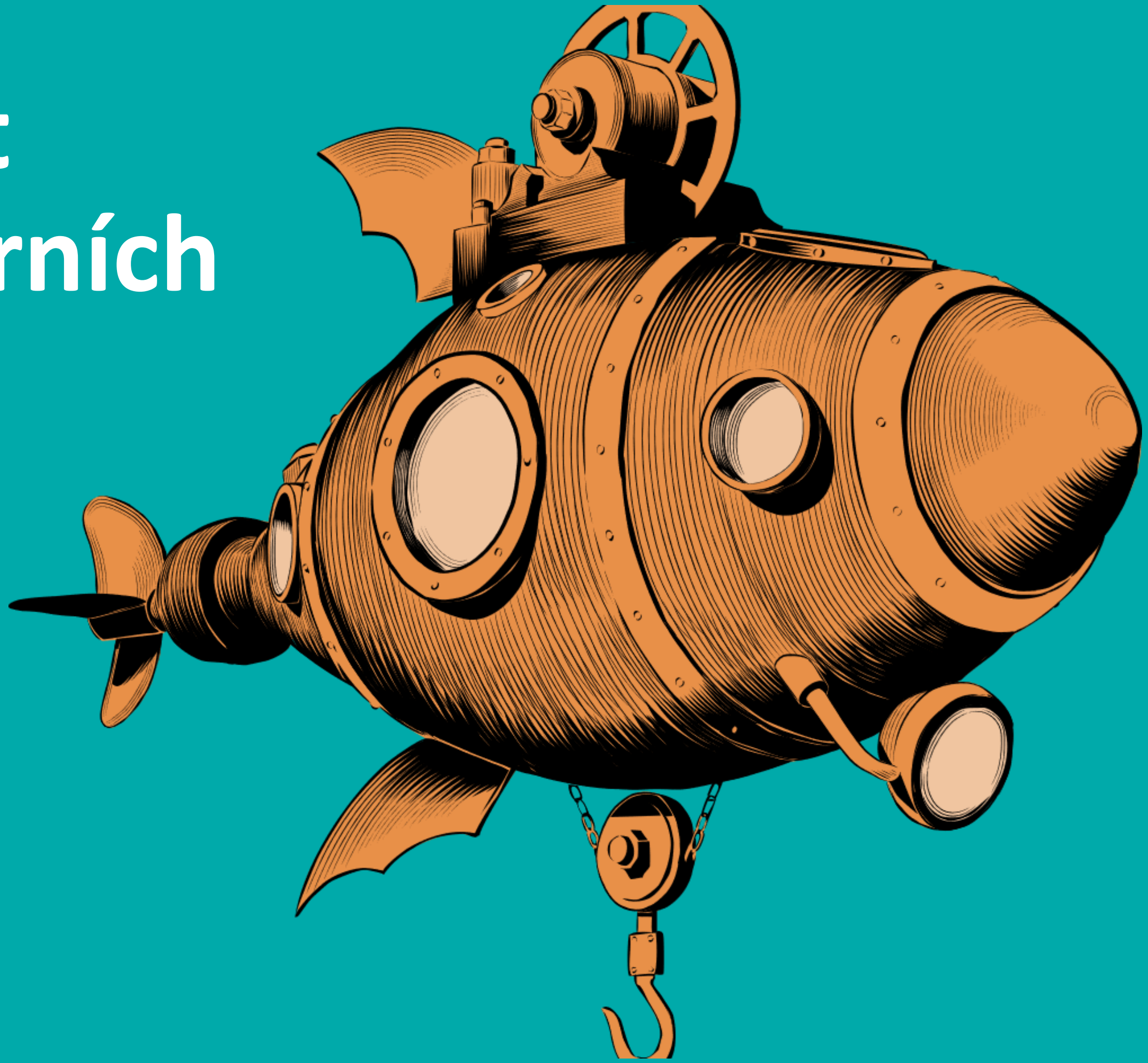
ALEF

Kybernetická bezpečnost medicínských a laboratorních systémů



23. 2. 2023

Tomáš Poledno
Senior Security Consultant
Security Architect

Agenda

- Představení
- Kybernetická bezpečnost jako celek
- Zdroje, procesy
- Technické řešení

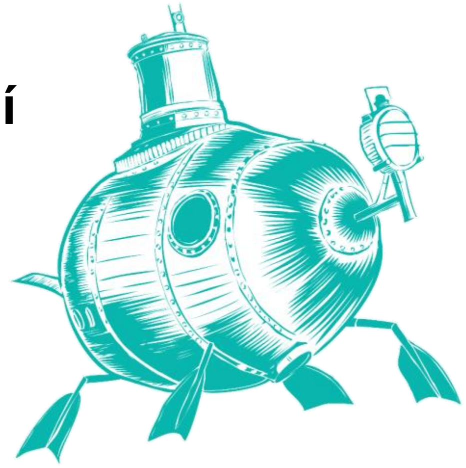
Legislativní rámce

Zákon 181 / 2014 Sb. a jeho prováděcí vyhláška 82 / 2018 Sb.

o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Evropská směrnice NIS2

směrnici Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2 a její následná transpozice do české legislativy



ALEF

Strategické cíle MZ ČR

Soustava strategických cílů

- GC1 Zavedení řízení bezpečnosti informací jako mandatorního procesu všech poskytovatelů zdravotních služeb
- GC2 Zajištění minimálního technického standardu kybernetické bezpečnosti
- GC3 Zvyšování bezpečnostního povědomí
- GC4 Kybernetická bezpečnost elektronického zdravotnictví
- GC5 Kybernetická bezpečnost zdravotnických prostředků

