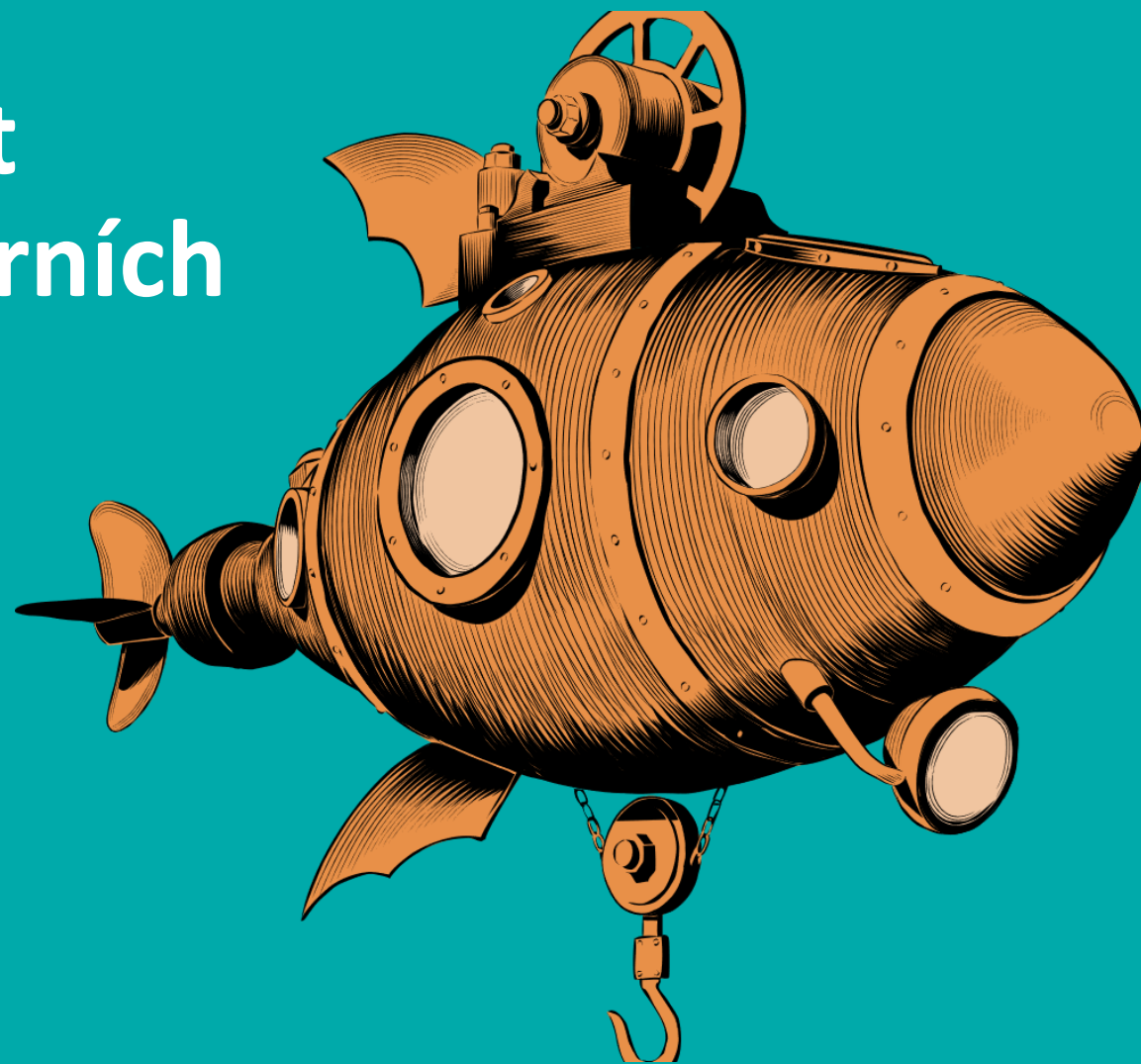


X ALEF

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



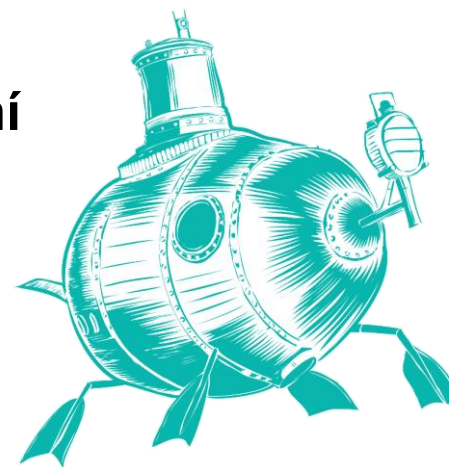
Legislativní rámce

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

směrnicí 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



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

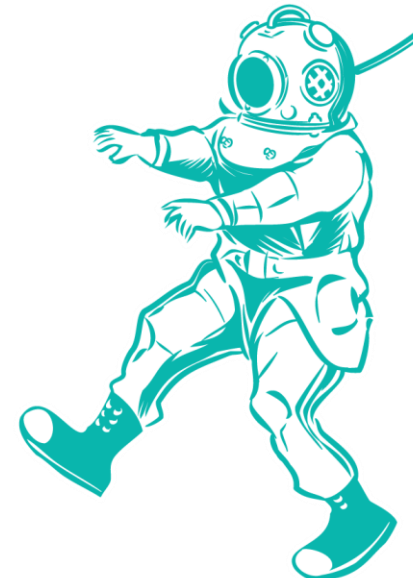
Lidé

Procesy
a
dokumentace

Technické
prostředky

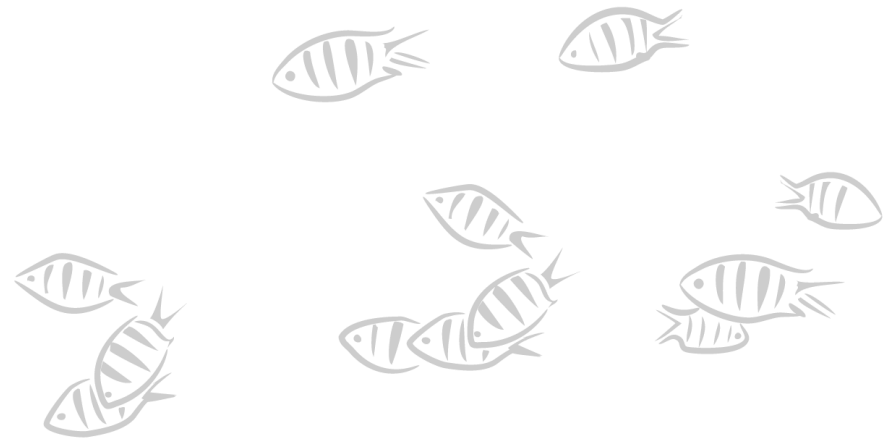
Uživatelské role

- **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



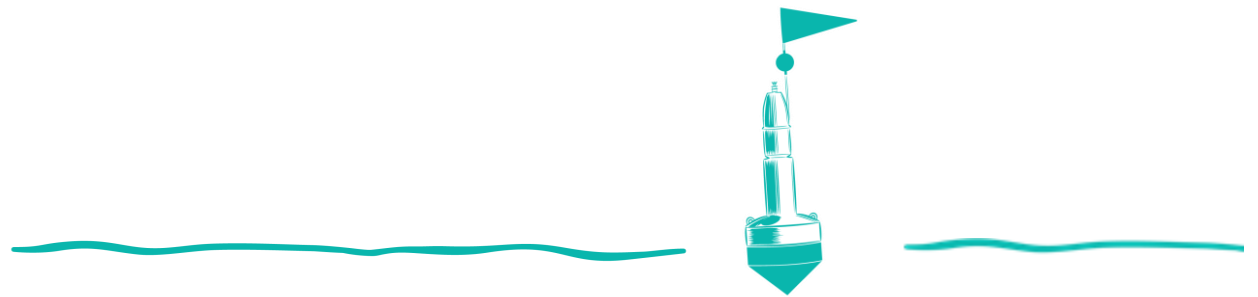
Role pracovníků kybernetické bezpečnosti

