Ministerstvo zdravotnictví České republiky, Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Kybernetická bezpečnost resortu zdravotnictví 2021-2025

Informační bulletin 5/12-2022

NÁRODNÍ CENTRUM
ELEKTRONICKÉHO
ZDRAVOTNICTVÍ

Úvodník

Tento dokument přináší aktuální informace z oblasti kybernetické bezpečnosti v resortu MZ ČR.

Dnešní informace je zaměřena na výsledky provedeného Proof of Concept (dále jen „PoC“) nástroje pro zajištění komplexního bezpečnostního řešení IoT a IoMT, nástroje řešícího bezpečnostní rizika se zaměřením na zdravotnickou techniku a jiná aktiva v síti.

Předmětem PoC realizovaného v pražské nemocnici je nástroj Medigate stejnojmenné společnosti, která poskytuje řešení v oboru automatického rozpoznání medicínských zařízení a řízení jejich rizik.

Zdůvodnění potřebnosti

Bezpečnost zdravotnické techniky je jedním z témat v rámci Strategie kybernetické bezpečnosti resortu MZ ČR na roky 2021 až 2025. Zajištění evidence včetně analýzy rizik považuje MZ ČR za nezbytné k zajištění kybernetické bezpečnosti nemocnice jako celku. MZ ČR v této věci připravuje metodické doporučení.

MZ ČR si velmi silně uvědomuje slabé místo zdravotnických zařízení právě v kybernetické bezpečnosti zdravotnických prostředků. Zdravotnické prostředky jsou často postaveny na operačních systémech, které již nemají podporu výrobců, a proto je potřeba k jejich zabezpečení přistupovat s daleko větší pečlivostí než u běžných počítačových zařízení. Zároveň platí, že výrobci zdravotnických prostředků nechtějí portovat své zdravotnické prostředky na nejnovější operační systémy, a tudíž se s kybernetickým zabezpečením zdravotnických prostředků musí vypořádat IT administrátoři.

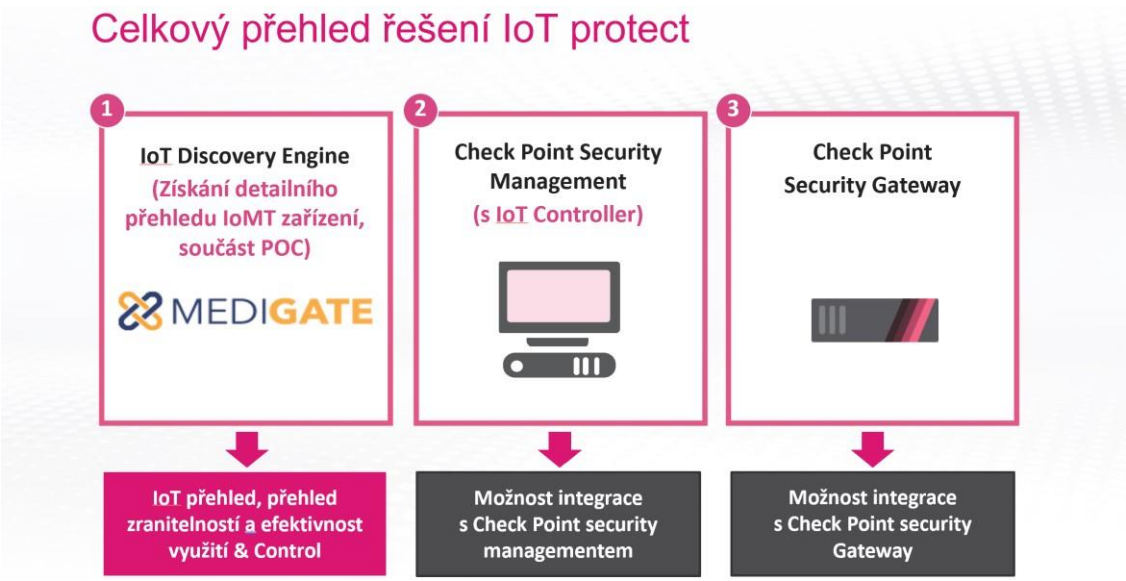
MZ ČR využilo realizace PoC k prezentování výsledků tohoto PoC pro možnost využití i v ostatních zdravotnických zařízeních. Jedná se o již druhý výstup PoC, který se týká zdravotnických prostředků (první výstup naleznete v Bulletinu č. 4).