Fungující ISMS

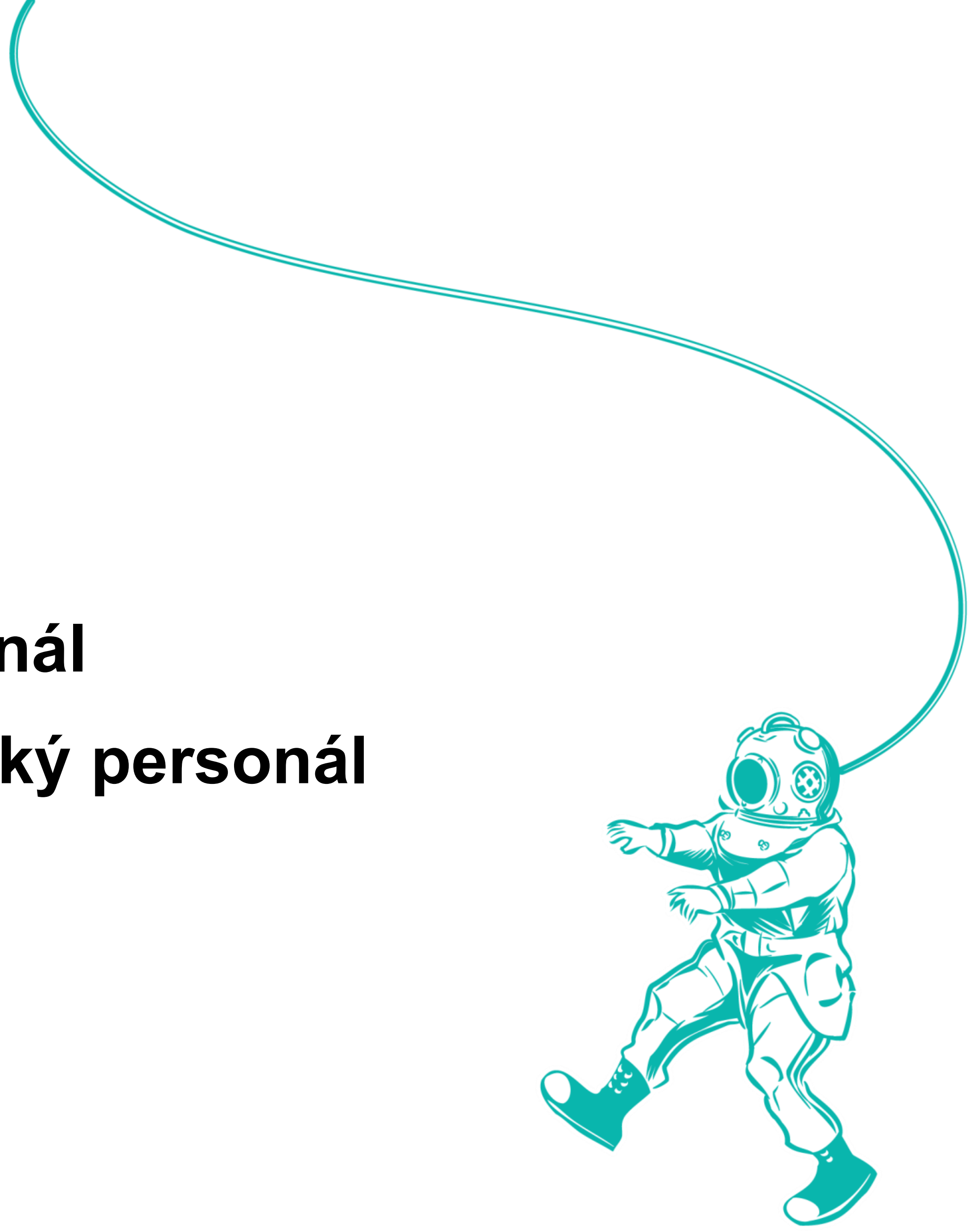
Lidé

Procesy
a
dokumentace

Technické
prostředky

Uživatelské role

- Obsluhující lékařský personál
- Personál laboratoří
- Vyhodnocující lékařský personál
- Ostatní nelékařský zdravotnický personál
- Medicínští inženýři
- Management



Role a úlohy ICT

- ICT administrátoři a síťoví správci
  - Implementace (Segmentace, integrace)
  - Patchování
  - Zálohování
  - Provozní dokumentace
  - DR plány

Role pracovníků kybernetické bezpečnosti

Bezpečnostní specialisté

- Procesy
- Bezpečnostní dokumentace
- Přístupová oprávnění
- Definice bezpečnostních procesů pro celý životní cyklus medicínských a laboratorních systémů (onboarding zařízení, údržba, zálohování, testování, …)

SOC

- Proaktivní dohled
- Auditing
- SOC

ALEF

Dodavatelé

- HLD
- LLD
- Implementace
- Provozně bezpečnostní dokumentace
- Servis a provozní podpora

Dokumentace

Provozní dokumentace

- Uživatelské příručky
- Administrátorské postupy
- Plány záloh a DRP

Administrativní dokumentace

- Dodavatelské smlouvy
- Auditní zprávy
- Zprávy z testování

Bezpečnostní dokumentace

- Bezpečnostní politiky, směrnice, …
- Evidence aktiv
- Analýza rizik
- Plán zvládání rizik

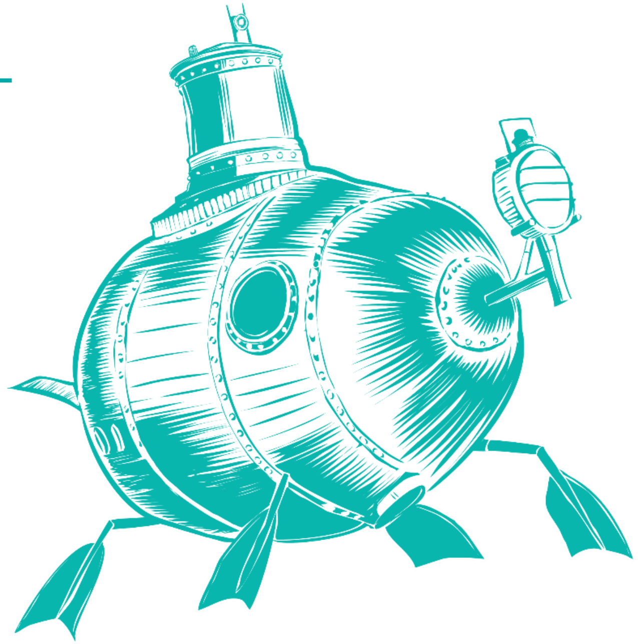
Bezpečnostní procesy

- Řízení změn
- Řízení zranitelností
- Analýza rizik
- SOC Procesy
- Onboarding procesy

Onboarding zdravotnických systémů

- Vedoucí lékaři a vedoucí laboratoři
- Management nemocnice
- Medicínští inženýři

- Správci ICT
- Bezpečnostní specialisté



Technické prostředky

- **Nástroj pro identifikaci, kategorizaci a ochranu připojených síťových zařízení s důrazem na zdravotnické systémy**

- **Nepřetržitá detekce a online scan vulnerabilit a ověřování souladu s bezpečnostní praxí**