Bezpečnostní specialisté

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

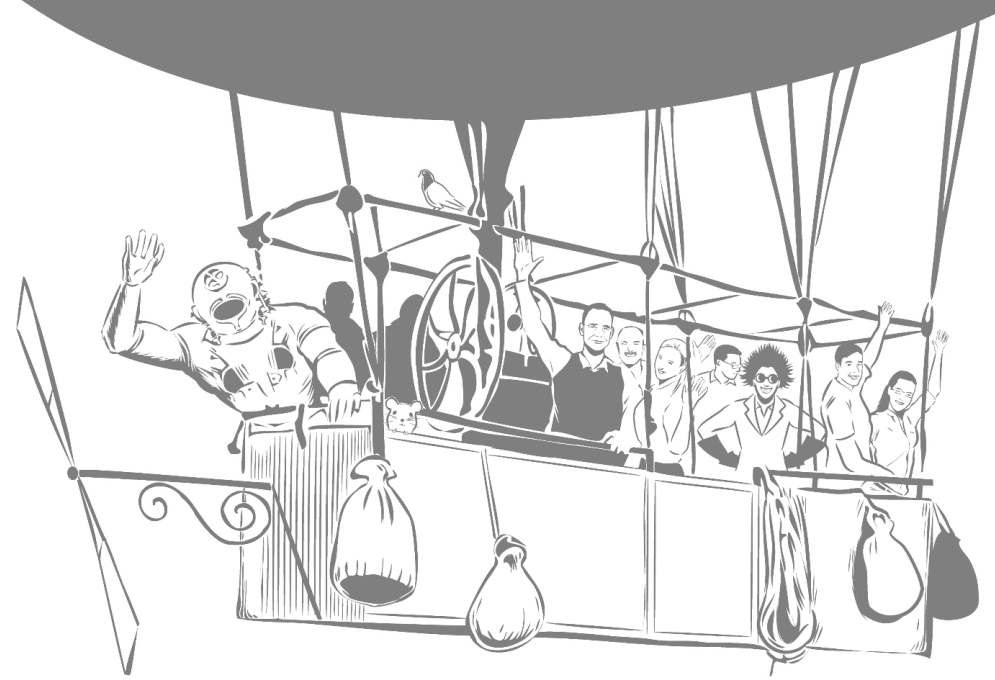
SOC

- Proaktivní dohled
- Auditing
- SOC



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 zvládnutí rizik

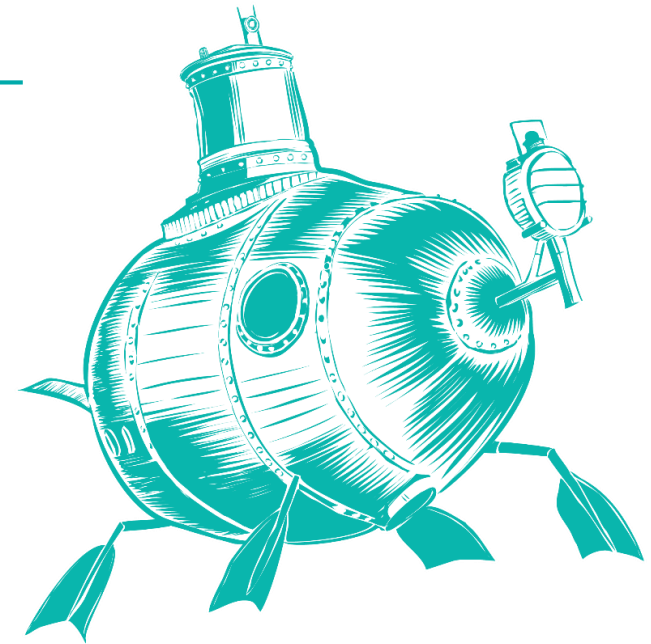
Bezpečnostní procesy

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



