ZMLUVA O POSKYTOVANÍ SLUŽBY

uzavretá podľa ust. § 269 ods. 2 zák. č. 513/1991 Zb. Obchodný zákonník
(ďalej aj „Zmluva") medzi

Objednávateľ:	**Fakultná nemocnica s poliklinikou Nové Zámky**
Sídlo:	Slovenská 11 A, Nové Zámky
IČO:	17336112
DIČ:	2021068324
IČ DPH:	SK2021068324
Zapísaný:	register organizácií vedený Štatistickým úradom Slovenskej republiky a živnostenský register Okresného úradu Nové Zámky pod č. 404-9729
Bankové spojenie:	IBAN SK88 8180 0000 0070 0054 0295, vedený v Štátnej pokladnici
,	
E-mail:	email@nspnz.sk
Zastúpený:	MUDr. Karol Hajnovič-riaditeľ

(ďalej len „**Objednávateľ**")

a

Poskytovateľ:	AXENTA s.r.o
Sídlo:	Mlynská 898/12, 031 01 Liptovský Mikuláš
IČO:	51142708
DIČ:	2120600878
Zapísaný:	v Obchodnom registri Okresného súdu Žilina, oddiel: Sro, vložka číslo: 68671/L
Bankové spojenie:	SK81 7500 0000 0040 2509 1867
E-mail:	lichvar@axenta.sk
Zastúpený:	ing. Ján Lichvár, konateľ

(ďalej len „**Poskytovateľ**")

(Objednávateľ a Poskytovateľ ďalej aj ako „**Zmluvná strana**", alebo „**Zmluvné strany**")

Článok I.
Úvodné ustanovenie

1. Účelom tejto Zmluvy je úprava práv a povinností Zmluvných strán pri vykonávaní predmetu Zmluvy špecifikovaného v článku II. tejto Zmluvy.

Článok II.
Predmet zmluvy

1. Predmetom tejto Zmluvy je záväzok Poskytovateľa za podmienok dohodnutých v tejto Zmluve poskytovať Objednávateľovi služby monitoringu kybernetickej bezpečnosti a riadenia kybernetických bezpečnostných incidentov v priestoroch prevádzky Objednávateľa a poskytovať služby dohľadového centra „SOC" (Security Operation Centre) (ďalej aj „SOC") v priestoroch prevádzky Poskytovateľa, pričom poskytovanie služieb monitoringu kybernetickej bezpečnosti a riadenia kybernetických bezpečnostných incidentov a poskytovanie služieb dohľadového centra SOC (Security Operation Centre) je neoddeliteľne prepojené (ďalej aj „Služby"). Rozsah služby poskytnutý Poskytovateľom je špecifikovaný v prílohe č. 1 ako súčasť zmluvy.
2. Predmetom tejto zmluvy je zároveň aj záväzok Objednávateľa uhradiť Poskytovateľovi za poskytnuté služby podľa ods. 1 tohto článku Zmluvy odmenu dohodnutú podľa tejto Zmluvy.

3. Služby poskytované Poskytovateľom pozostávajú z implementačnej časti a postimplementačnej časti.

4. Implementačná časť podľa predchádzajúceho odseku tohto článku tejto Zmluvy pozostáva z inštalácie hardverových zariadení(2U server, CPU: 8 jadier – 16 vlákien, RAM: 64 GB RAM, HDD: 4x4TB 7.2k, Napájanie: 2x a softvérového vybavenia Poskytovateľa za účelom zabezpečenia bezpečnostného monitoringu informačných systémov a IT/OT sietí v sídle Objednávateľa a ich následné pripojenie na dohľadové cetrum SOC prevádzkované v sídle Poskytovateľa, za účelom vytvorenia uceleného funkčného systému, ktorý zabezpečí kybernetickú bezpečnosť informačných systémov Objednávateľa vo forme komplexného monitoringu IT/OT infraštruktúry Objednávateľa, kontroly činností všetkých registrovaných užívateľov IT/OT infraštruktúry Objednávateľa na všetkých úrovniach, spracovanie dát, sledovania dátovej prevádzky informačnej infraštruktúry Objednávateľa, pričom systém musí byť schopný registrovať interné a externé kybernetické útoky na systémy IT/OT infraštruktúru Objednávateľa a zároveň ich aj priebežne odhaľovať. Inštalované hardvérové zariadenia a softwérové vybavenie Poskytovaľa musí umožniť v celom rozsahu následné zabezpečenie služby SOC (ďalej aj „implementačná časť").