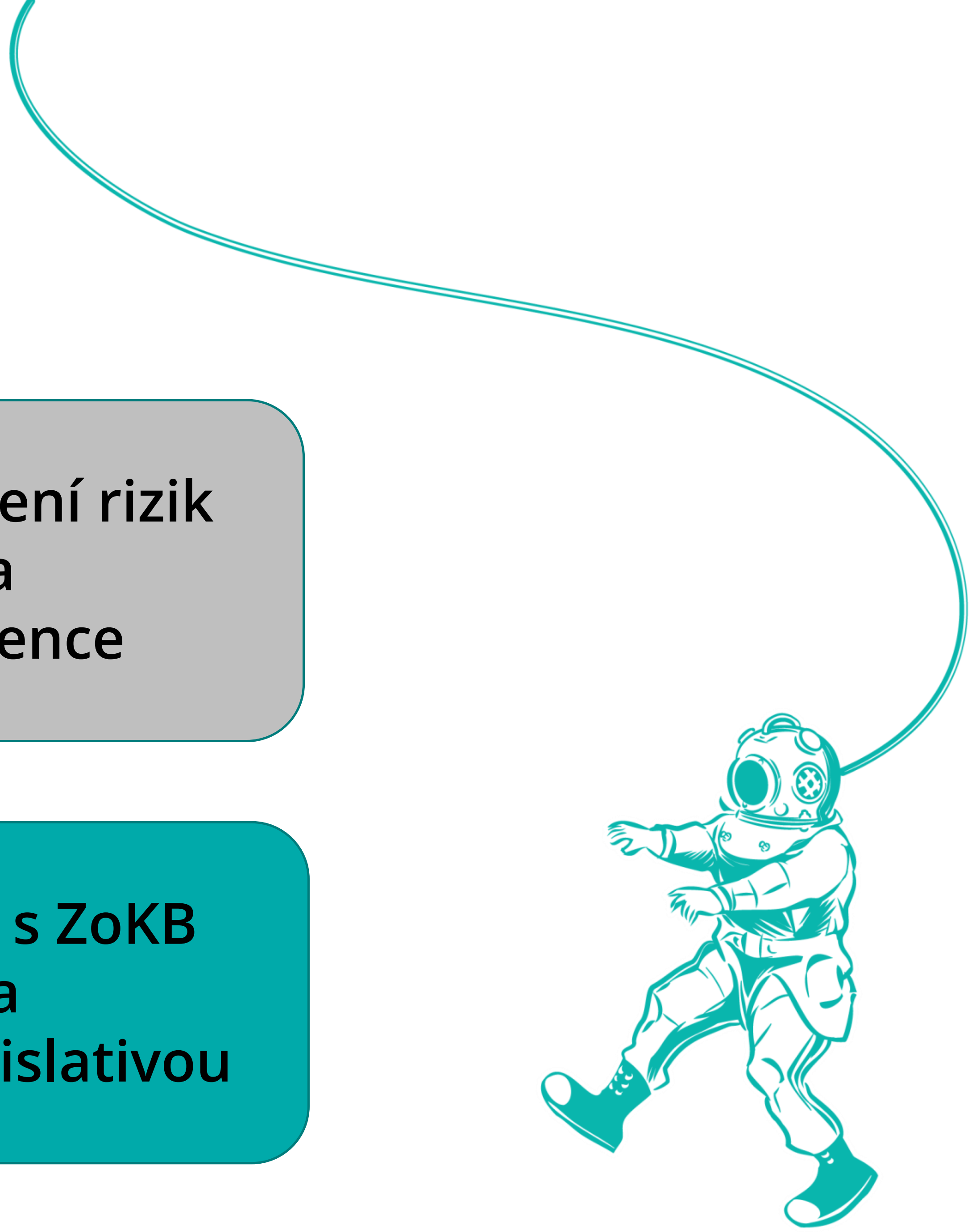
Motivace

Inventarizace a sledování zařízení

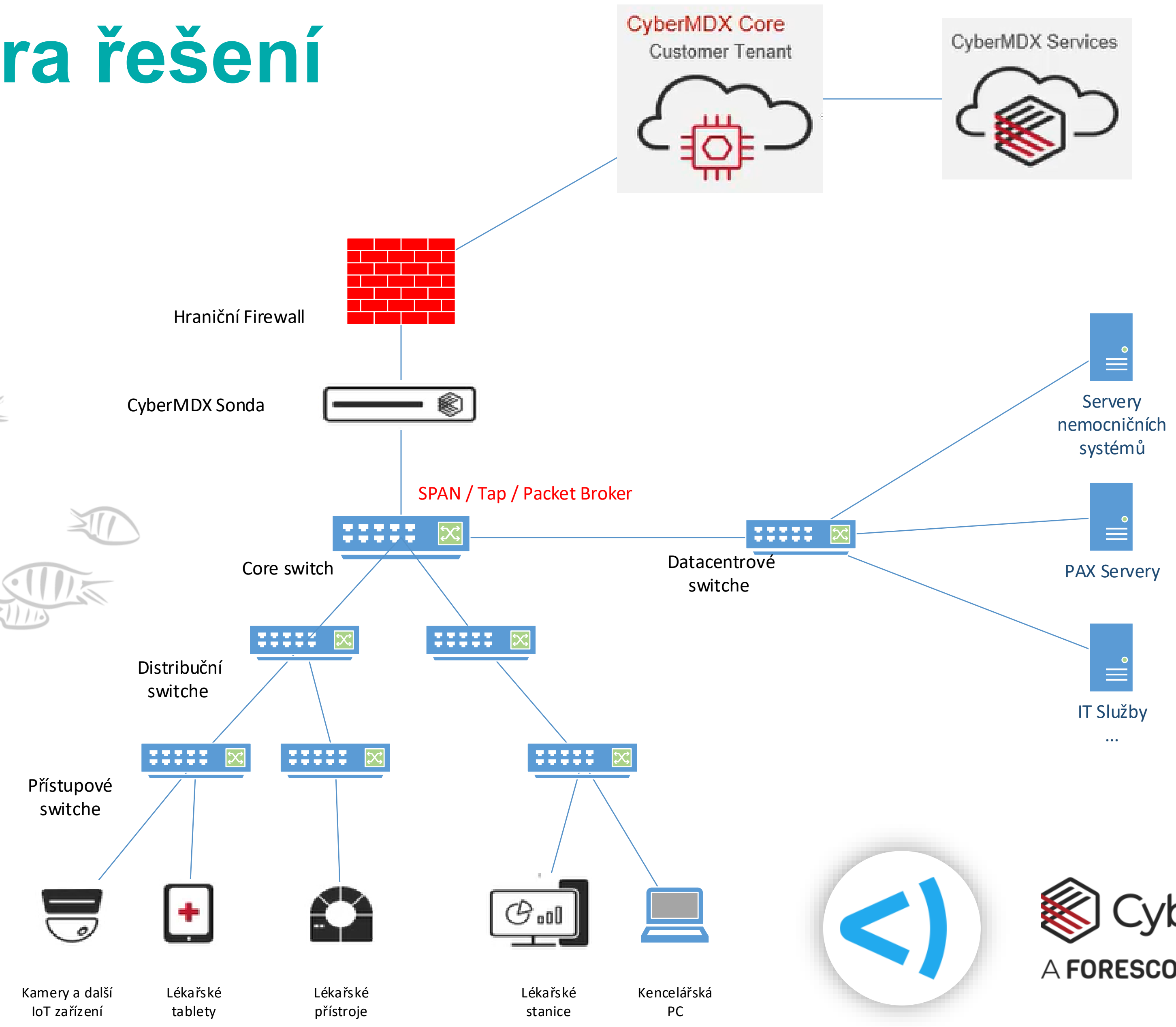
Hodnocení rizik
a
prevence

Detekce zranitelností a reaktivní opatření

Soulad s ZoKB
a
další legislativou



Architektura řešení



CyberMDX
A FORESCOUT COMPANY

ALEF

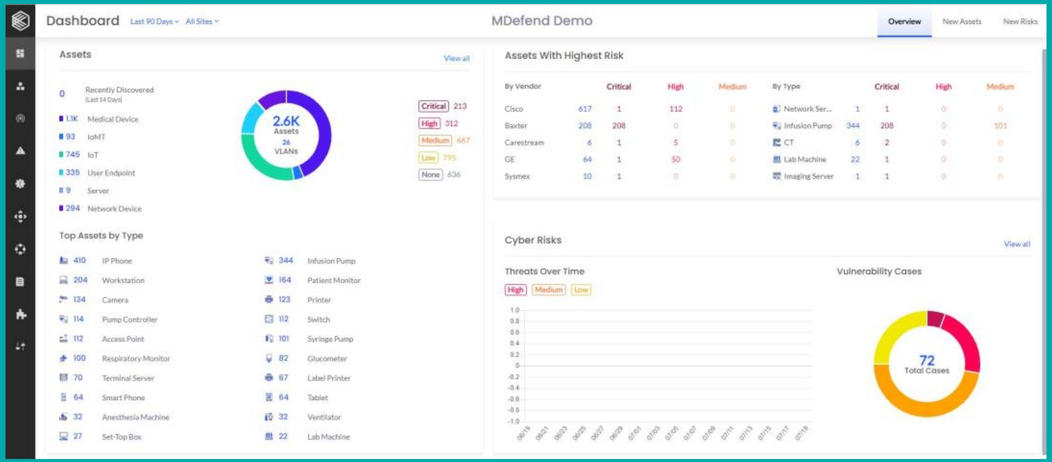
Architektura řešení

- Pasivní systém napojen na SPAN, Tap, …
