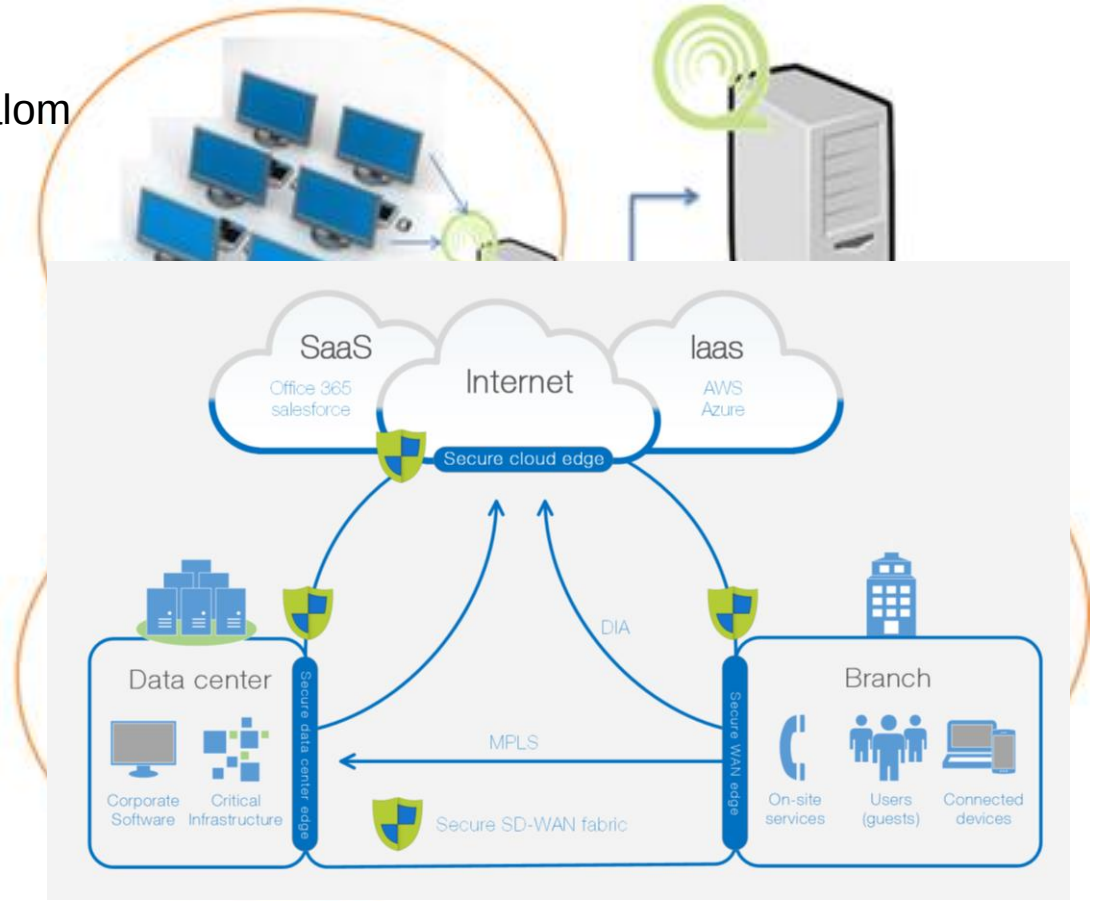


Adminisztratív feladatok 3

- Reagáló csapatok
  - Vezetői támogatás ! – gyakori IT ellenérdekeltség
  - Megkerülésük (ki, hogyan, milyen elszámoltatás mellett?)
    - Felelősség kérdése
  - SOAR?
- SOC teljesítmény mérése – KPI-ok meghatározása
  - Mérhető kell legyen
- HR stratégia
  - Kiégés

