ALEF

3 velké výzvy OT bezpečnosti a jak se s nimi vypořádat

Jan Kopřiva

jan.kopriva@alef.com

Když se řekne průmyslový a specifický systém

- Vybrané moderní systémy v důsledku trendu IT/OT konvergence relativně blízké IT
- Časté však historické sítě a systémy, nebo systémy podporující historické standardy
  - Velmi dlouhý životní cyklus
  - Často proprietární, uzavřená řešení
- Omezená možnost změn v chráněných prostředích

→ Specifická prostředí musí být vždy považována za zranitelná

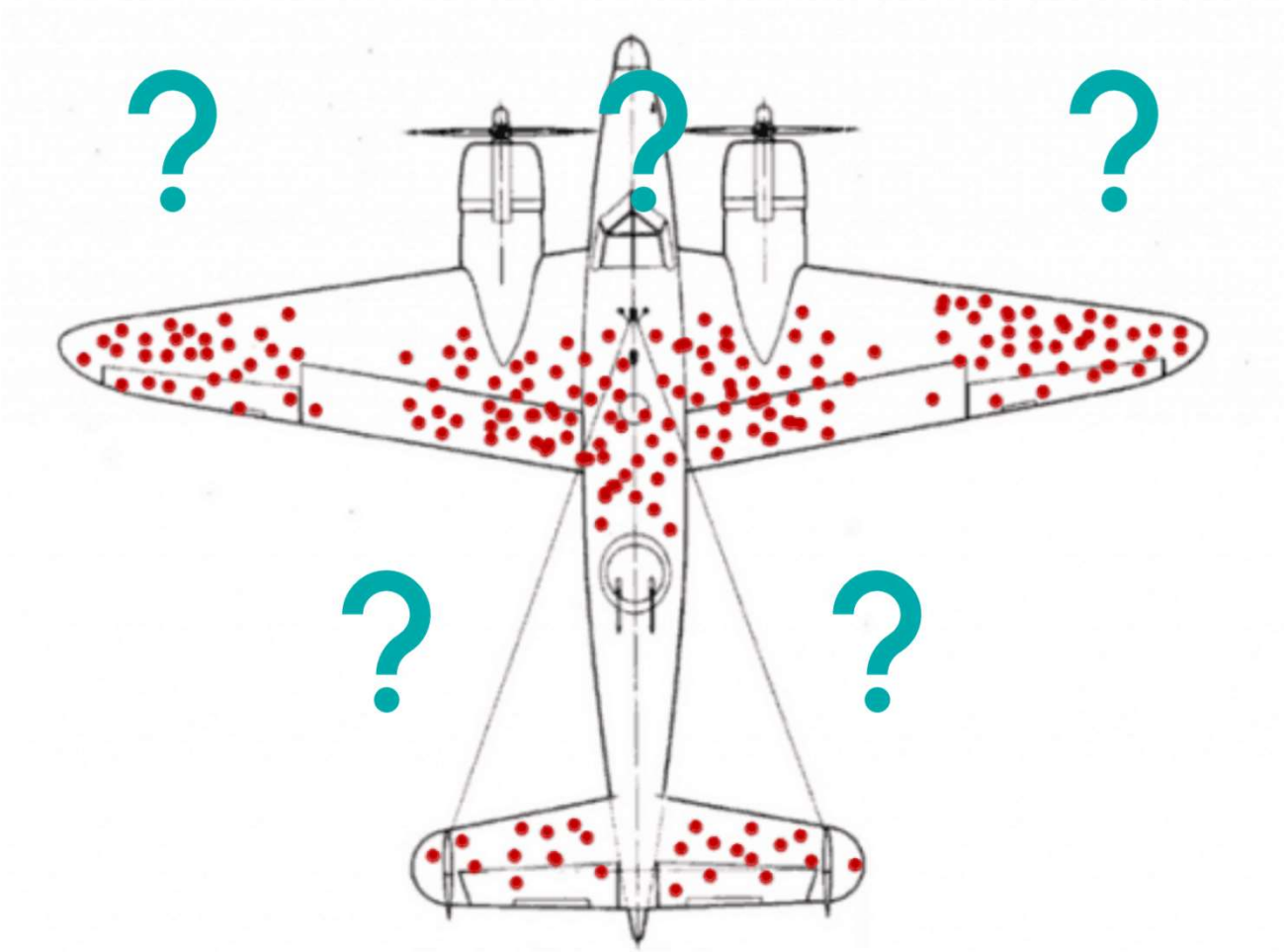
ALEF

Jak zabezpečit zranitelné prostředí?