Jak nástroj funguje

Platforma Medigate sdílí identifikované informace o zařízeních a detekovaných komunikačních vzorcích přes API propojení. Síťové nástroje tyto informace využívají pro automatizované vytvoření síťových objektů, logických skupin a pravidel pro řízení komunikace. Možnosti identifikovat zdravotnická zařízení podle jejich typu, funkce, dodavatele a názvu modelu umožňuje podrobnější řízení bezpečnostní politiky. Díky kontinuálnímu rozpoznávání zařízení systém Medigate zajišťuje, že objekty a logické skupiny jsou neustále aktualizovány a bezpečnostní pravidla jsou tak neustále aktuální i bez nutnosti instalace politiky.

V rámci evidence zdravotnické techniky a dalších IoT prvků a jejich zabezpečení se typicky postupuje v navrhovaných krocích. V případě PoC došlo dosud k realizaci pouze prvního z následujících popsaných kroků.

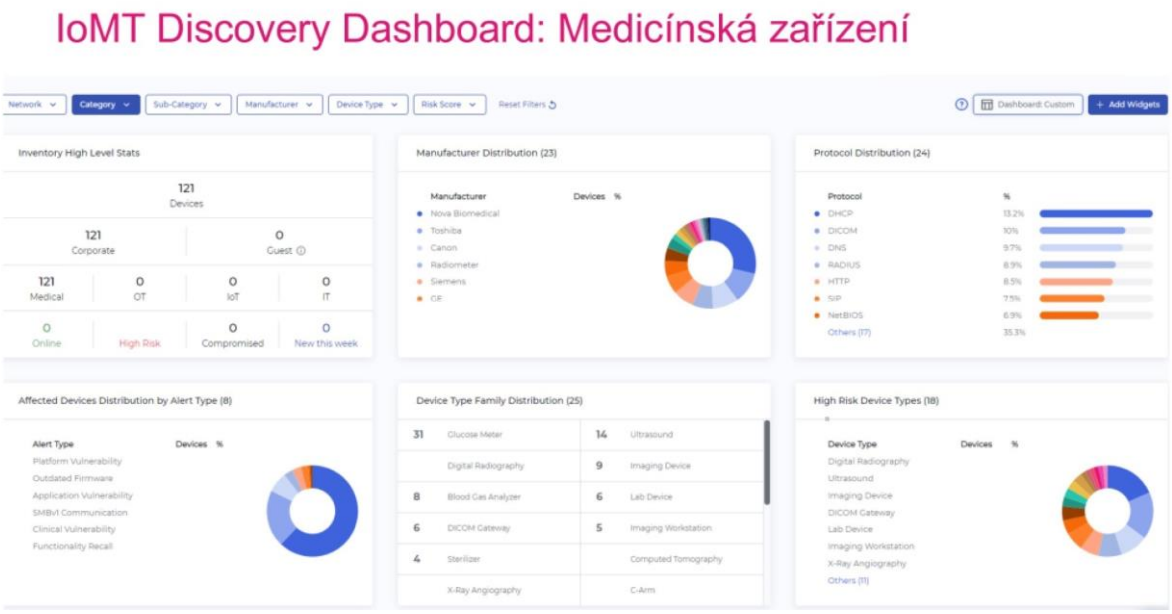
Obrázek č. 1 Celkový přehled



Po nasazení řešení Medigate Automatický “Discovery engine” – systém eviduje a rozpozná medicínskou techniku a vytváří katalog zařízení pro asset management.