- HW, nebo virtuální sondy
- Škálovatelnost – více lokalit, jedna správa
- Vyhodnocení pomocí AI v cloudové platformě i on-prem

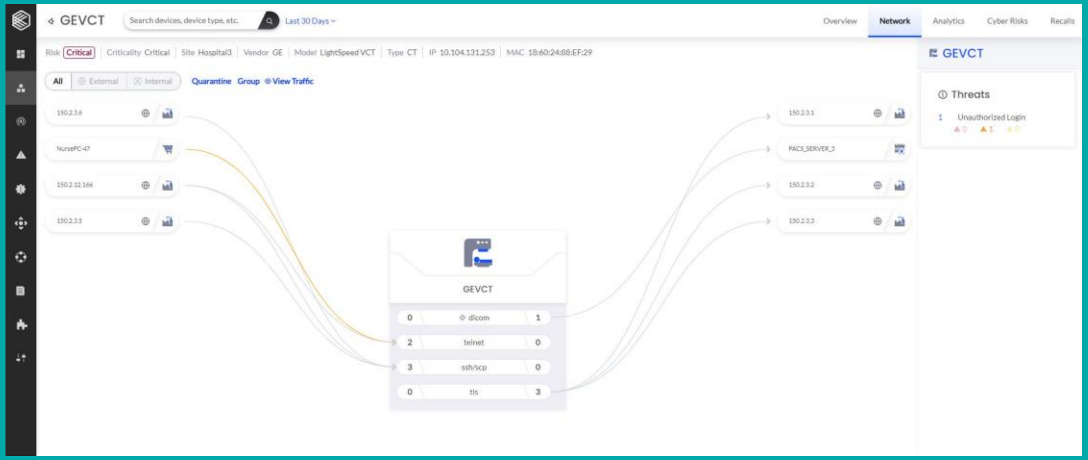
CyberMDX
A FORESCOUT COMPANY

Klíčové funkcionality

- Monitoring připojených zařízení
- Detekce zranitelností a podpora v řešení nápravných opatření
- Dynamická aplikace pravidel reagující na znalost prostředí a protokolů