- Závisí na definici bezpečnosti?
  - CIA
  - Parkerovská hexáda
  - CI3A
- Ne
  - Je-li určitý systém („systém systémů“) zranitelný specifickou/škodlivou interakcí, pak jeho zabezpečení principiálně musí záviset na omezení interakčního povrchu

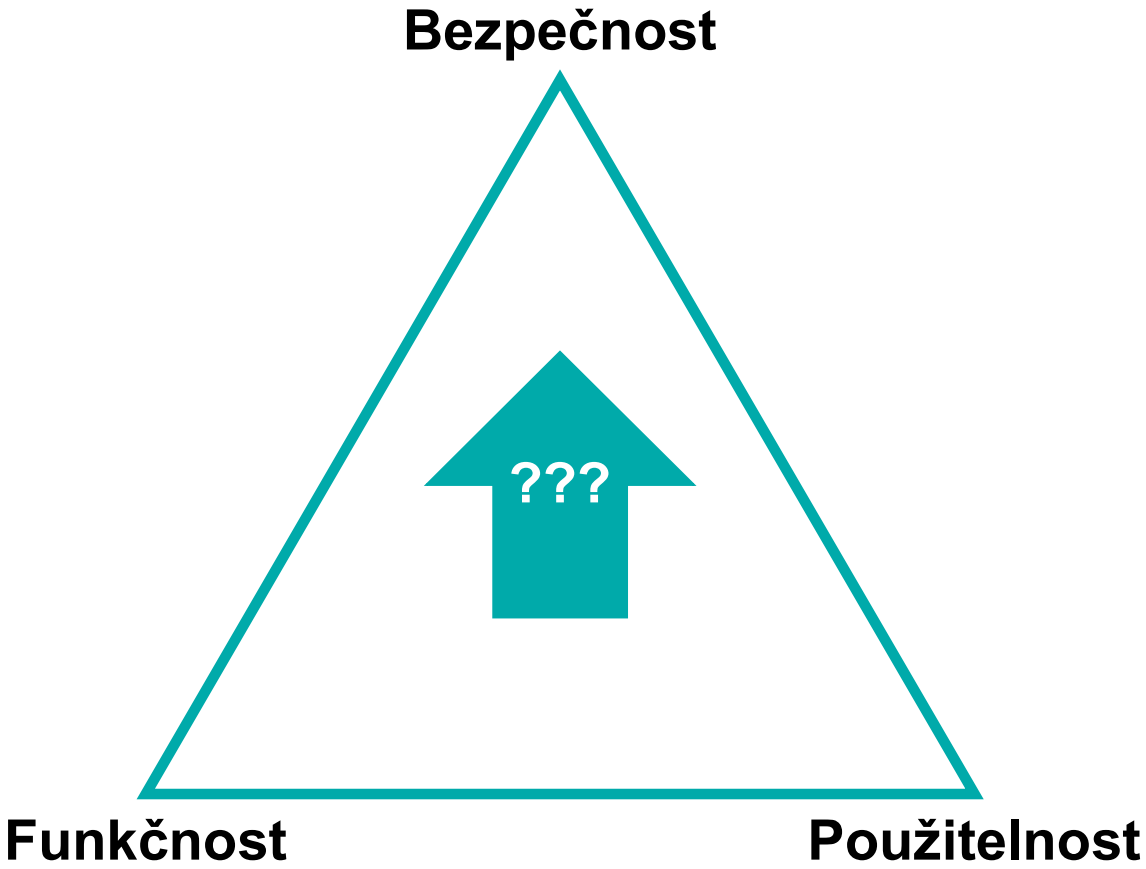
ALEF

Určování interakčního povrchu



ALEF

Minimalizace interakčního povrchu



