Smlouva na zajištění dodávky a implementace skeneru zranitelností

kterou podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**"), za přiměřeného použití § 2358 a násl. občanského zákoníku a § 2586 a násl. občanského zákoníku, níže uvedeného dne, měsíce a roku uzavřely tyto smluvní strany:

I.

Smluvní strany

1. Jihomoravský kraj

Sídlo:	Žerotínovo náměstí 3, 601 82 Brno
IČO:	70888337
DIČ:	CZ70888337
Zastoupený:	Mgr. Janem Grolichem, hejtmanem Jihomoravského kraje
Kontaktní osoba ve věcech smluvních:	Mgr. Martin Koníček, vedoucí odboru kancelář ředitele Krajského úřadu Jihomoravského kraje telefon: 541 651 261 e-mail: konicek.martin@jmk.cz

(dále jen „**objednatel**")

a

2.

Obch. firma/název/jméno:	**AXENTA a.s.**
Sídlo:	Mlýnská 326/13, Trnitá, 602 00 Brno
IČO:	28349822
DIČ:	CZ28349822
Zastoupený:	Ing. Lukášem Přibylem, předsedou představenstva
Zapsán v:	obchodním rejstříku vedeném Krajským soudem v Brně pod sp.zn. B 5888
Bankovní spojení:	4291128001/5500
Kontaktní osoba:	Ing. Lukáš Přibyl, předseda představenstva telefon: [redacted] e-mail:

(dále jen „**dodavatel**")

Další kontaktní osoby a spojení na objednatele:

- **Kontaktní osoba ve věcech technických:** Ing. Aleš Staněk, vedoucí oddělení Kybernetické operační centrum odboru kancelář ředitele Krajského úřadu Jihomoravského kraje, telefon: 541 658 903, e-mail: stanek.ales@jmk.cz
- **RT-IR ticketovací portál:** www.koc.kr-jihomoravsky.cz

Další kontaktní osoby a spojení na dodavatele:

A. Realizační tým:

- **Architekt:**
- **Specialista č. 1:**
- **Specialista č. 2:**
- **Specialista č. 3:**

[redacted]

B. Servisní kanály: Telefonicky na číslech: [redacted]
E-mailem na adrese: [redacted]

II.
Úvodní ustanovení

1. Tato smlouva je uzavřena na základě výsledků zadávacího řízení na nadlimitní veřejnou zakázku na služby s názvem **„Skener zranitelností“** (dále jen „**veřejná zakázka**“), která byla zadávána v souladu s ustanovením § 56 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“). Jednotlivá ustanovení této smlouvy i jejích příloh budou vykládána v souladu se zadávacími podmínkami předmětné veřejné zakázky.
2. Dodavatel výslovně prohlašuje, že je oprávněn k přijetí všech závazků vyplývajících z této smlouvy, že disponuje odbornými předpoklady pro řádné plnění předmětu této smlouvy a že vlastní potřebné certifikační a partnerské úrovně jednotlivých výrobců pro potřeby odborné realizace předmětu této smlouvy.
3. Objednatel má zájem na dodání předmětu dle této smlouvy v souladu se zásadami společensky odpovědného veřejného zadávání (dále jen „**SOVZ**“) a dbá o to, aby při plnění této smlouvy byly striktně dodržovány veškeré relevantní právní předpisy, zejména pracovněprávní předpisy.

III.
Účel smlouvy

Účelem této smlouvy je zajistit objednateli dodávku, implementaci a podporu softwarového řešení, které v objednatelem stanovených sítích jednotlivých organizací zavede a zvýší schopnost objednatele detekovat kybernetické bezpečnostní hrozby a zranitelnosti a reagovat na ně.

IV.
Předmět smlouvy

1. Předmětem této smlouvy je závazek dodavatele zajistit následující plnění:
   a) dodávka a implementace skeneru zranitelností („Vulnerability Management“) pro 14 oddělených sítí níže uvedených organizací včetně zaškolení odpovědných osob;
   b) technická podpora dodavatele;
   c) maintenance;

   (dále společně jen „**předmět plnění**“).

   Součástí předmětu plnění je i předání veškeré potřebné dokumentace, která se k předmětu plnění vztahuje.