5. Postimplementačná časť podľa čl. II. ods. 3 tejto Zmluvy predstavuje poskytovanie služby dohľadového centra SOC po dobu 36 mesiacov (ďalej aj „postimplementačná časť").

Článok III.
Čas a miesto plnenia

1. Zmluvné strany sa dohodli, že Poskytovateľ začne s inštaláciou hardvérových zariadení a softvérového vybavenia podľa čl. II. ods. 3 tejto Zmluvy v prevádzke Objednávateľa najneskôr do 30 pracovných dní odo dňa nadobudnutia účinnosti tejto Zmluvy, pričom Poskytovateľ začne poskytovať Služby špecifikované v čl. II. ods. 4 tejo Zmluvy, najneskôr do troch mesiacov odo dňa začatia inštalácie hardvérových zariadení a softvérového vybavenia v prevádzke Objednávateľa.

2. Poskytovateľ bude poskytovať Služby SOC v pracovných dňoch v čase od 07:00 hod. do 17:00 hod.

   Miestom poskytovania služieb je prevádzka Objednávateľa, v ktorej sú umiestnené IT/OT systémy Objednávateľa, a to prevádzka umiestnená na adrese sídla Objednávateľa: Slovenská 11A, Nové Zámky. Miestom poskytovania služieb je tiež miesto umiestnenia dohľadového centra SOC, umiestnené na adrese sídla Poskytovateľa.

Článok IV.
Cena za poskytované služby a platobné podmienky

1. Cena za poskytované Služby je určená dohodou Zmluvných strán vo výške 52 200,00EUR (päťdesiatdvatisícdvesto) bez DPH (62 640,00 EUR s DPH) za celú zmluvu za obdobie tridsaťšesť mesiacov.
   Cenu za obdobie tridsaťšesť mesiacov bez DPH tvorí:
   A) Vulnerability Assessment a Vulnerability Management vo výške 7200,00EUR
   B) Log Management – systém zberu logov vo výške 30960,00EUR
   C) Služba Security Operation Centra - SOC vo výške 14040,00EUR
   Cena za poskytované Služby je určená dohodou Zmluvných strán vo výške 1 450,00 EUR bez DPH za jeden kalendárny mesiac poskytovania Služby.

2. K cene za Služby bude pripočítaná DPH v zmysle platných právnych predpisov. Dohodnutá cena je konečná a zahŕňa všetky náklady Poskytovateľa súvisiace s poskytovaním Služieb.

3. Poskytovateľ sa zaväzuje vystaviť a odoslať faktúru poskytnuté služby mesačne podľa čl. II. tejto Zmluvy do 5. dňa mesiaca nasledujúceho po mesiaci, v ktorom boli Služby poskytnuté.

4. Za okamih úhrady ceny za Služby sa považuje okamih, kedy bola fakturovaná čiastka pripísaná v celom rozsahu na bankový účet Poskytovateľa.

5. Lehota splatnosti faktúry je 60 (šesťdesiat) dní odo dňa jej doručenia Objednávateľovi.

Článok V.
Povinnosti zmluvných strán

1. Poskytovateľ sa zaväzuje realizovať predmet Zmluvy s odbornou starostlivosťou, v súlade s právnymi predpismi, najmä so zák. č. 69/2018 Z.z. o kybernetickej bezpečnosti a jeho vykonávacími predpismi s prihliadnutím na prevádzkované základné služby Objednávateľa.

2. Poskytovateľ sa zaväzuje poskytovať Objednávateľovi Služby najmenej v rozsahu požadovanom v prílohe č. 1 tejto Zmluvy.