Onboarding zdravotnických systémů

- **Vedoucí lékaři a vedoucí laboratoří**
 - **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**

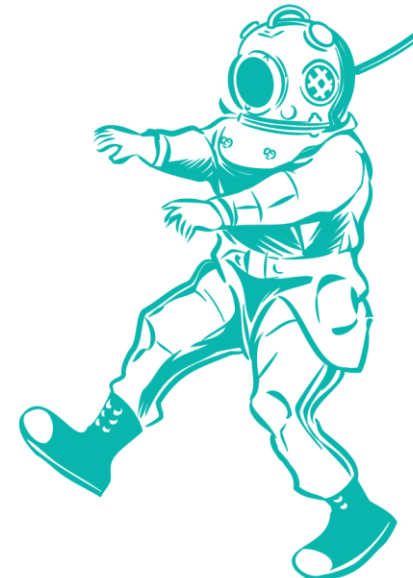
Motivace

Inventarizace a
sledování zařízení

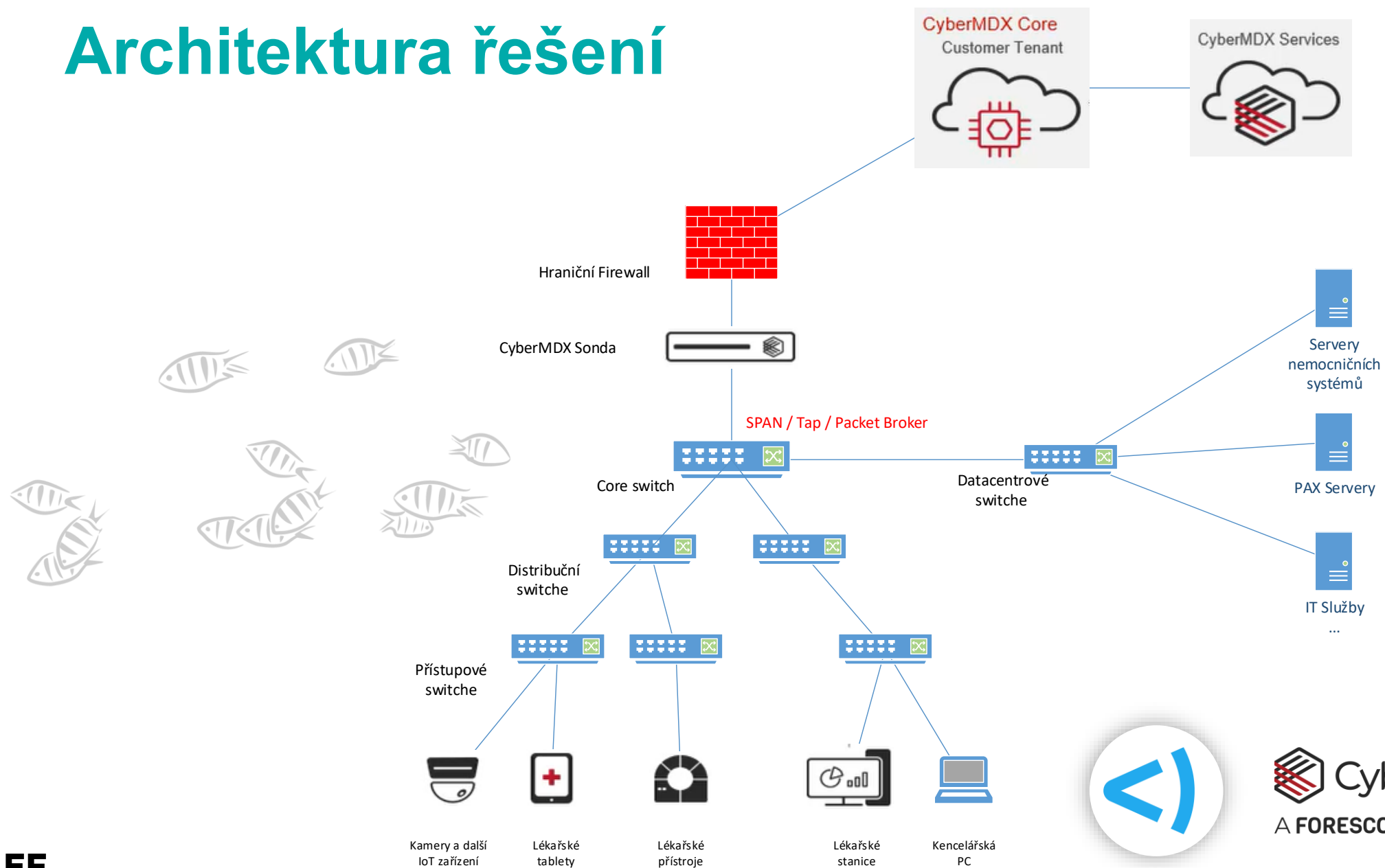
Detekce
zranitelností a
reaktivní opatření