   Podrobná specifikace všech částí předmětu plnění je uvedena v příloze č. 1 této smlouvy – technická specifikace – popis řešení dodavatele, a v příloze č. 2 této smlouvy – technické podmínky.
2. Součástí předmětu plnění jsou i činnosti v předchozím článku smlouvy výslovně nespecifikované, které jsou však k řádnému poskytnutí předmětu plnění nezbytné a o kterých dodavatel vzhledem ke své kvalifikaci a zkušenostem měl, nebo mohl vědět. Provedení těchto činností nezvyšuje smlouvou sjednanou cenu za poskytnutí předmětu plnění.
3. Dodávka předmětu plnění bude určena pro oddělené sítě níže uvedených organizací:
   - Nemocnice TGM Hodonín, příspěvková organizace, IČO: 00226637, se sídlem Purkyňova 2731/11, 695 01 Hodonín,
   - Nemocnice Ivančice, příspěvková organizace, IČO: 00225827, se sídlem Široká 390/16, 664 91 Ivančice,
   - Nemocnice Kyjov, příspěvková organizace, IČO: 00226912, se sídlem Strážovská 1247/22, 697 01 Kyjov,
   - Nemocnice Tišnov, příspěvková organizace, IČO: 44947909, se sídlem Purkyňova 279, 666 01 Tišnov,

- Nemocnice Letovice, příspěvková organizace, IČO: 00387134, se sídlem Pod Klášterem 55/17, 679 61 Letovice,
- Nemocnice Vyškov, příspěvková organizace, IČO: 00839205, sídlem Purkyňova 235/36, Nosálovice, 682 01 Vyškov,
- Nemocnice Znojmo, příspěvková organizace, IČO: 00092584, se sídlem MUDr. Jana Janského 2675/11, 669 02 Znojmo,
- Nemocnice Břeclav, příspěvková organizace, IČO: 00390780, se sídlem U Nemocnice 3066/1, 690 02 Břeclav,
- Nemocnice Hustopeče, příspěvková organizace, IČO: 04212029, se sídlem Brněnská 716/41, 693 01 Hustopeče,
- Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace, IČO: 00346292, se sídlem Kamenice 798/1d, 625 00 Brno,
- Správa a údržba silnic Jihomoravského kraje, příspěvková organizace, IČO: 70935581, se sídlem Žerotínovo náměstí 449/3, Veveří, 602 00 Brno,
- Moravian Science Centre Brno, příspěvková organizace, IČO: 29319498, se sídlem Křížkovského 554/12, Pisárky, 603 00 Brno,

  (dále společně jen jako „***POJMK***“),
- Krajský úřad Jihomoravského kraje (dále jen „***KrÚJMK***“),
- oddělení Kybernetické operační centrum odboru kancelář ředitele Krajského úřadu Jihomoravského kraje (jeho IT infrastrukturu) (dále jen „***KOC***“),

(dále společně také jen jako „***organizace***“).

4. Zadavatel si v souladu s ustanovením § 100 odst. 3 ZZVZ vyhrazuje možnost využití jednacího řízení bez uveřejnění spočívající v poskytnutí nových služeb dodavatelem, tedy spočívající ve změně závazku z této smlouvy (dále jen „***opční právo***“) v rozsahu a za podmínek níže uvedených:

   4.1. Předmětem opčního práva je oprávnění objednatele zakoupit funkční řešení dle odst. 1 až 2 tohoto článku pro až 10 nových organizací v kategorii A, B, C dle potřeb objednatele tak, aby nově zakoupená řešení byla plně funkční po zbývající dobu trvání této smlouvy.

   4.2. Využití opčního práva je výlučným právem objednatele. Objednatel je oprávněn dle své úvahy opční právo zcela nevyužít, využít ho postupně, popř. využít jen jeho část.

   4.3. Objednatel realizuje opční právo odesláním písemné výzvy dodavateli v souladu se ZZVZ a za podmínek stanovených touto smlouvou.

   4.4. Právo opce je objednatel oprávněn využít tak, aby výzva k uplatnění opčního práva byla dodavateli doručena nejpozději do 3 let ode dne uzavření této smlouvy. V případě, že objednatel právo opce v této době nevyužije, toto právo zaniká. V daném případě nemá dodavatel nárok na jakoukoliv finanční kompenzaci související s nevyužitým opčním právem.