Medigate dále provádí kategorizaci zařízení – nalezená zařízení jsou rozčleněna do logických skupin, ke kterým lze následně přistupovat v rámci nastavení dalších systémů bez nutnosti vytvářet pravidla pro každé zařízení zvlášť. Součástí evidence je rovněž automatizované vyhodnocení zranitelnosti – díky schopnosti rozpoznat aktuální verzi systému/firmware a propojení na znalostní databázi zranitelností systém reportuje riziková zařízení, což umožňuje efektivní navázání na proces např. pro patch management.

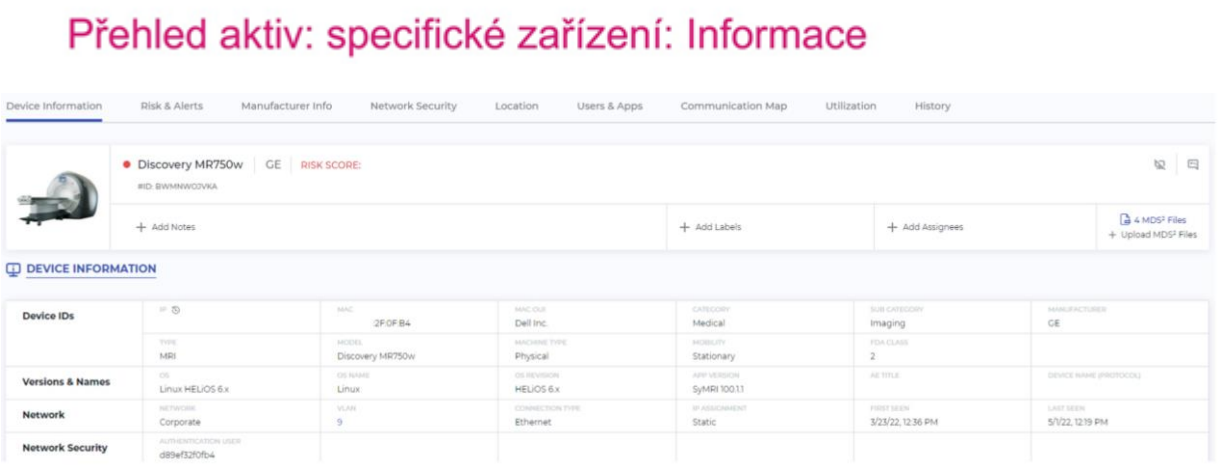
Obrázek č. 2 Evidence medicínských zařízení



Obrázek č. 3 Klasifikace zařízení

Rozsah získaných informací o jednotlivých zařízeních je v detailu zobrazen na následujícím obrázku, přičemž část je získána z prostředí a část z vlastní znalostní databáze Medigate.