Hodnocení rizik
a
prevence

Soulad s ZoKB
a
další legislativou



Architektura řešení



Architektura řešení

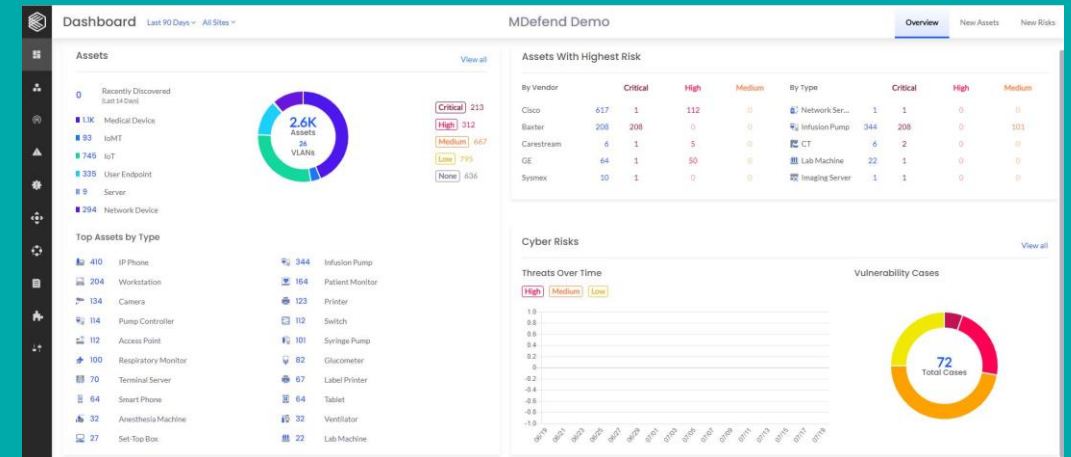


- **Pasivní systém napojen na SPAN, Tap, ...**
- **HW, nebo virtuální sondy**
- **Škálovatelnost – více lokalit, jedna správa**
- **Vyhodnocení pomocí AI v cloudové platformě i on-prem**