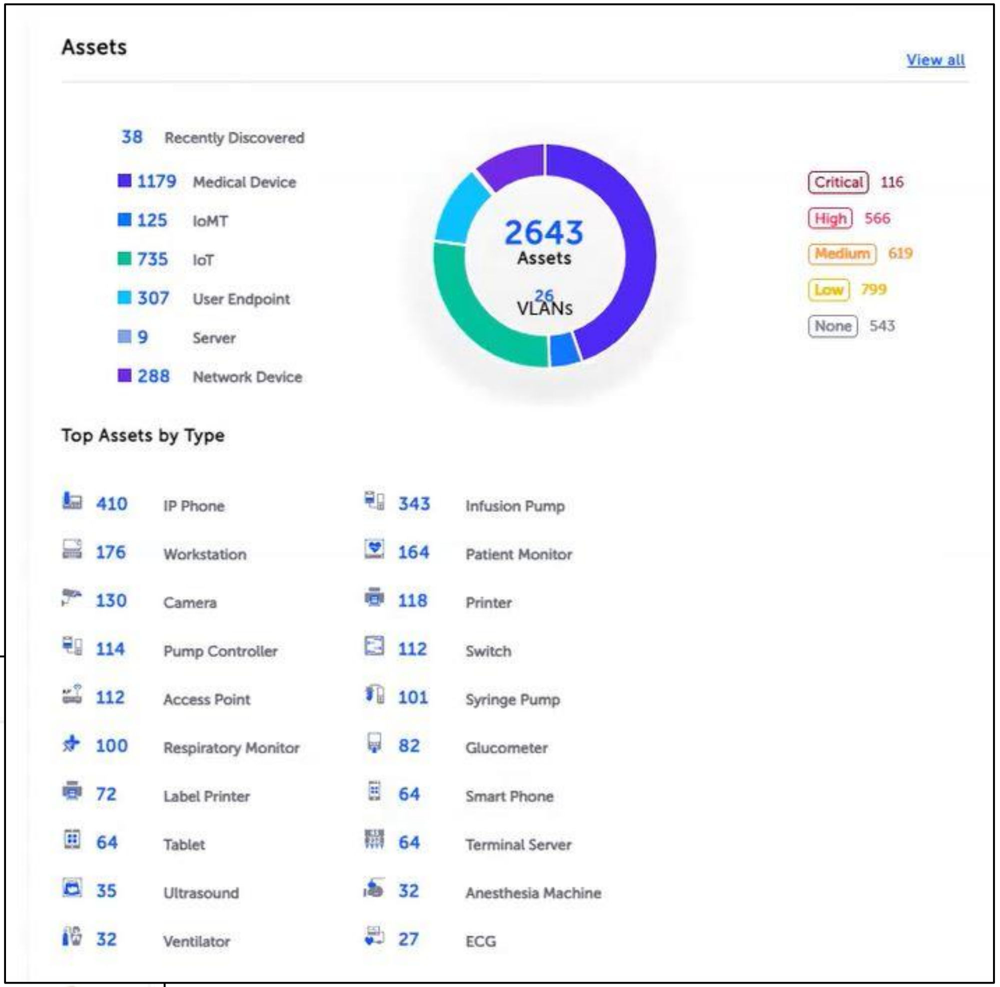


- Hodnocení rizik a prevence
- Zvýšení souladu s legislativními požadavky



Klíčové funkcionality

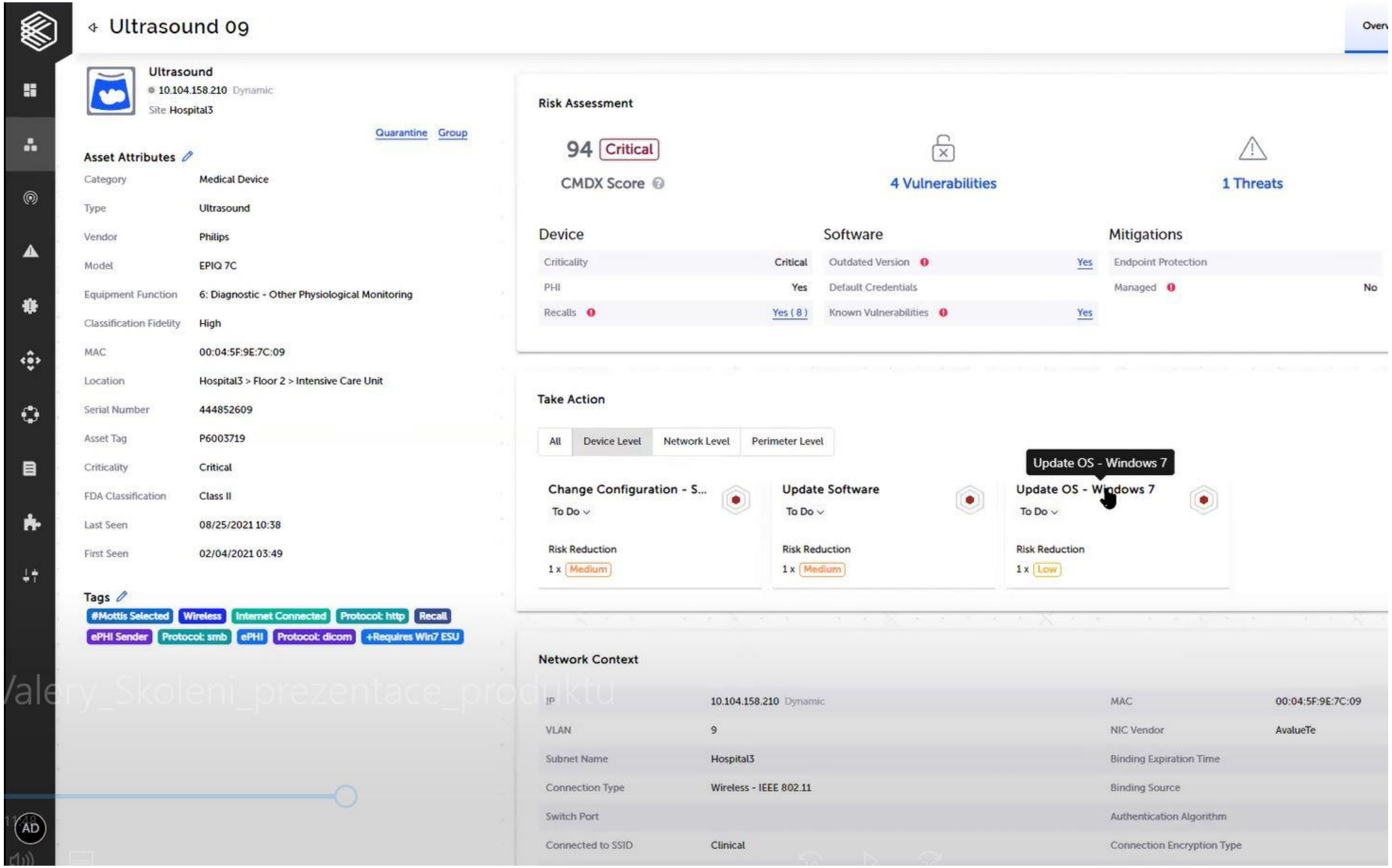
- Inventarizace
- Rozčlenění dle funkčních typů
- Dodržování standardů a dobré praxe
- Identifikace provozních problémů
- Přehled hrozeb a zranitelnosti




Assets With Highest Risk

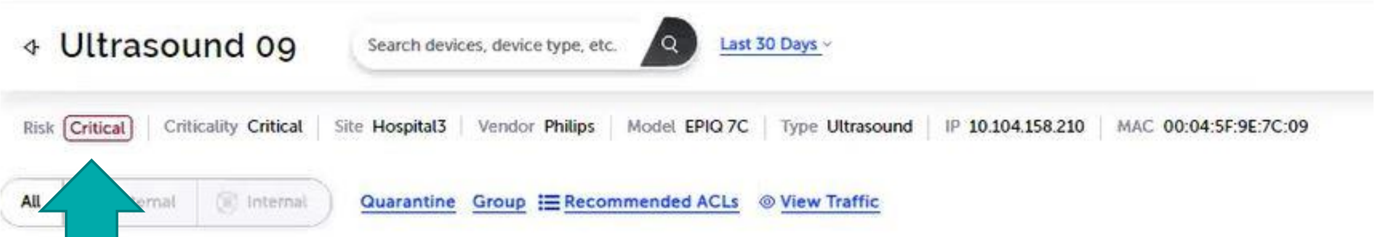
By Vendor		Critical	High	Medium	By Type		Critical	High
BD	429	114	0	203	Pump Controller	114	114	0
Philips	117	1	84	0	Ultrasound	35	1	19
GE	73	1	68	0	CT	11	1	0
Baxter	208	0	208	0	Infusion Pump	343	0	208
DigiBoard	32	0	32	0	Patient Monitor	164	0	132