3. Poskytovateľ je ďalej povinný:

    a) zabezpečiť všetky prostriedky potrebné na realizáciu predmetu Zmluvy,
    b) zabezpečiť dohodnuté poskytovanie Služieb riadne a včas tak, aby nedošlo k prerušeniu plnenia predmetu Zmluvy,
    c) zotrvávať v priestoroch Objednávateľa len na čas nevyhnutne potrebný na plnenie predmetu Zmluvy a tieto priestory opustiť bezodkladne po splnení predmetu Zmluvy,
    d) postupovať podľa pokynov Objednávateľa,
    e) upozorniť Objednávateľa na zjavnú nevhodnosť jeho pokynov, v prípade, ak Objednávateľ napriek upozorneniu trvá splnení pokynov, Poskytovateľ nezodpovedá za vzniknutú škodu,
    f) byť zapísaný v registri partnerov verejného sektora podľa zák. č. 315/2016 Z.z. o registri partnerov verejného sektora, najneskôr ku dňu podpisu tejto Zmluvy, pričom zápis v registri partnerov verejného sektora musí trvať minimálne po celú dobu trvania tejto Zmluvy.

4. Objednávateľ je povinný vytvoriť Poskytovateľovi všetky podmienky tak, aby predmet Zmluvy mohol plniť včas a riadne a za tým účelom úzko spolupracovať s Poskytovateľom.

5. Objednávateľ zabezpečí v nevyhnutnom rozsahu Poskytovateľovi prístup do všetkých priestorov nevyhnutných na poskytovanie Služieb.

6. Objednávateľ sa zaväzuje poskytnúť Poskytovateľovi všetky relevantné informácie a doklady potrebné na plnenie predmetu Zmluvy.

7. Zmluvné strany sa dohodli, že o odovzdaní a prevzatí implementačnej časti Služieb spíšu protokol, v ktorom bude uvedený minimálne deň začatia a ukončenia inštalácie hardvérových zariadení a softvérového vybavenia implementačnej časti Služieb a zoznam inštalovaných hardvérových zariadení a softvérového vybavenia a prác vykonaných v súvislosti s tým.

8. Zmluvné strany sú si povinné navzájom poskytovať súčinnosť o všetkých otázkach, ktoré sú nevyhnutné na plnenie predmetu tejto Zmluvy. V prípade

omeškania niektorej zmluvnej strany s poskytnutím súčinnosti, nie je druhá zmluvná strana v omeškaní s plnením svojej povinnosti podľa tejto Zmluvy.

Článok VI.
Zodpovednosť za škodu

1. Zmluvná strana zodpovedá za škodu, ktorú spôsobí druhej Zmluvnej strane porušením svojej povinnosti zo Zmluvy a je povinná ju nahradiť, okrem prípadov, kedy preukáže, že porušenie povinnosti bolo spôsobené okolnosťami vylučujúcimi zodpovednosť.

2. Zmluvné strany sa dohodli, že žiadna zo Zmluvných strán nezodpovedá za škodu, ktorá vznikla v dôsledku vecne nesprávneho alebo inak chybného zadania druhej Zmluvnej strany.

3. Zmluvné strany sa dohodli, že žiadna zo zmluvných strán nie je zodpovedná za nesplnenie svojho záväzku v dôsledku omeškania druhej Zmluvnej strany.

4. Zmluvné strany nezodpovedajú za škody, ktoré by mohli spôsobiť, resp. spôsobili druhej Zmluvnej strane porušením povinnosti podľa Zmluvy v prípade, ak toto bolo spôsobené vyššou mocou, za ktorú daná zmluvná strana nenesie zodpovednosť, a ktorú ani pri vynaložení dostupnej starostlivosti nemohla ovplyvniť.

5. Ak príde k porušeniu akejkoľvek povinnosti podľa tejto Zmluvy, ktorej porušenie je zabezpečené zmluvnou pokutou podľa čl. VIII. tejto Zmluvy, nemá Zmluvná strana popri nároku na zmluvnú pokutu, nárok na náhradu škody.

Článok VII.
Dohoda o mlčanlivosti

1. Pri plnení predmetu tejto Zmluvy poskytuje Objednávateľ Poskytovateľovi dôverné informácie, a to najmä časť svojho obchodného a výrobného know-how, obchodnej stratégie, informácie súvisiace s duševným vlastníctvom Objednávateľa, s jeho výrobnými kapacitami, ekonomickými ukazovateľmi (ďalej len „dôverné informácie“).