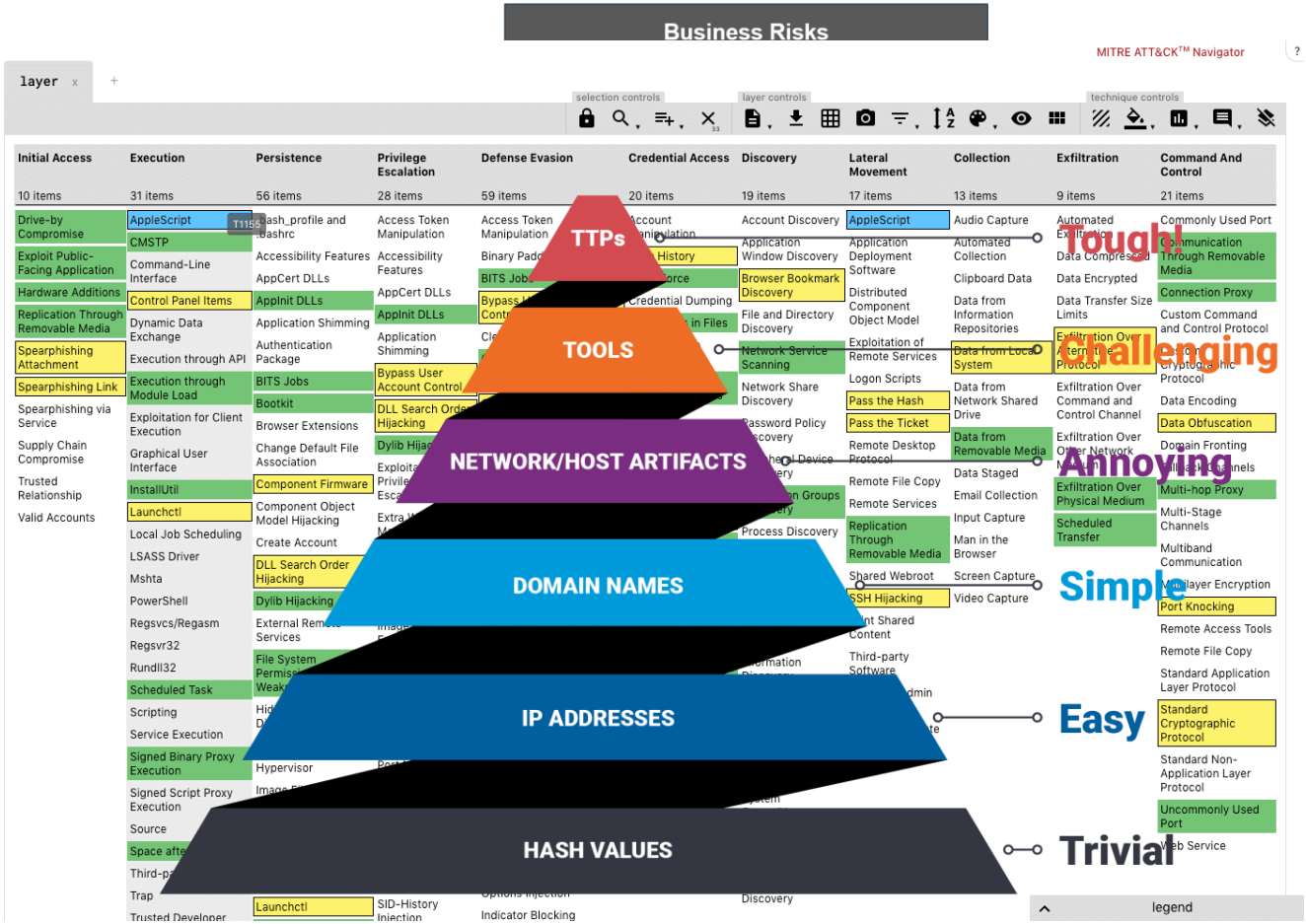
Technikai feladatok

- Architektúra, hálózat **pontos** ismerete
  - Telephelyek, azok összeköttetései (VPN, MPLS, SD-WAN)
  - Használt Cloud technológiák elérése. SSE technológiák?
  - Hálózati architektúra, (mikro)szegmentálás, É-D, K-NY forgalom irányítása
  - Virtualizált hálózati architektúra: kontérerek/podok közötti forgalom, SD-LAN
  - Hálózaton belüli védelmi technológiák (Honey-pot, IDS, stb.)
  - Használt rendszerek, azok interfészei, összeköttetései
- A naplók eljuttatás módjának felmérése
  - Kollektorok, feldolgozók
  - Hardver, operációs rendszer, adatbázis, alkalmazás log
  - Flow adatok bekötése? Virtuális LAN bekötése?
- A naplók felmérése
  - Részletesség (audit naplók)
  - Meglévő, szükséges parserek



Láthatóság (Use-casek)

- Use-case-ek
  - Mitre Att&ck keretrendszer alapján 50-60 use-case
  - IT, ITB elvárások, ötletek, compliance
  - Üzleti oldal (pl. csalás megelőzés)
  - CTI feed-ek --» folyamatos fejlesztés
- Megvalósíthatóság
  - Szükséges adatok rendelkezésre állnak-e
  - Hogyan lehet biztosítani az adatokat.
- Szabályrendszerek, riasztások elkészítése
  - Treshold meghatározása
  - ”Pyramid of Pain” módszertan figyelembe vétele



Bevezetési stratégiák

KÜRT
INFORMÁCIÓMENEDZSMENT

Idősík

Bevezetési idősávok

Megvalósíthatósági dokumentum elfogadása

Felkészülési időszak (0-6 hónap)

Felsővezetői támogatás Magas szintű elvárások Személyek

Soft opening (6-12 hónap)

5/8 működés
Szerepkörök 50%+
CMDB, Ticketing
SIEM,SOAR

Operatív működés (12-18 hónap)

5/8 + készenlét
Szerepkörök 90%+
Előmeneteli rendszer
Marketing

Hatáselemzett működés (18+ hónap)

7/24 működés
Elvárásoknak való megfelelés
Automatizmusok
Képességek kiterjesztése

Bevezetési stratégiák (folyt.)

Nincs elég pénz, státusz

- ”Mini SOC” koncepció
  - Ellenérvek: hamis biztonságérzet, támadóknál nincs munkaidő...
  - A bevezetés ugyanaz, a tanácsadó szerepe nagyobb
  - Nincs SOC manager, csupán néhány „L1 analyst”
  - L2 analyst külsős (pl. MSSP)
  - Első sikerek: kisebb félrekonfigurálások, támadások észlelése: Jobb alkupozíció
- MSSP (Managed Security Service Provider) alkalmazása
  - Bevezetés itt is kell
  - Felelősség kérdése, adatok biztonsága
  - Szolgáltatás minősége ellenőrizendő

Bevezetési stratégiák (folyt.)

Nincs elég pénz, státusz, érettség, igény

- Seconical
  - Cél: biztonság növelése, (kiszervezett) IT ellenőrzése, megfelelés biztosítása
  - Egyszerűen, szaktudás nélkül használható
  - Jóval rövidebb bevezetési idő
  - Real-time monitoring
  - Riasztások generálása
  - Automatikusan elemzi a beérkező logokat
  - Vezetők számára is érthető riportokat generál
  - Hosszú távon biztonságosan, visszakereshetően tárolja a logokat
  - Átfogó képet biztosít a biztonság helyzetéről, az IT működéséről
  - IBTV megfelelést segíti

Köszönöm a figyelmet!