   4.5. V případě využití opčního práva nesmí skutečná cena za poskytnutí nových služeb bez DPH přesáhnout 30% ceny za poskytnutí předmětu plnění dle této smlouvy, ani o více než 30 % přesáhnout předpokládanou hodnotu vyhrazené změny závazku uvedenou v zadávací dokumentaci veřejné zakázky, na základě které byla uzavřena tato smlouva.

5. Za dodaný předmět plnění se objednatel zavazuje zaplatit dodavateli cenu dle čl. VI. odst. 1 této smlouvy.

V.
Doba a místo plnění

1. Sken zranitelností je pořizován na 4 roky od jeho implementace.
2. Dodavatel se zavazuje předat objednateli předmět plnění takto:
   a. část předmětu plnění dle čl. IV. odst. 1 písm. a) nejpozději ve lhůtě do 3 měsíců od účinnosti smlouvy;
   b. část předmětu plnění dle čl. IV. odst. 1 písm. b) a c) pak v průběhu doby dle odst. 1 tohoto článku smlouvy.
3. Místem plnění dle této smlouvy je zejména budova sídla objednatele na adrese Žerotínovo nám. 3, 601 82 Brno, a sídla PO JMK. Smluvní strany předpokládají také plnění prostřednictvím vzdáleného přístupu.

VI.
Cena za poskytnutí předmětu smlouvy

1. Cena za předmět plnění dle této smlouvy je uvedena v příloze č. 3 smlouvy – Rozpočtu.
2. V ceně za předmět plnění jsou zahrnuty veškeré náklady, rizika a zisk dodavatele.
3. Cenu za část předmětu plnění dle čl. IV. odst. 1 písm. b) a c) této smlouvy je dodavatel oprávněn upravit (zvýšit nebo snížit), o procentuální hodnotu, o níž míra inflace vyjádřená přírůstkem průměrného ročního indexu spotřebitelských cen zveřejněná Českým statistickým úřadem za předchozí kalendářní rok přesáhne 3 %, resp. -3 % v případě deflace. Upravenou výši cen oznámí dodavatel objednateli písemně nejpozději do 30. června příslušného kalendářního roku, v němž ke změně cen v souladu s tímto článkem smlouvy dochází. Budou-li splněny podmínky podle tohoto odstavce smlouvy, bude úprava (zvýšení nebo snížení) ceny platná a účinná vždy od 1. července příslušného kalendářního roku, počínaje 1. 7. 2025.
4. Dodavatel prohlašuje, že:
   - nemá v úmyslu nezaplatit DPH u zdanitelného plnění podle této smlouvy,
   - nejsou mu známy skutečnosti nasvědčující tomu, že se dostane do postavení, kdy nemůže daň zaplatit a ani se ke dni podpisu této smlouvy v takovém postavení nenachází,
   - nezkrátí daň nebo nevyláká daňovou výhodu.

VII.
Platební podmínky

1. Cena za předmět plnění dle této smlouvy bude objednatelem uhrazena takto:
   a. cena za část předmětu plnění dle čl. IV. odst. 1 písm. a) této smlouvy bude uhrazena po předání této části předmětu plnění [viz čl. V. odst. 2 písm. a) této smlouvy];
   b. cena za část předmětu plnění dle čl. IV. odst. 1 písm. b) této smlouvy bude hrazena měsíčně dle počtu skutečně využitých MD technické podpory v daném kalendářním měsíci;
   c. cena za část předmětu plnění dle čl. IV. odst. 1 písm. c) této smlouvy bude hrazena ročně po předání příslušné části předmětu plnění na základě předchozího požadavku objednatele, a to ve výši nabídnuté ceny za maintenance za všechny organizace na 1 rok, nebyla-li již cena za poskytnutí maintenance ve 2. – 4. roce trvání smlouvy zhotovitelem zahrnuta v ceně dle čl. VII. odst. 1 písm. a) této smlouvy.
2. Objednatel neposkytuje zálohy na úhradu ceny.