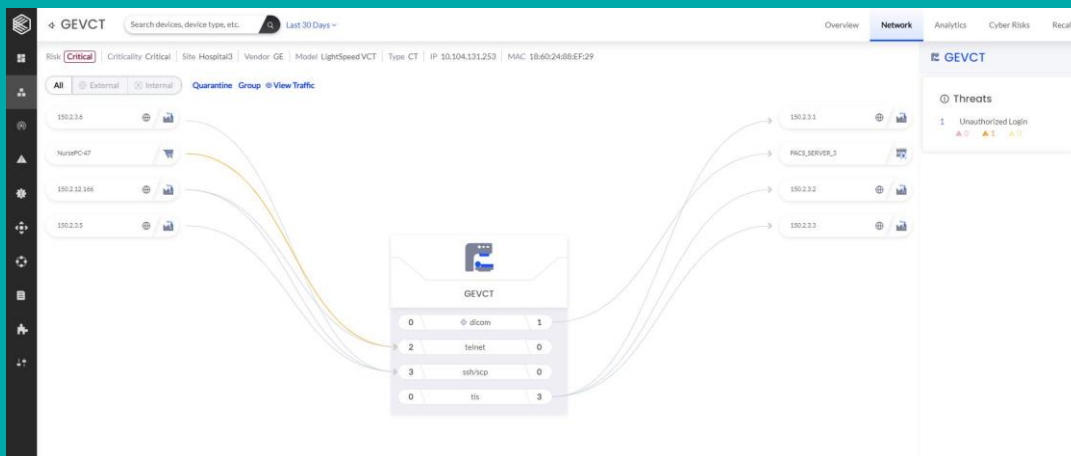


Klíčové funkcionality

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

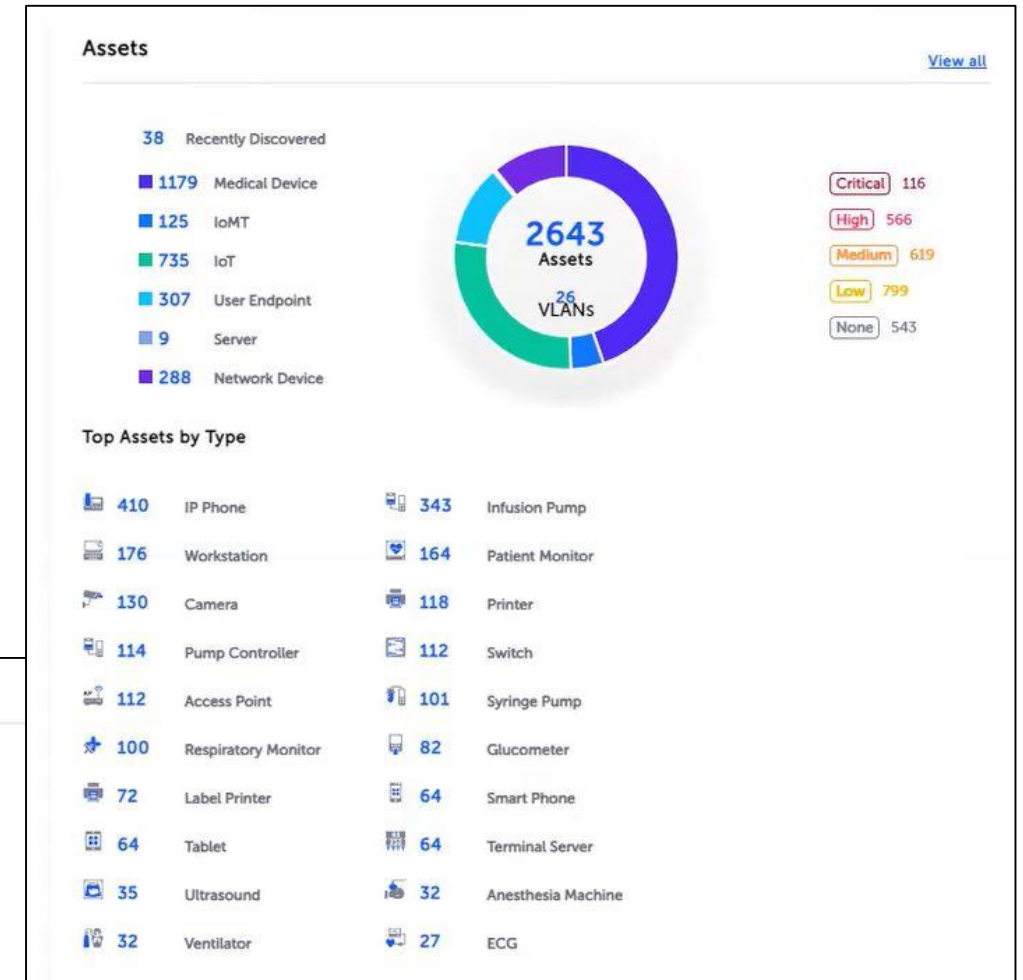


- Hodnocení rizik a prevence
- Zvýšení souladu s legislativními požadavky



Klíčové funkcionality

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



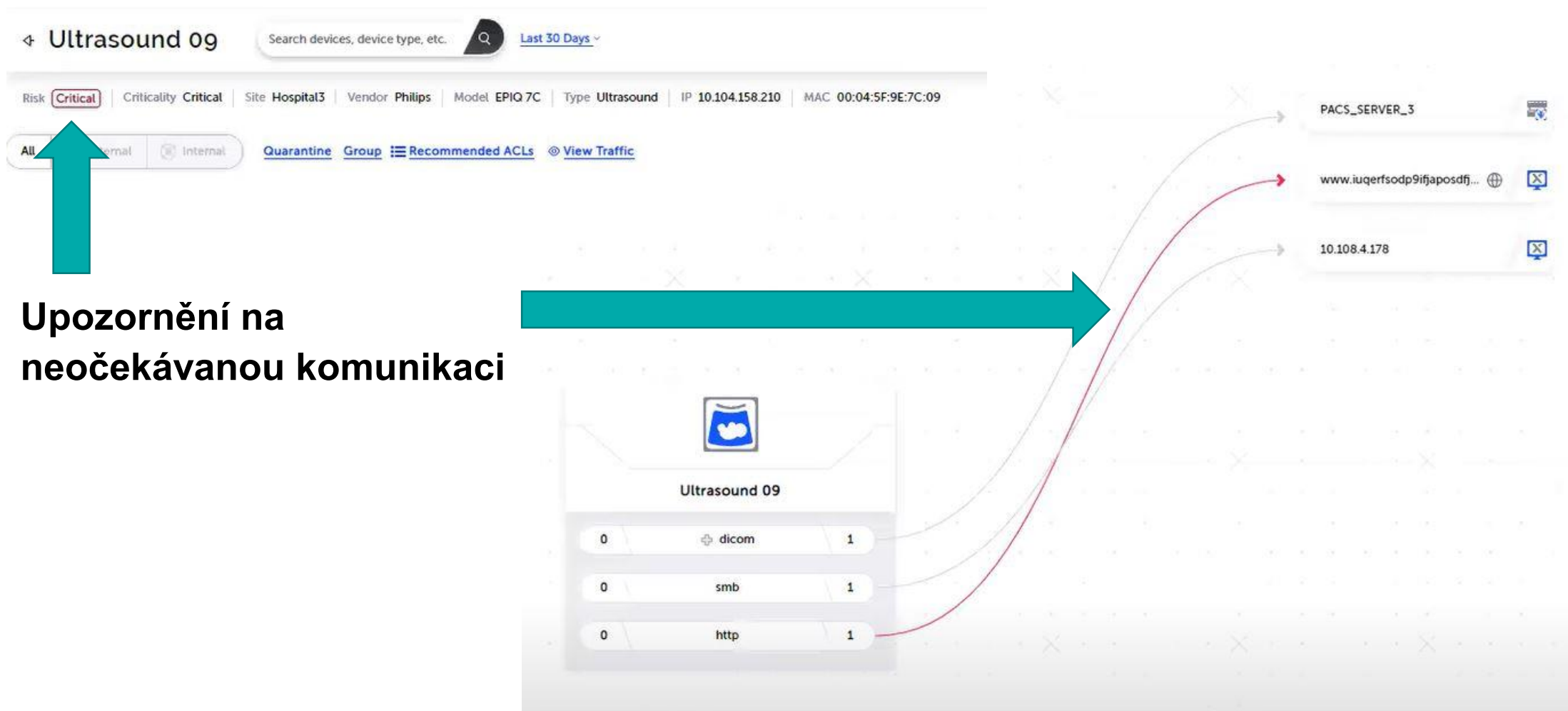
Assets With Highest Risk						
By Vendor				By Type		
		Critical	High	Medium		
BD	429	114	0	203	Pump Controller	114
Philips	117	1	84	0	Ultrasound	35
GE	73	1	68	0	CT	11
Baxter	208	0	208	0	Infusion Pump	343
DigiBoard	32	0	32	0	Patient Monitor	164

Inventarizace aktiv

The screenshot displays a network asset management interface for an Ultrasound device. The interface is divided into several sections:

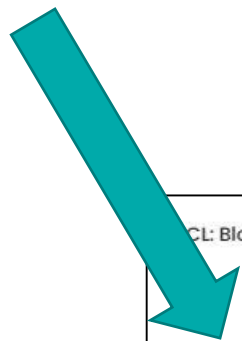
- Asset Attributes:** A list of device details including Category (Medical Device), Type (Ultrasound), Vendor (Philips), Model (EPIQ 7C), Equipment Function (6: Diagnostic - Other Physiological Monitoring), Classification Fidelity (High), MAC (00:04:5F:9E:7C:09), Location (Hospital3 > Floor 2 > Intensive Care Unit), Serial Number (444852609), Asset Tag (P6003719), Criticality (Critical), FDA Classification (Class II), Last Seen (08/25/2021 10:38), and First Seen (02/04/2021 03:49).