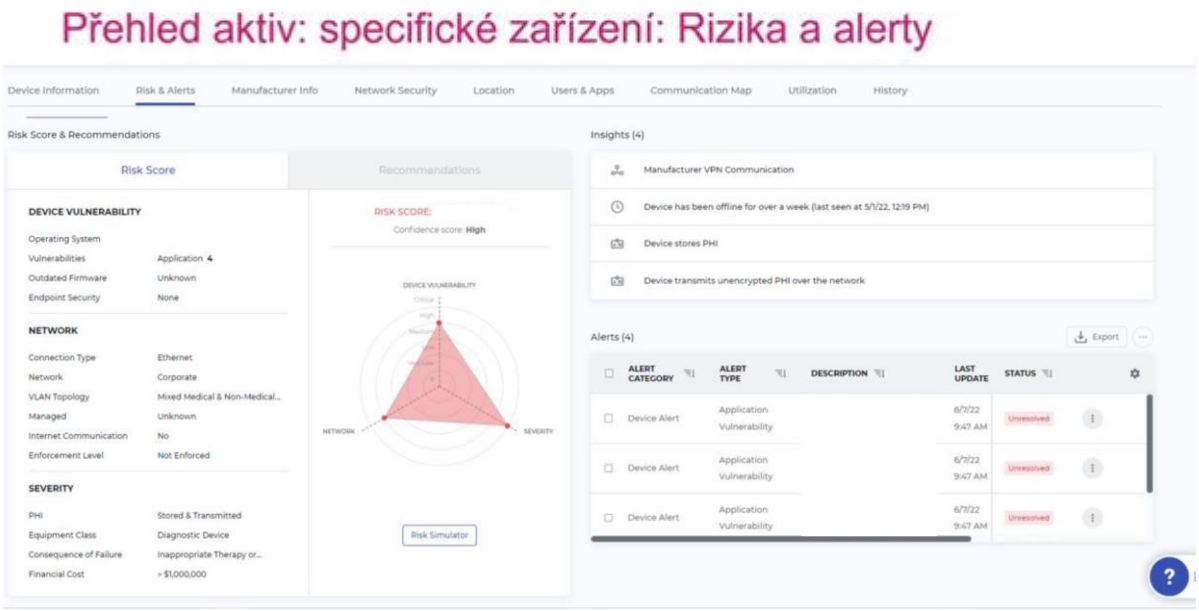
Obrázek č. 4 Informace o zařízeních



Na následujícím obrázku je vidět automatizovaně provedená analýza rizik. V rámci připravované metodiky zaměřené na zdravotnickou techniku bylo provedeno detailní vyhodnocení některých parametrů, na základě kterých je analýza prováděna, namátkově

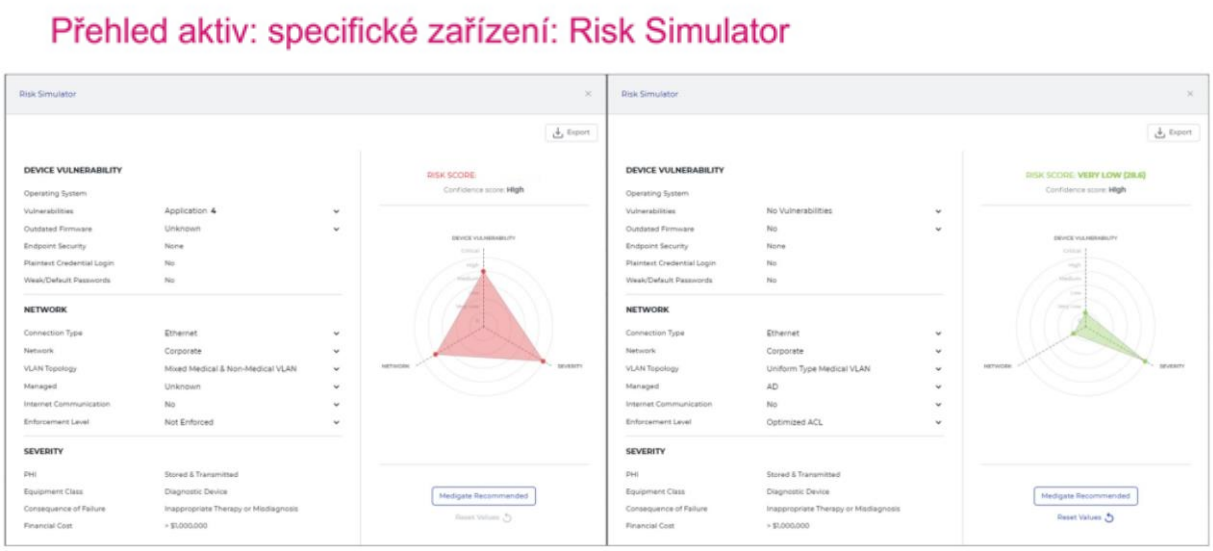
- Zda-li se jedná o komunikaci interní/externí - Zda jsou zařízení oddělená v samostatné VLAN
- Zda je síť řízena, tj. managed aj.