Inventarizace aktiv

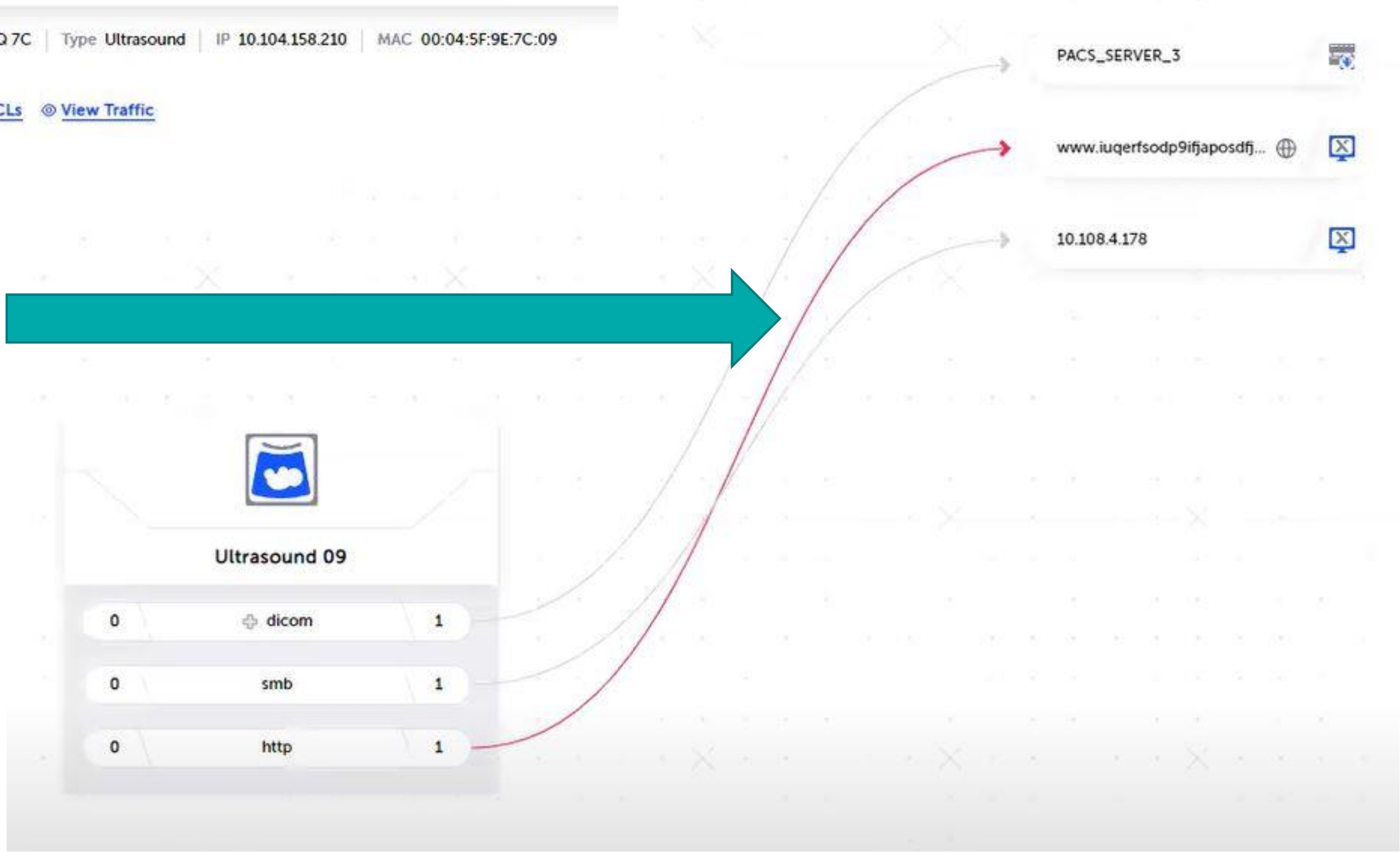


ALEF

Mapy komunikací

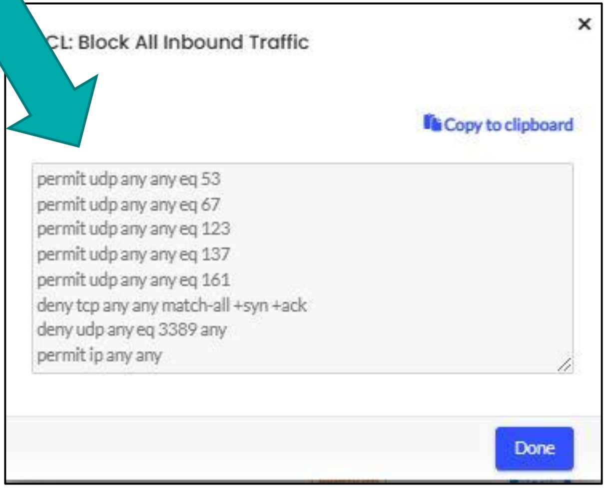


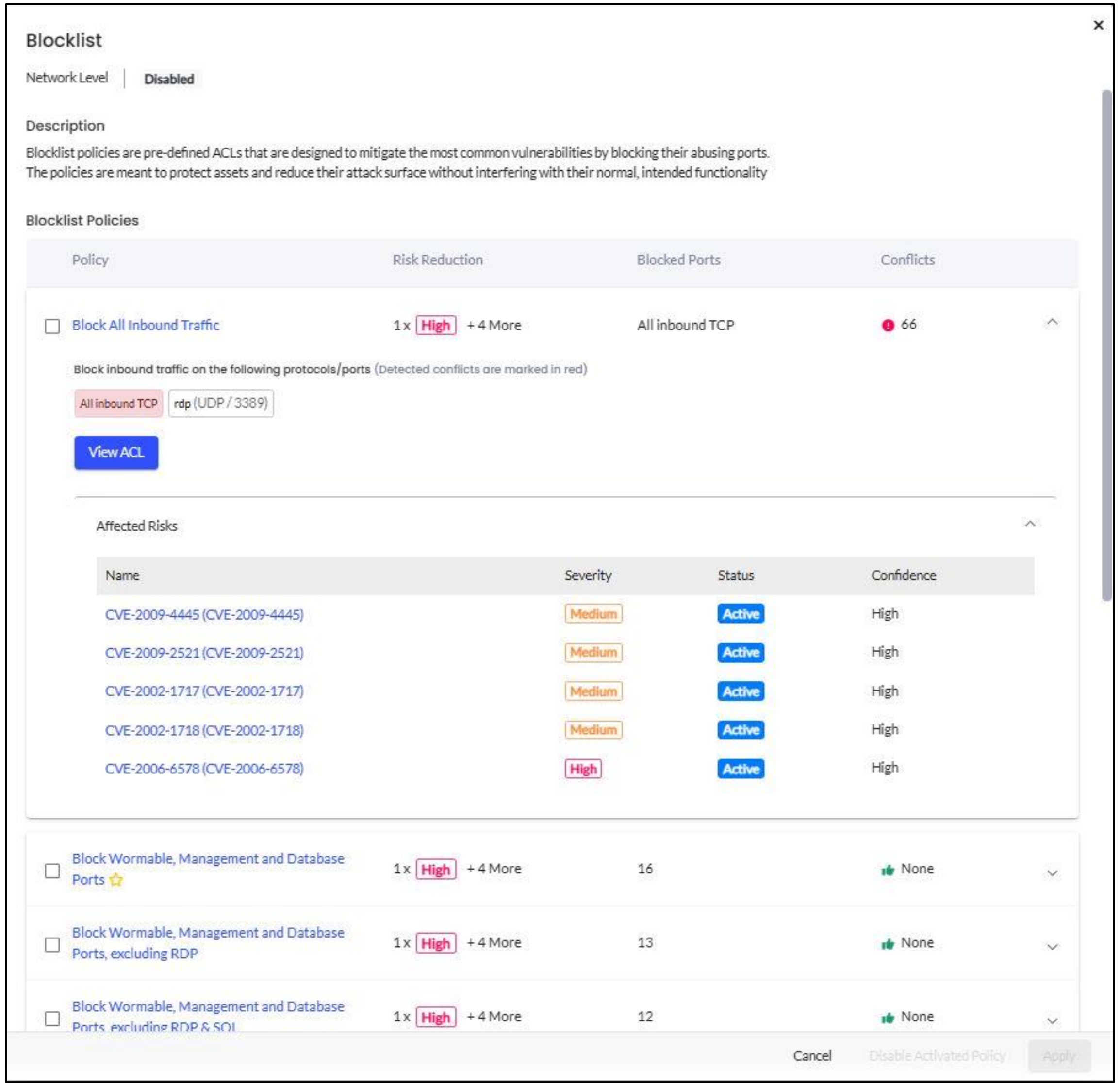