2. Poskytovateľ sa podpisom tejto Zmluvy výslovne zaväzuje, že zachová mlčanlivosť o všetkých dôverných informáciach, o ktorých sa v súvislosti s plnením predmetu Zmluvy dozvie, najmä sa zaväzuje:
   a) uchovávať a chrániť ako dôverné všetky informácie, o ktorých sa pri plnení predmetu Zmluvy dozvedel,
   b) používať poskytnuté dôverné informácie výlučne pre účely plnenia predmetu Zmluvy a v súlade s pokynmi Objednávateľa,
   c) neposkytnúť tretej osobe žiadnu z dôverných informácií,
   d) zabezpečiť uchovávanie všetkých dôverných informácií tak, aby k nim nemali prístup neoprávnené osoby,
   e) nevyhotovovať kópie dôverných informácií bez predchádzajúceho písomného súhlasu Objednávateľa,
   f) chrániť všetky nosiče obsahujúce dôverné informácie pred ich stratou, poškodením, odcudzením, zničením, nedovoleným rozmnožovaním, rozširovaním alebo iným neoprávneným použitím, a to bez ohľadu na ich formu.

3. Poskytovateľ môže sprístupniť poskytnuté dôverné informácie len tým svojim zamestnancom, alebo povereným osobám, ktorých oboznámenie sa s dôvernými informáciami je nevyhnutné pre účely plnenia predmetu Zmluvy. Poskytovateľ v celom rozsahu preberá zodpovednosť za to, že všetci jeho zamestnanci a ním poverené osoby budú rovnako dodržiavať mlčanlivosť podľa tejto Zmluvy.

4. Po zániku tejto Zmluvy je Poskytovateľ povinný vrátiť Objednávateľovi na jeho žiadosť všetky dôverné informácie, ktoré mu boli poskytnuté písomne, v elektronickej alebo inej podobe, a to vrátane všetkých ich kópií, rovnako je povinný zabezpečiť likvidáciu všetkých dôverných informácií, ktoré mu boli poskytnuté písomne, v elektronickej alebo inej podobe.

5. Poskytovateľ je povinný rešpektovať všetky práva duševného a/alebo priemyselného vlastníctva, ktoré sa viažu k poskytnutým dôverným informáciám.

Článok VIII.
Sankcie

1. V prípade omeškania Poskytovateľa s riadnym poskytnutím Služieb podľa tejto Zmluvy a/alebo v prípade omeškania reakcie Poskytovateľa na bezpečnostný incident v reakčnej dobe podľa prílohy č. 1 tejto Zmluvy, má Objednávateľ právo na zaplatenie zmluvnej pokuty vo výške 0,05 % z ceny Služieb za každý, i začatý deň omeškania.

2. V prípade omeškania reakcie Poskytovateľa na reklamáciu Služieb Objednávateľom v lehote 3 dní odo dňa doručenia reklamácie Služieb; v prípade omeškania Poskytovateľa s odstránením reklamovanej vady Služieb v lehote 10 dní, resp. v dodatočne dohodnutej lehote odo dňa doručenia reklamácie Služieb; v prípade omeškania reakcie Poskytovateľa na bezpečnostný incident v reakčnej dobe podľa prílohy č. 1 tejto Zmluvy, má Objednávateľ právo na zaplatenie zmluvnej pokuty vo výške 33,- EUR za každý, aj začatý deň omeškania.

3. V prípade omeškania Objednávateľa s úhradou ceny za Služby podľa čl. IV. tejto Zmluvy, má Poskytovateľ právo na zaplatenie zmluvnej pokuty v zákonom stanovenej výške za každý, i začatý deň omeškania s úhradou.

   V prípade, ak Poskytovateľ, akýkoľvek jeho zamestnanec alebo Poskytovateľom poverená osoba poruší akúkoľvek povinnosť mlčanlivosti, bude Objednávateľ oprávnený požadovať od Poskytovateľa zaplatenie náhrady škody.