- Tags:** A set of color-coded tags including #Mottis Selected, Wireless, Internet Connected, Protocol: http, Recall, ePHI Sender, Protocol: smb, ePHI, Protocol: dicom, and +Requires Win7 ESU.
- Risk Assessment:** A summary section showing a CMDX Score of 94 (Critical), 4 Vulnerabilities, and 1 Threats.
- Device, Software, and Mitigations:** A table comparing device status with software updates and mitigations. The table has three columns: Device, Software, and Mitigations. The Device column shows Criticality (Critical), PHI (Yes), and Recalls (Yes (8)). The Software column shows Outdated Version (Yes), Default Credentials (Yes), and Known Vulnerabilities (Yes). The Mitigations column shows Endpoint Protection (Managed) and a status of No.
- Take Action:** A section with three cards: Change Configuration - S..., Update Software, and Update OS - Windows 7. Each card shows a risk reduction of 1 x Medium.
- Network Context:** A table showing network details for the device, including IP (10.104.158.210), VLAN (9), Subnet Name (Hospital3), Connection Type (Wireless - IEEE 802.11), Switch Port, Connected to SSID (Clinical), MAC (00:04:5F:9E:7C:09), NIC Vendor (AvalueTe), Binding Expiration Time, Binding Source, Authentication Algorithm, and Connection Encryption Type.