Obrázek č. 5 Přehled rizik



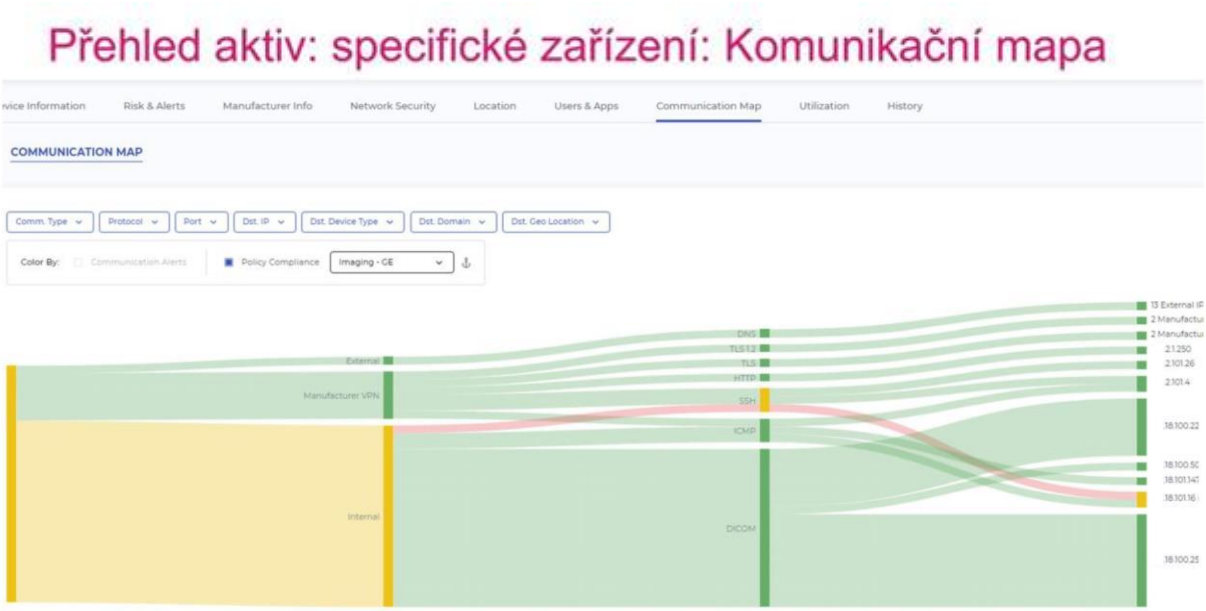
Na následujícím obrázku jsou navíc predikována rizika plynoucí z dalších zjištění, tj. typ operačního systému, zda-li je podporován či nikoli, zda má zařízení aktuální firmware (tj. je řádně patchováno), zda byly defaultní hesla na zařízení změněna, zda je na zařízení zajišťována bezpečnost na úrovni koncového zařízení atp.