Upozornění na neočekávanou komunikaci



Interaktivní návrhy opatření

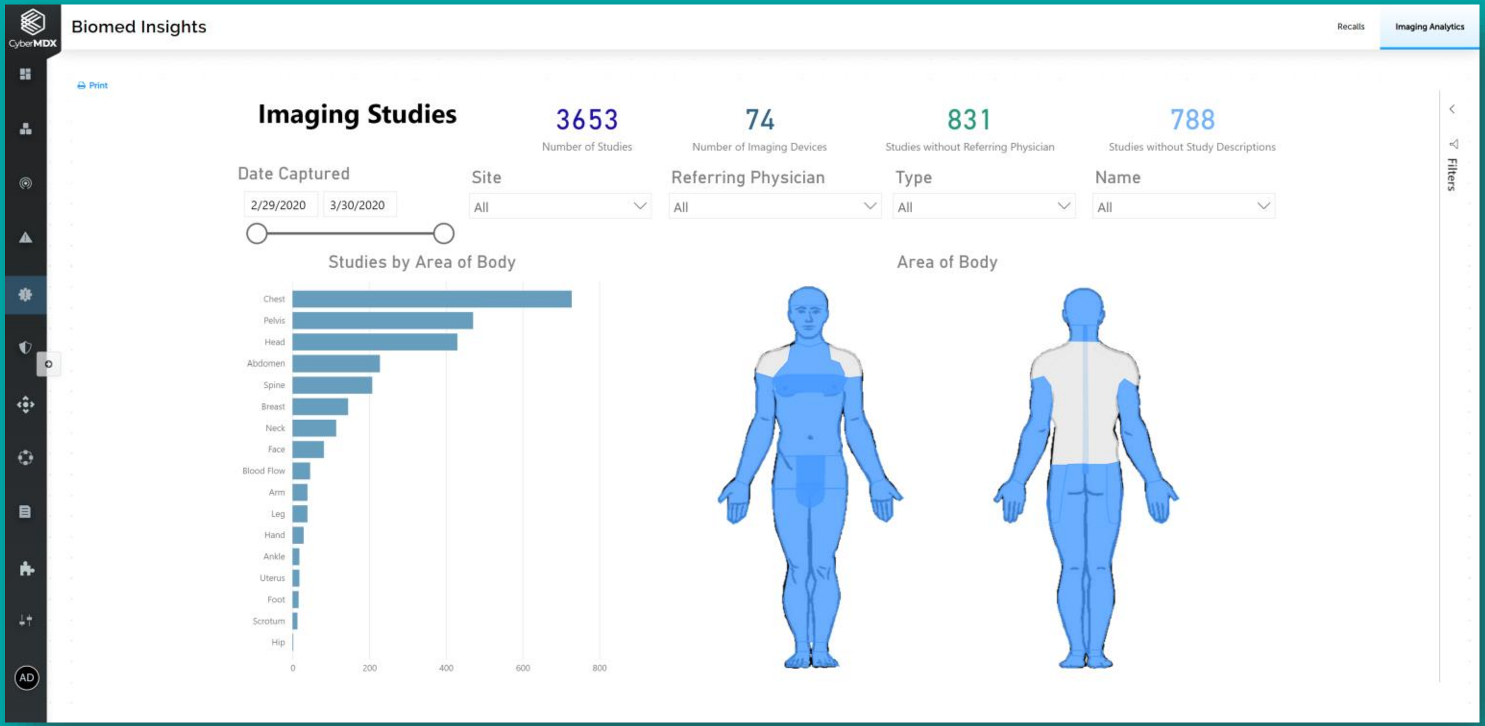
- **Návrh remediace až na úroveň ACL a firewallových pravidel**