Článok IX.
Trvanie a ukončenie zmluvy

1. Táto Zmluva sa uzatvára na dobu určitú, a to do uplynutia 36 kalendárnych mesiacov odo dňa začatia poskytovania služby. Deň začatia poskytovania Služby je zhodný s dňom kedy táto Zmluva nadobudne účinnosť. Zmluva nadobudne účinnosť v deň nasledujúci po dni zverejnenia Zmluvy v Centrálnom registri zmlúv, ak sa Zmluvné strany nedohodnú inak.

2. Zmluvné strany sa dohodli, že táto Zmluva môže byť ukončená iba:

   a) písomnou dohodou Zmluvných strán a to ku dňu uzavretia takejto dohody;
   b) písomným odstúpením:
      i. Objednávateľa v prípade, ak Zhotoviteľ neposkytne Služby ani do 30 (tridsať) dní odo dňa nasledujúceho po dni, kedy mali byť Služby podľa čl. III. ods. 1 tejto Zmluvy poskytnuté,
      ii. Objednávateľa v prípade, ak počas trvania tejto Zmluvy príde k ukončeniu Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností uzavretej medzi Zmluvnými stranami dňa],
      iii. Poskytovateľa iba v prípade, ak Objednávateľ neposkytol Poskytovateľovi potrebnú súčinnosť a informácie potrebné pre poskytnutie Služieb v súlade s čl. V. tejto Zmluvy, alebo ak je Objednávateľ v omeškaní s úhradou ceny za Služby v súlade s čl. IV tejto Zmluvy;

c) písomnou výpoveďou, aj bez udania dôvodu.

3. V prípade ukončenia tejto Zmluvy písomným odstúpením sa Zmluvné strany dohodli, že písomné odstúpenie musí byť zaslané doporučene na adresu sídla druhej Zmluvnej strany a musí v ňom byť uvedený dôvod odstúpenia.

4. V prípade ukončenia tejto Zmluvy písomnou výpoveďou sa Zmluvné strany dohodli, že písomná výpoveď musí byť zaslaná doporučene na adresu sídla druhej Zmluvnej strany, pričom výpovedná lehota je 1 (jeden) mesiac a začína plynúť prvého dňa mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej Zmluvnej strane.

5. Objednávateľ je povinný uhradiť Zhotoviteľovi pomernú časť ceny za Služby a preukázateľne vynaložené náklady súvisiace s poskytnutím Služieb a to k dátumu odstúpenia od Zmluvy Objednávateľom.

Článok X.
Doručovanie

1. Všetky oznámenia, žiadosti a iné písomnosti, ktorých doručenie druhej Zmluvnej strane predpokladá táto Zmluva musia byť urobené v písomnej forme a doručené druhej Zmluvnej strane e-mailom, osobne, kuriérom alebo doporučenou poštou na adresu uvedenú v záhlaví tejto Zmluvy, ak príslušné ustanovenia tejto Zmluvy nevyžadujú doručenie listiny konkrétnym spôsobom.

2. Tieto oznámenia, žiadosti a iné písomnosti podľa predchádzajúceho odseku tohto článku tejto Zmluvy sa považujú za doručené:
   a) dňom ich prevzatia adresátom, alebo,
   b) dňom odmietnutia ich prevzatia adresátom, čo musí byť na písomnosti (zásielke) vyznačené, alebo
   c) dvadsiatym dňom odo dňa ich zaslania adresátovi, a to aj v prípade, ak sa adresát o obsahu zásielky nedozvie, alebo
   d) v prípade e-mailu dňom nasledujúcim po dni, kedy bol e-mail odoslaný, ak odosielateľ neobdržal správu o nedoručiteľnosti e-mailu.

3. Zmluvná strana doručuje oznámenia, žiadosti a iné písomnosti na adresu sídla druhej Zmluvnej strany uvedenú v záhlaví tejto Zmluvy, pokiaľ táto Zmluvná strana písomne neoznámi zmenu svojej adresy druhej Zmluvnej strane.