Mapy komunikací



Interaktivní návrhy opatření

- Návrh remediacce až na úroveň ACL a firewallových pravidel



ACL: Block All Inbound Traffic

```
permit udp any any eq 53
permit udp any any eq 67
permit udp any any eq 123
permit udp any any eq 137
permit udp any any eq 161
deny tcp any any match-all +syn +ack
deny udp any eq 3389 any
permit ip any any
```

Done

Blocklist

Network Level | Disabled

Description
Blocklist policies are pre-defined ACLs that are designed to mitigate the most common vulnerabilities by blocking their abusing ports. The policies are meant to protect assets and reduce their attack surface without interfering with their normal, intended functionality

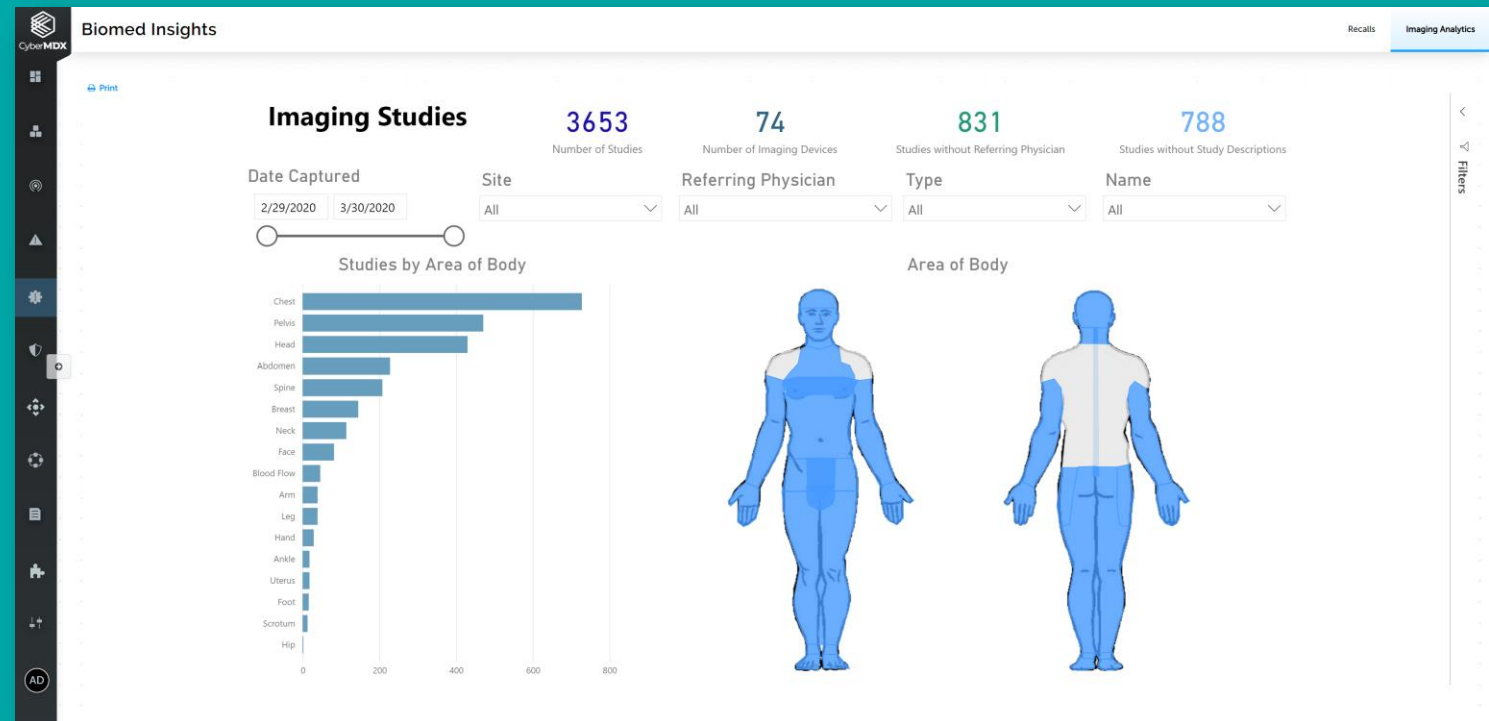
Blocklist Policies

Policy	Risk Reduction	Blocked Ports	Conflicts
☐ Block All Inbound Traffic	1 x High + 4 More	All inbound TCP	66
Block inbound traffic on the following protocols/ports (Detected conflicts are marked in red)			
All inbound TCP rdp (UDP / 3389)			
View ACL			
Affected Risks			
Name	Severity	Status	Confidence
CVE-2009-4445 (CVE-2009-4445)	Medium	Active	High
CVE-2009-2521 (CVE-2009-2521)	Medium	Active	High
CVE-2002-1717 (CVE-2002-1717)	Medium	Active	High
CVE-2002-1718 (CVE-2002-1718)	Medium	Active	High
CVE-2006-6578 (CVE-2006-6578)	High	Active	High
☐ Block Wormable, Management and Database Ports	1 x High + 4 More	16	None
☐ Block Wormable, Management and Database Ports, excluding RDP	1 x High + 4 More	13	None
☐ Block Wormable, Management and Database Ports, excluding RDP & SQL	1 x High + 4 More	12	None