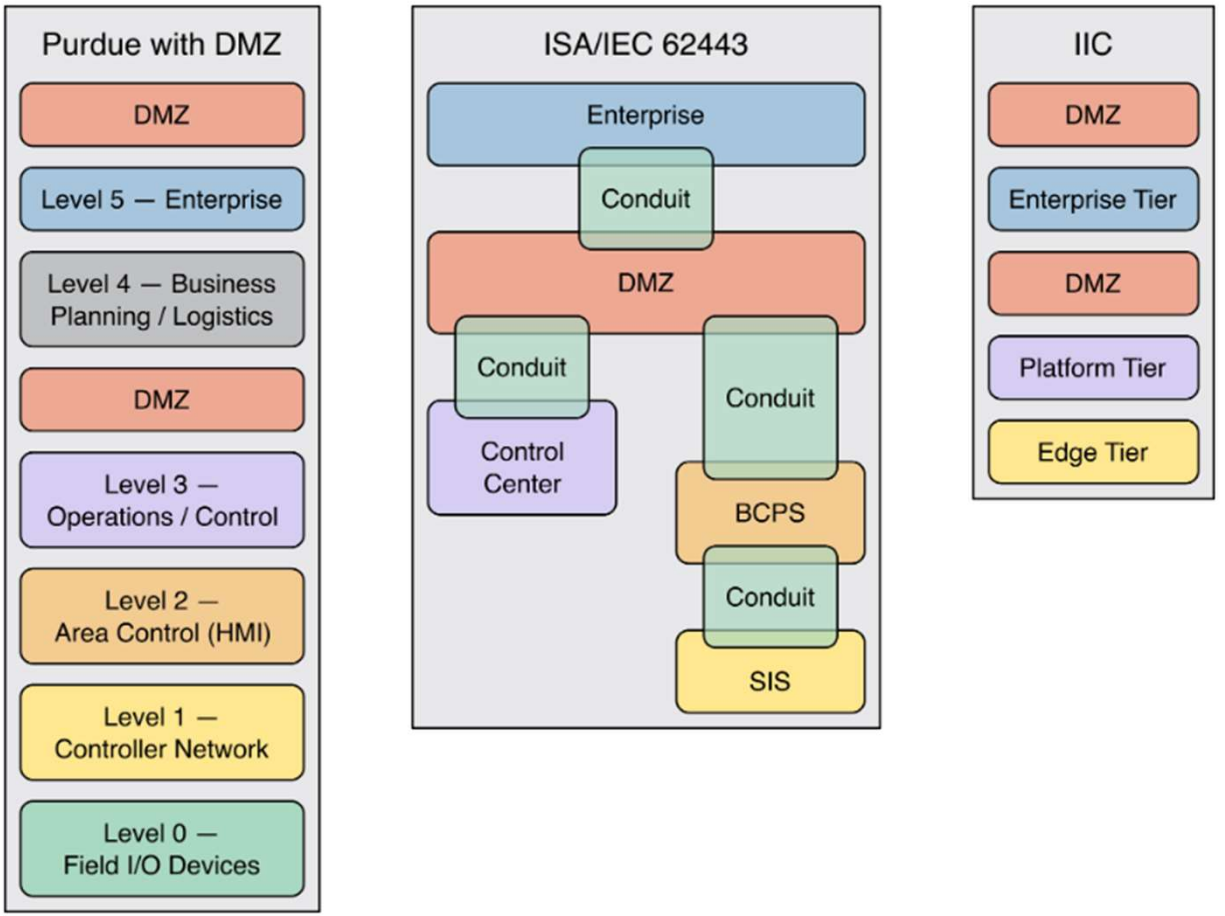
ALEF

3 velké výzvy OT bezpečnosti

- Bezpečné řízení přístupu zaměřené na minimalizaci interakčního povrchu
- Smysluplné řízení zranitelností umožňující maximálně zabezpečit nezbytný interakční povrch
- Efektivní zvládání bezpečnostních incidentů, kterým se principiálně není možné plně vyhnout