Obrázek č. 6 Simulace rizik

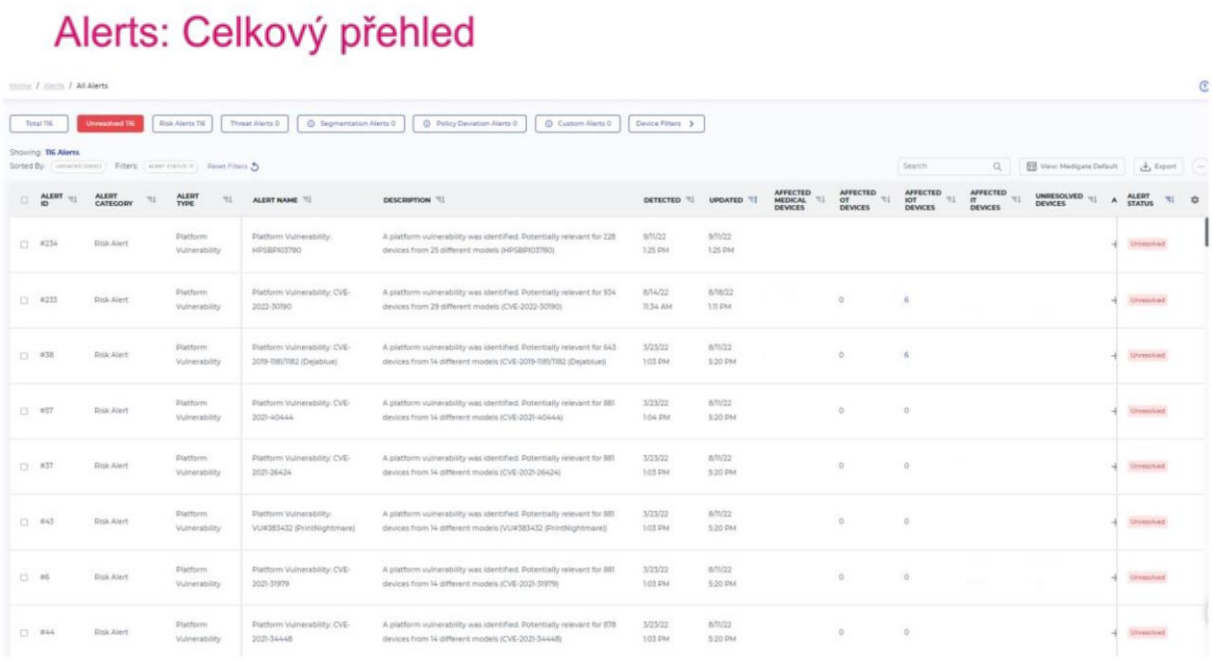


Součástí funkcí nástroje je rovněž část „Monitoring provozu“ – která zajišťuje vytvoření komunikační mapy pro ověření validity provozu, reporting odchylek/změn provozu, čímž je možno efektivně odchytit pokusy o nevalidní komunikaci. Jedná se o poměrně přehledný nástroj s rychlou informační hodnotou.

Obrázek č. 7 Komunikační mapa

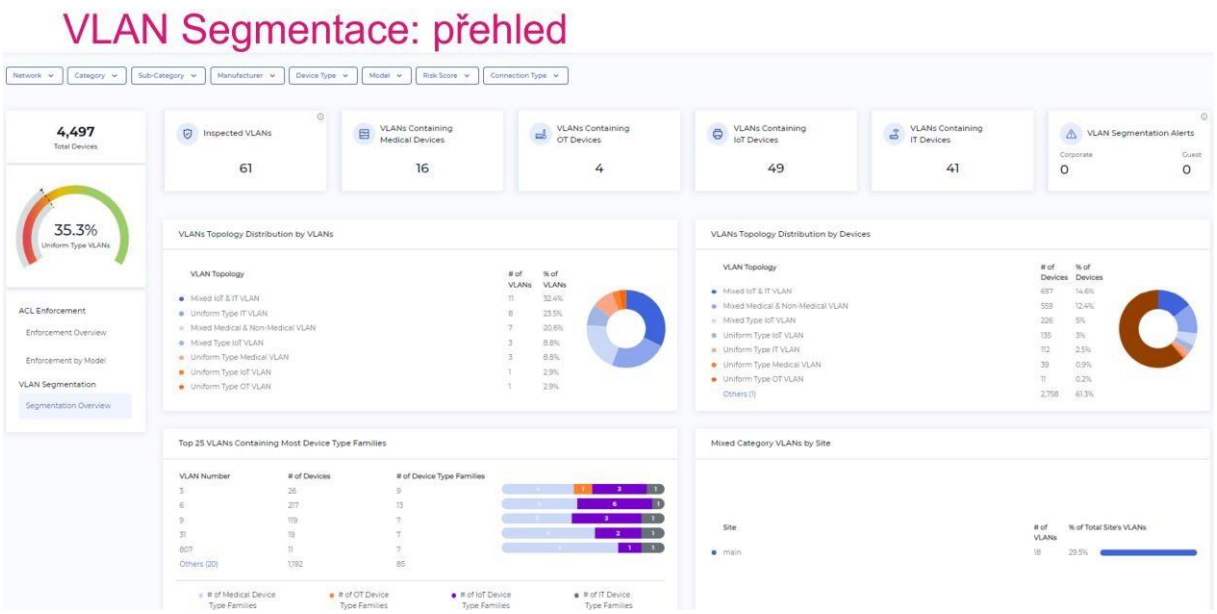


Medigate dále přináší indikátory kompromitace (IoC) pro dané prostředí – specifické indikátory kompromitace pro nemocniční prostředí pomohou odhalit potenciální incident v preinfekční i postinfekční fázi. Řešení Medigate obsahuje nástroje Threat Intelligence specifické pro nemocniční prostředí. Část disponibilního přehledu je uvedena na následujícím obrázku. Obrázek č. 8 Přehled alertů



Součástí výstupů PoC je i přehled o umístění zdravotnických prostředků společně s dalšími aktivy v rámci segmentované sítě.