Článok XI.
Záverečné ustanovenia

1. Postúpenie pohľadávok Poskytovateľa podľa § 524 a nasl. Zákona č.40/1964 Zb. Občiansky zákonník v znení neskorších predpisov(ďalej len ,,Občiansky zákonník") bez predchádzajúceho súhlasu Objednávateľa je zakázané. Právny úkon, ktorým budú postúpené pohľadávky Poskytovateľa v rozpore s dohodou Objednávateľa a Poskytovateľa podľa predchádzajúcej vety bude podľa § 39 Občianskeho zákonníka neplatné.

2. Akceptácia ručiteľského vyhlásenia podľa § 303 a nasl. Zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov zo strany Poskytovateľa je bez predchádzajúceho súhlasu Objednávateľa zakázaná. Právny úkon, ktorým Poskytovateľ akceptuje ručiteľské vyhlásenie tretej osoby, na základe ktorého sa tretia osoba stane objednávateľovým veriteľom v rozpore s dohodou Objednávateľa a Poskytovateľa podľa predchádzajúcej vety bude podľa § 39 Zákona č.40/1964 Zb. Občiansky zákonník v znení neskorších predpisov neplatné.

3. Poskytovateľ poskytne Objednávateľovi v pdf formáte revidovanú zmluvu pre účel zverejnenia v CRZ.

4. Táto Zmluva predstavuje konečnú dohodu Zmluvných strán o všetkých záležitostiach v nej obsiahnutých.

5. Zmluvné strany vyhlasujú, že sa podrobne oboznámili s obsahom tejto Zmluvy pred jej podpisom, vyhlasujú, že obsahu Zmluvy porozumeli, že Zmluva bola uzavretá na základe ich slobodnej a vážnej vôle a že Zmluva nebola uzavretá v tiesni alebo za nápadne nevýhodných podmienok.

6. Zmluvu je možné meniť alebo dopĺňať len písomnými a číslovanými dodatkami, podpísanými Zmluvnými stranami.

7. Na práva a povinnosti neupravené touto Zmluvou sa vzťahujú príslušné ustanovenia Obchodného zákonníka.

8. V prípade, že sa niektoré ustanovenie tejto Zmluvy stane neplatným alebo neúčinným, neznamená to, že celá Zmluva stráca platnosť. V takom prípade sa Zmluvné strany dohodli, že nájdu formulácie a znenie čo najviac podobné pôvodnému zámeru a nahradia ho tak, aby bol zachovaný účel a cieľ tejto Zmluvy.

9. Táto Zmluva nadobúda platnosť dňom jej podpisu oboma Zmluvnými stranami a účinnosť v súlade s ust. § 5a zák. č. 211/2000 Z.z. o slobode informácií v spojení s ust. §47a zák. č. 40/1964 Zb. Občiansky zákonník, dňom nasledujúcim po dni jej zverejnenia.

10. Táto zmluva je vyhotovená v dvoch (2) rovnopisoch s povahou originálu pre každý z nich, po jednom (1) pre každú Zmluvnú stranu.

V Nových Zámkoch, dňa

Za objednávateľa:

.....
FNsP NZ
MUDr.Karol Hajnovič- riaditeľ

V Liptovskom Mikuláši,
dňa

Za poskytovateľa:

.....
AXENTA s.r.o
Ing. Ján Lichvár, konateľ

Príloha č.1

Špecifikácia služby:

- Inštalácia, implementácia služby – počas implementačnej fázy
- - Zber a archivácia logov s retenciou:

○ online – 100 dní
○ offline – 200 dní (nad rámec online) ○ Hunting
○ Reporting

- - Ticketing (evidencia a spustenie Incident Response)
- - Centrálny dashboard
- - Dostupnosť služby 8x5
- - Služby **ACREDITED AXENTA CSIRT** tímu.

https://www.trusted-introducer.org/directory/teams/axenta-csirt.html

Návrhy riešenia

Komplexné nasadenie bezpečnostného monitoringu:

1. Služba **AXENTA CyberSOC**
Návrh je postavený na produktoch, ktoré sú štandardne využívané v Slovenskej a Českej republike,

majú dostatočné zastúpenie a certifikovanú podporu partnerov:

- Vulnerability managment
- LM
- Ticketing – Best Practical Request Tracker for Incident Response

On-premise

LM

Vzhľadom na veľkosť spoločnosti (z pohľadu objemu logov – 360 EPS) je LM realizovaný v podobe All-In-One appliance, ktorá môže byť v podobe SW/Virtual alebo HW. Centrálna konzola zabezpečuje detekciu, vyhodnotenie a reporting zozbieraných logov.