ALEF

Řízení přístupu ke specifickým prostředím



ALEF

Zdroj: NIST

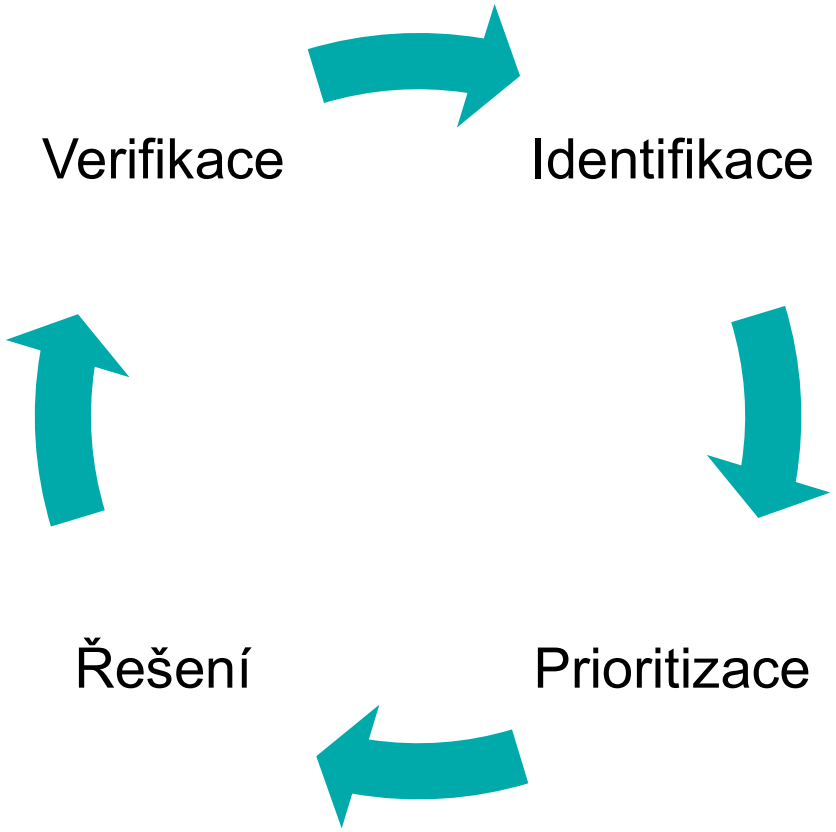
Řízení přístupu ke specifickým prostředím

- Datová komunikace dovnitř/z prostředí pouze přes DMZ
  - Informace ze specifického prostředí přes „hop“ v DMZ
  - Přenos dat do specifického prostředí pouze přes řízený kanál v DMZ
    - Možnost analýzy všech přenášených dat (updaty, nástroje, …)
- Řízený fyzický i vzdálený přístup s možností připojení pouze specificky nakonfigurovaných zařízení, vzdálený přístup navíc pouze přes „jump servery“

→ Komplikované, avšak principiálně jediné bezpečné řešení

ALEF

Základní životní cyklus řízení zranitelností



ALEF

Řízení zranitelností

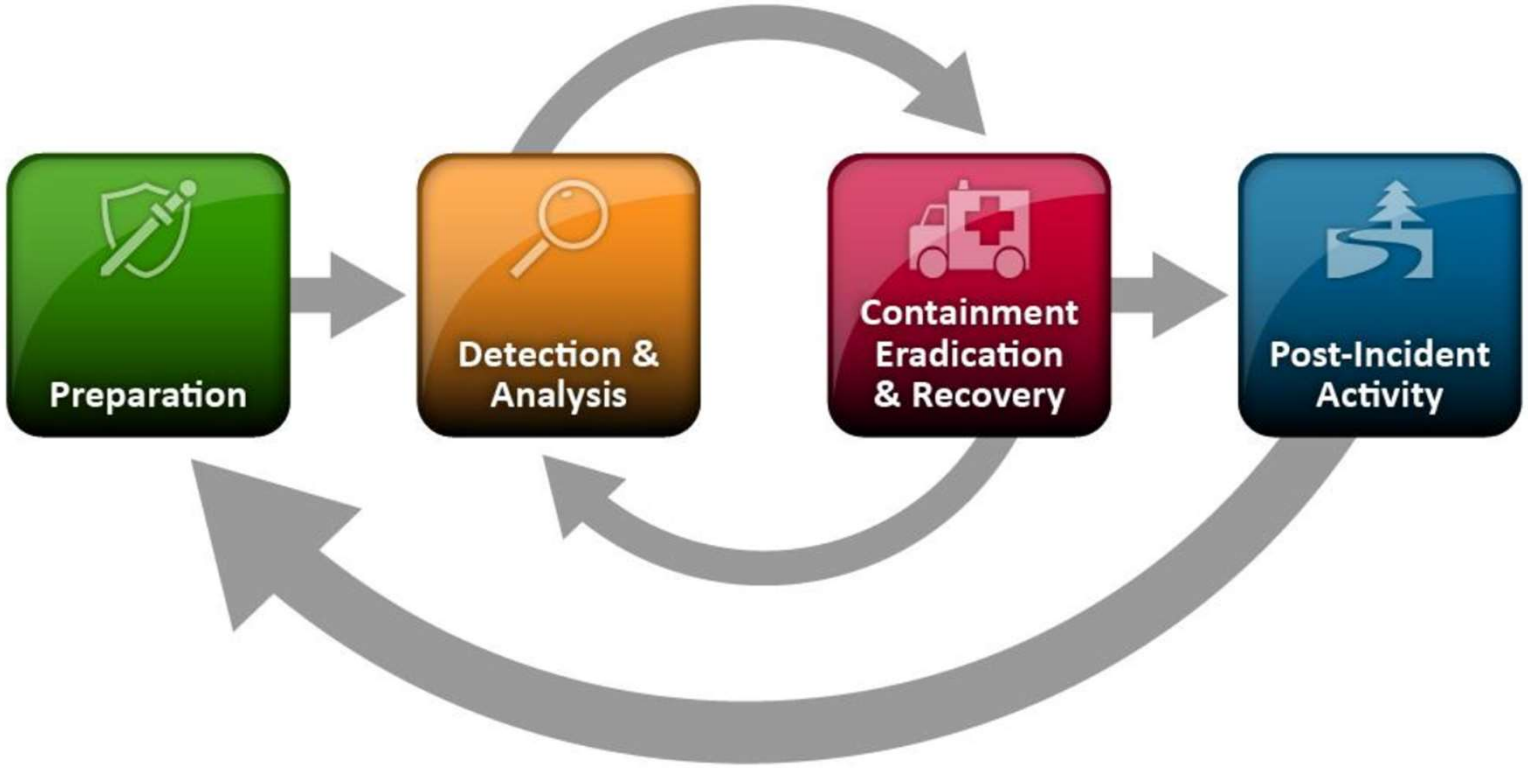
- Netriviální i v dobře řízených IT prostředích
- Ve specifických prostředích vyvstávají dodatečné problémy
  - Omezené informace o existenci zranitelností
  - Omezená dostupnost záplat
  - Omezené možnosti detekce zranitelných systémů
  - Omezené možnosti záplatování