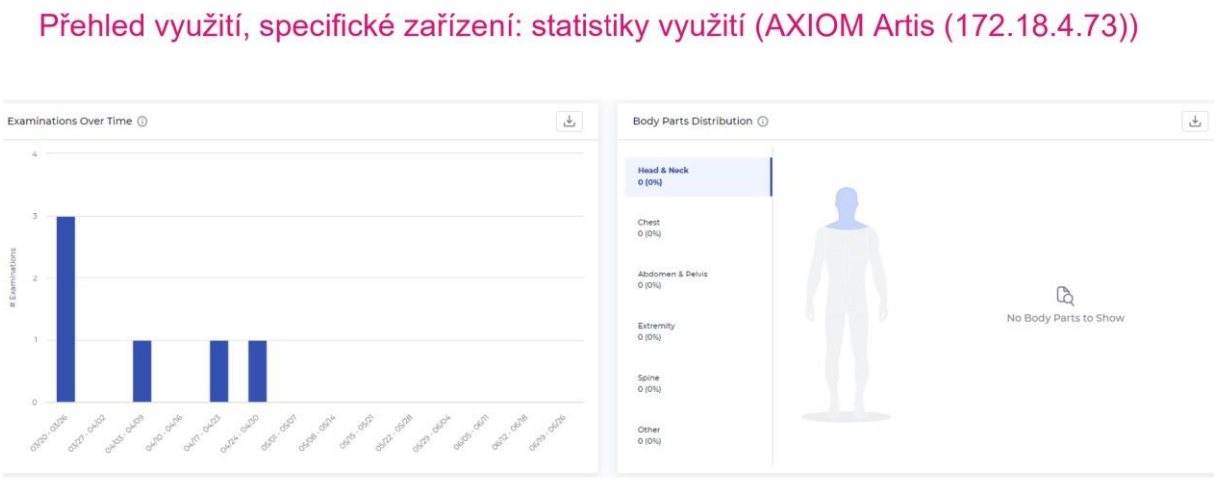
Obrázek č. 9 Přehled segmentace sítě



Poměrně zajímavou komponentou již mimo oblast kybernetické bezpečnosti je utilizace přístrojové techniky – vytváření statistik pro reálnou utilizaci zařízení, lokalizace zařízení v rámci objektů organizace (při integraci s WiFi kontrolerem), statistiky využití zařízení v čase a z pohledu prováděných vyšetření.

Lze se tedy jednoduše dostat k informacím o tom, jak často a v jakých časech je zdravotnická technika

v organizaci využívána. Podrobnosti na jednom vzorovém zařízení v následujícím obrázku. Obrázek č. 10 Statistika



Shrnutí přínosů nástroje

Po provedení odzkoušení bezpečnostního nástroje Check Point IoT Protect řešení, můžeme identifikovat následující tvrzení a přínosy:

- Medicínská zařízení jsou zranitelná
- Pro možnost efektivně řídit bezpečnost je nutný detailní přehled aktiv, řízení zranitelností a detekce anomálií
- Řešení Discovery engine poskytuje detailní přehled aktiv, řízení zranitelností, detekce anomálií a přehled využití prostředků
- Discovery engine se může snadno a efektivně integrovat s bezpečnostním řešením Check Point

Seznamte se

Představujeme aktualizovaný seznam organizací podílejících se na zavádění kybernetické bezpečnosti v rámci resortu Ministerstva zdravotnictví ČR, a osoby, které se na realizaci podílí.