Vytížení kapacit zdravotnických zařízení

- Přehledy využití
- Plánování servisu a údržby

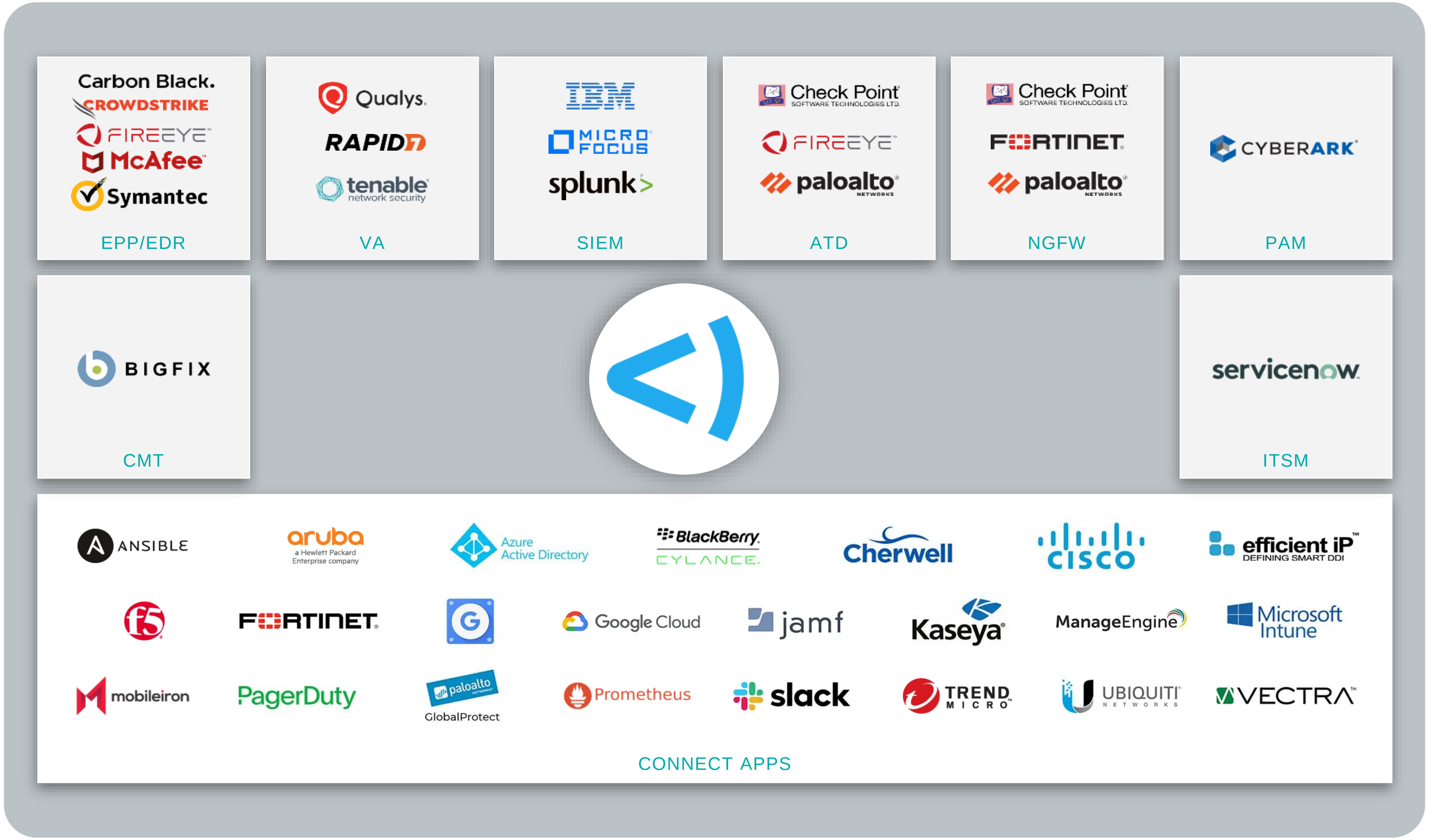


Komu je systém určen?

- ICT – technici a pracovníci provozních dohledů
- Informační bezpečnost a zaměstnanci bezpečnostních dohledů, SOC teamy
- Biomedicínští inženýři a pracovníci údržby zdravotnických zařízení a systémů
- Management nemocnice a vedení lékařské péče
- Pacienti

ALEF

Integrace


Carbon Black.
CROWDSTRIKE
FIREEYE
McAfee
Symantec
EPP/EDR
Qualys.
RAPID7
tenable network security
VA
IBM
MICRO FOCUS
splunk>
SIEM
Check Point SOFTWARE TECHNOLOGIES LTD.
FIREEYE
paloalto NETWORKS
ATD
Check Point SOFTWARE TECHNOLOGIES LTD.
FORTINET
paloalto NETWORKS
NGFW
CYBERARK
PAM
BIGFIX
CMT
servicenow
ITSM
ANSIBLE
aruba a Hewlett Packard Enterprise company
Azure Active Directory
BlackBerry CYLANCE
Cherwell
cisco
efficient iP DEFINING SMART DDI
f5
FORTINET
Google Cloud
jamf
Kaseya
ManageEngine
Microsoft Intune
mobileiron
PagerDuty
paloalto GlobalProtect
Prometheus
slack
TREND MICRO
UBIQUITI NETWORKS
VECTRA
CONNECT APPS

Co systém přináší?

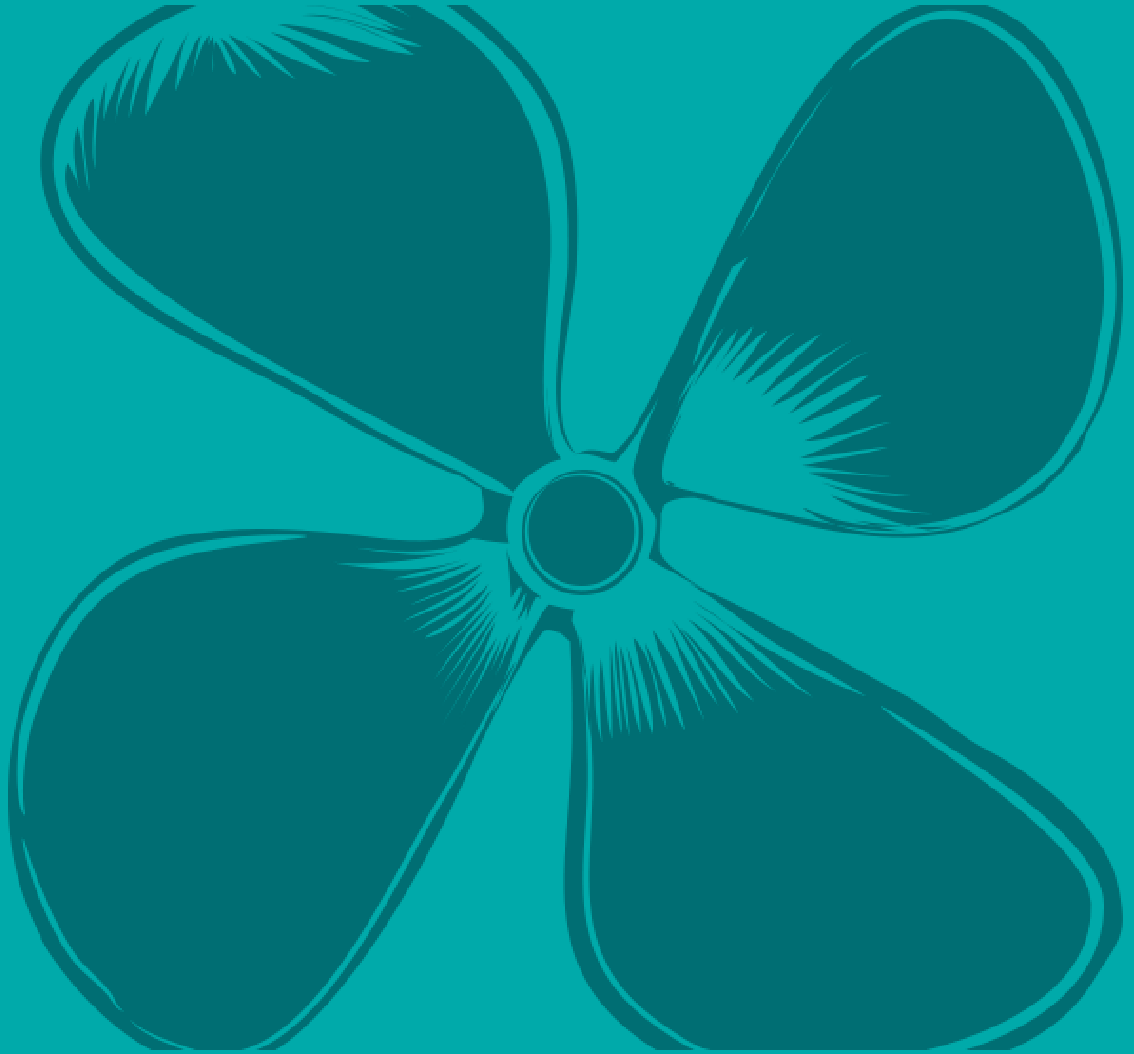
Zvýšení bezpečnosti a efektivnosti medicínských systémů

Ochrana dat pacientů

Ochrana před finančními ztrátami a ztrátou reputace

- **Prostor pro dotazy a diskuzi**

Děkuji za pozornost



Tomáš Poledno
tomas.poledno@alef.com
+420 724 815 483

CompTIA Secutity+
ISO27001 Lead Auditor
ISO27001 Lead Implementer