Cancel Disable Activated Policy Apply

Vytížení kapacit zdravotnických zařízení

- Přehledy využití
- Plánování servisu a údržby

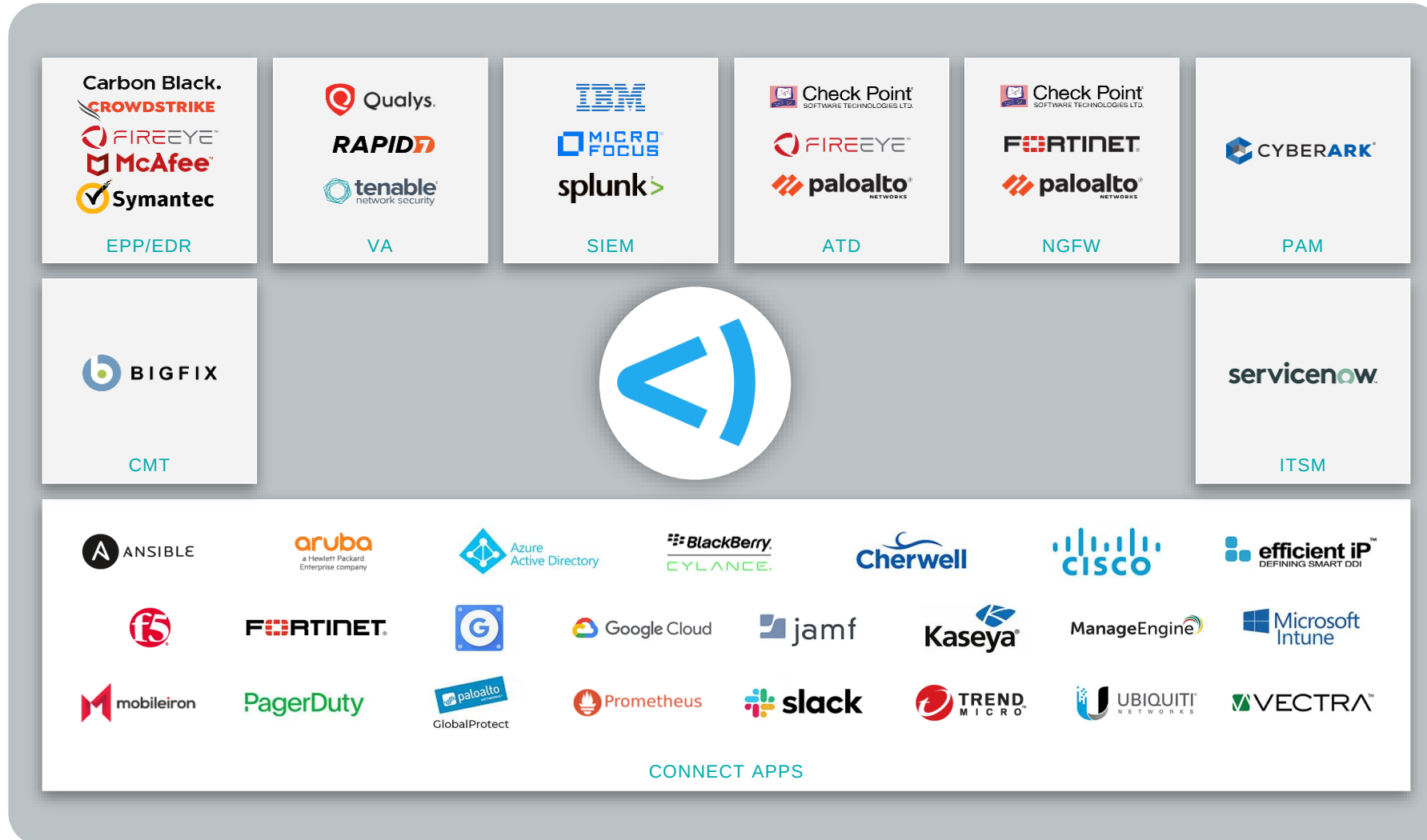


Komu je systém určen?

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



Integrate



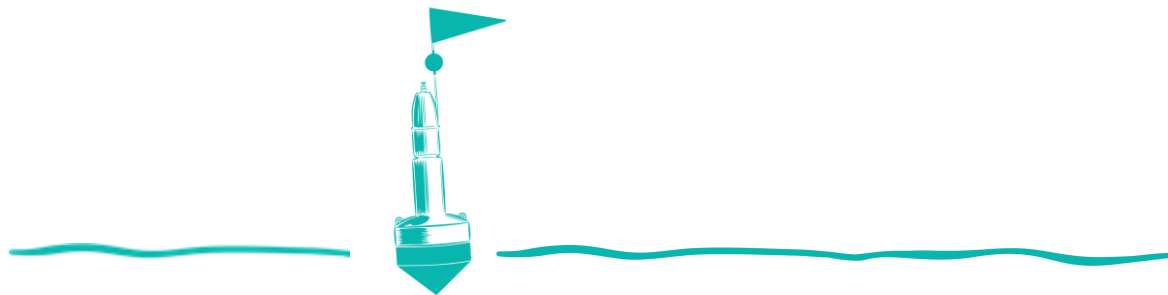
Co systém přináší?

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 Security+

ISO27001 Lead Auditor

ISO27001 Lead Implementer