ALEF

Řízení zranitelností

- Záplaty obvykle možné pravidelně aplikovat na IT prvky, na specifická zařízení jen zřídka
  - Vhodné standardizovat podmínky a postupy
- Defense in depth je obecně dobrý koncept
  - Záplaty jsou jen jednou „obrannou vrstvou“, a tu musíme ve specifických prostředích někdy oželet
    - K dispozici zpravidla kompenzační mechanismy a opatření
      - Zejména řízení interakčního povrchu (ACL, allow-listing, …)

Zvládání KBI (nejen) ve specifických prostředích



ALEF

Zdroj: NIST

Zvládání KBI ve specifických prostředích

- Podmínkou pro efektivní zvládání KBI při minimalizaci dopadů je jejich včasná detekce
- Bezpečnostní monitoring v **dobře řízených** (nejen) specifických prostředích je principiálně jednodušší než v dynamicky se měnících sítích
  - V případě dobře řízeného interakčního povrchu detekce potenciálně škodlivého/nebezpečného chování zjednodušená

ALEF

Zvládání KBI ve specifických prostředích

- „Žádný plán nepřežije střet s nepřítelem“
  - Potvrzuje i Mike Tyson se svými zkušenostmi
- Realistická cvičení a testy reakce na KBI mohou rizika spojená se vznikem neočekávaných situací citelně snížit
- Smysluplné mohou být vedle table top cvičení i vhodně nastavené purple team testy

ALEF

Zvládání KBI ve specifických prostředích

- Vybrané koncepty aktivní obrany velmi vhodné pro specifická prostředí
  - Zejména možnost dynamického řízení interakčního povrchu může citelně pomoci v případě masivní kompromitace
- Vhodné předem jednoznačně stanovit možnosti a podmínky pro izolaci prostředí/přechod do „ostrovního režimu“

ALEF

Pár slov na závěr

- Zranitelnosti ve specifických (OT/ICS, zdravotnických apod.) prostředích a systémech nelze principiálně řídit stejně jako v IT
  - Specifická prostředí budou vždy nezbytně „zranitelná“
- (Nejen) zranitelnosti je principiálně možné mitigovat efektivním řízením interakčního povrchu
  - Nezbytné citelné omezení přístupu
  - Řízený, deterministický interakční povrch a řízený formát interakce citelně napomáhají bezpečnostnímu monitoringu a detekci incidentů

ALEF

ALEF

Děkuji Vám za pozornost