Subjekty z pohledu zajišťování kybernetické bezpečnosti

Název subjektu	Role subjektu
MZ ČR	Nositel projektu zavedení KB a povinná osoba dle ZoKB.
NÚKIB	Je správním úřadem pro kybernetickou bezpečnost.
CESNET	Je sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu.
ÚZIS ČR	ÚZIS ČR je správcem Národního zdravotnického informačního systému.
NCeZ	Zabezpečuje působnost ministerstva v oblasti strategického a koncepčního rozvoje digitalizace zdravotnictví a související činnosti např. • Přípravu a správu Informační koncepce ministerstva a dalších resortních informatických koncepcí vydávaných ministerstvem. • Zabezpečuje agendu Národního kontaktního místa pro elektronické zdravotnictví. • Zabezpečuje činnost vnitrostátní sítě pro digitální zdravotnictví.

Osoby podílející se na realizaci programu zavádění KB

Jméno	Role osoby
Vít Lidinský	Manažer kybernetické bezpečnosti MZ ČR Předseda Rady bezpečnostních rolí kybernetické bezpečnosti
Jakub Tomas	Architekt kybernetické bezpečnosti MZ ČR
Václav Minářů	Tajemník: • Výboru pro řízení kybernetické bezpečnosti • Rady bezpečnostních rolí kybernetické bezpečnosti

Dalšími klíčovými osobami podílejícími se na realizaci programu jsou:

- Členové Výboru pro řízení kybernetické bezpečnosti MZ ČR,
- Členové Rady bezpečnostních rolí kybernetické bezpečnosti.

Zkratky a pojmy

CESNET	Sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu pro vědu, výzkum a vzdělávání zahrnující počítačovou síť, výpočetní gridy, datová úložiště, prostředí pro spolupráci a nabízející širokou škálu služeb
ESF	Evropský sociální fond
hSOC	hospital Security Operation Center - komunitní iniciativ a platforma
HaSIM	Health and Social Insider Monitor
IROP	Integrovaný regionální operační program
ISMS	Information Security Management System - mezinárodní zkratka pro systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací podle normy ISO27001
IKT	Odbor informačních technologií a elektronizace zdravotnictví MZ ČR
IoT	Internet of Things (Internet věcí)
IoMT	Internet of Medical Things (Internet lékařských věcí)
KB	Kybernetická bezpečnost
MPO	Ministerstvo průmyslu a obchodu České republiky
MZ ČR	Ministerstvo zdravotnictví České republiky.
NAKIT	Národní agentura pro komunikační a informační technologie, s. p.
NCeZ	Národní centrum elektronického zdravotnictví
NCKB	Národní centrum kybernetické bezpečnosti je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)
NPO	Národní plán obnovy
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PoC	Proof of Concept (Studie proveditelnosti)
SOC	Security Operation Center (Operační centrum informační bezpečnosti)
SŘBI	Systém řízení bezpečnosti informací – česká zkratka a význam pro ISMS
Strategie KB	Dokument Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025
ÚZIS ČR	Ústav zdravotnických informací a statistiky ČR
VoKB	Vyhláška o kybernetické bezpečnosti
ZoKB	Zákon o kybernetické bezpečnosti

Legislativa

Základní legislativa ke kybernetické bezpečnosti

- Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti https://www.zakonyprolidi.cz/cs/2014-181

NÚKIB vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb.

- Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

  https://www.zakonyprolidi.cz/cs/2018-82

- Vyhláška č. 437/2017 Sb. Vyhláška o kritériích pro určení provozovatele základní služby

  https://www.zakonyprolidi.cz/cs/2017-437

Základní legislativa k informačním systémům veřejné správy

- Zákon 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů https://www.zakonyprolidi.cz/cs/2000-365
- Vyhláška č. 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

  https://www.zakonyprolidi.cz/cs/2006-529

- Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů.

  https://www.zakonyprolidi.cz/cs/2020-360 https://www.zakonyprolidi.cz/cs/2014-317