LM - licenčný model
Analýza, zber, transport, uloženie logov z prostredia, ich filtrovanie, korelácia, parsing na eventy,
a taktiež preposielanie / integrácia so SIEMom tak aby tvorili komplexné riešenie pre bezpečnostný monitoring v súlade s požiadavkami NBU. Log Management neobsahuje funkcionality pre monitoring bezpečnosti – neobsahuje korelačné mechanizmy pre real-time (near-real time) detekciu bezpečnostných udalostí (tie obsahuje SIEM). **Cena je závislá od počtu spracovaných logových udalostí (auditné záznamy/logy) za jednotku času, typicky EPS (Events Per Second).**

Archivácia/retencia logov v rozsahu minimálne 200dní (6+ mesiacov).

Low-level architektúra / sizing

- Počet zdrojov logov ○ 75
- Počet logov

○ 360 EPS
• Objem logov na disku (celkovo 200 dní)

○ 800 GB ONLINE (100 dní)
○ 3,2 TB OFFLINE (200 dní) nad rámec online

Štruktúra ceny za licencie

• LM=360EPS • NODES=1ks

VA/VM

RAPID 7 InsightVM je moderný nástroj, ktorý je založený na on-premise filozofii (s možnosťou rozšírenia o cloudové funkcionality ako kontajnery a externé scany), agenti pre samotný VA sken sa nasadzujú podľa potreby do on-premise prostredí alebo do cloudu a centrálny management beží ako on-premise server. Agenti pre externé zariadenia (napr. notebooky) sa ovládajú cez centrálny management v cloude, ktorý odosiela dáta do centrálnej konzoly (on-premise server). Samozrejmosťou je pokročilé API, ktoré bude integrované na jednotlivé komponenty bezpečnostného monitoringu.

Odporúčanie je robiť VA raz za mesiac a taktiež penetračné testovanie raz ročne. Výstupy z VA nástroja je nutné spracovať v rámci procesu riadenia zraniteľností (Vulnerability and Patch Management). Vulnerability Assessment a Vulnerability Management je možné realizovať v podobe služby od prevádzkovateľa SOC a Patch Management realizuje IT.

VA - licenčný model
Cena VA riešenia sa odvíja od počtu skenovaných IP adries VA/VM nástrojom. Štandardné

VA/VM nástroje majú licenciu v „pásmach“ po stovkách až tisícoch.

Low-level architektúra / sizing

• Počet IP adries pre skenovanie ○ 75

Štruktúra ceny za licencie
Rapid7 **InsightVM** je licencovaný produkt. Spôsob licencovania:

- Počet IP adries.
- Licencia je v podobe subscription, teda ročných poplatkov za službu (takto sú licencované všetky

  VA/VM produkty).

  Security Ticketing
  Navrhujeme využiť open source nástroj **Request Tracker** (RT) od spoločnosti Best

Practical, nakoľko tento produkt je plne konfigurovateľný a ohýbateľný, ale hlavne poskytuje Incident Response postupy v rámci rozšírenia **Request Tracker for Incident Response** (RTIR).

V tomto návrhu ide o štandardný ticketing nástroj, ktorý je modifikovaný a prispôsobený na plnenie špecifických požiadaviek evidencie a spracovania bezpečnostných udalostí / incidentov a prepojenia s Jednotným informačným systémom kybernetickej bezpečnosti NBÚ SR (ďalej JIS KB).

Ticketing - Licenčný model

Ticketing nástroj RT / RTIR je open source produkt pod licenciou GNU GLPv2, platená je len dobrovoľná podpora v podobe ročného poplatku. Existujú tri rôzne úrovne podpory, ktoré sa od seba odlišujú rozsahom služieb:

• BASIC

- Email Support
- Product Bug Triage and Handling
- Advanced Security Notifications **Low-level architektúra / sizing**

RTIR je prevádzkovaný ako klasický server vo virtuálnom prostredí, beží nad CENTOS 7: • RT maintenance / support – BASIC subscription