3. Podkladem pro zaplacení ceny za předmět plnění je daňový doklad – faktura, kterou je dodavatel oprávněn vystavit objednateli nejpozději do 15 kalendářních dnů od předání a převzetí příslušné části předmětu plnění. Přílohou faktury bude objednatelem potvrzený předávací protokol dle čl. VIII. této smlouvy.
4. Splatnost daňového dokladu je 30 dnů ode dne jeho doručení objednateli. Faktury dodavatel doručí objednateli v elektronické formě do datové schránky (ID: x2pbqzq) nebo e-mailem na adresu posta@jmk.cz.
5. Daňový doklad musí obsahovat veškeré zákonné náležitosti daňového dokladu dle obecně závazných právních předpisů, zejména dle občanského zákoníku a dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
6. Objednatel si vyhrazuje právo před uplynutím lhůty splatnosti vrátit daňový doklad dodavateli, pokud neobsahuje požadované náležitosti nebo obsahuje nesprávné údaje. Oprávněným vrácením daňového dokladu přestává běžet původní lhůta splatnosti. Opravená nebo přepracovaná faktura bude opatřena novou lhůtou splatnosti.

VIII.
Předání a převzetí předmětu plnění

O předání a převzetí předmětu plnění dle čl. IV. odst. 1 písm. a) až c) této smlouvy bude vždy vyhotoven předávací protokol podepsaný oběma smluvními stranami. Bude tak vyhotoven protokol po předání a převzetí části předmětu plnění uvedené v čl. IV. odst. 1 písm. a) této smlouvy (dodávka a implementace skeneru zranitelností včetně zaškolení odpovědných osob), následně jedenkrát měsíčně protokol po předání a převzetí části předmětu plnění uvedeného v čl. IV. odst. 1 písm. b) této smlouvy (zajištění technické podpory) a případně jednou ročně protokol po předání a převzetí části předmětu plnění uvedeného v čl. IV. odst. 1 písm. c) této smlouvy (maintenance na navazující roky trvání smlouvy).

IX.
Práva a povinnosti smluvních stran

1. Plnění předmětu smlouvy bude na straně dodavatele provádět realizační tým ve složení stanoveném touto smlouvou a prostřednictvím kterého dodavatel prokazoval kvalifikaci v zadávacím řízení na veřejnou zakázku. Změna člena realizačního týmu je možná
    a. pouze za osobu splňující požadovanou odbornou kvalifikaci, a zároveň
    b. po předchozím písemném schválení objednatelem.

    Na změnu poddodavatele se tento odstavec použije obdobně. Změna není změnou této smlouvy, a není proto potřeba uzavírat dodatek k ní.
2. Smluvní strany se zavazují poskytovat si potřebnou součinnost, vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.
3. Dodavatel se zavazuje poskytnout předmět plnění způsobem a v rozsahu stanoveném touto smlouvou včetně příloh, zadávací dokumentací k veřejné zakázce a nabídkou dodavatele předloženou v rámci zadávacího řízení veřejné zakázky.
4. Dodavatel je povinen plnit své povinnosti dle této smlouvy včas a v řádné kvalitě.
5. Dodavatel je povinen dodržovat obecně závazné předpisy a technické normy a je povinen postupovat s náležitou odbornou péčí a profesionálně.
6. Dodavatel je povinen chránit zájmy objednatele a včas jej písemně upozorňovat na všechny hrozící vady předmětu plnění či potencionální ohrožení doby plnění.
7. Dodavatel odpovídá v průběhu poskytování za škody způsobené porušením svých povinností

dle této smlouvy. Dodavatel je povinen počínat si tak, aby v rámci své činnosti nezpůsobil objednateli škodu nebo nepoškodil dobré jméno objednatele.

8. Dodavatel je povinen při plnění této smlouvy spolupracovat v intencích požadavků objednatele se třetími stranami a dodavateli jiného plnění ve prospěch objednatele, pokud plnění těchto osob souvisí s účelem či předmětem této smlouvy.

9. V případě, že vinou dodavatele dojde ke ztrátě či znehodnocení licence, jdou veškeré náklady na znovuobnovení či pořízení nové licence za dodavatelem.

10. Dodavatel nemůže bez předchozího písemného souhlasu objednatele postoupit svá práva, závazky a povinnosti plynoucí ze smlouvy třetí osobě.

11. Dodavatel se zavazuje komunikovat pouze s kontaktní osobou na straně objednatele, není-li dohodnuto jinak.

12. Dodavatel je povinen zajistit dodržování pracovněprávních předpisů, zejména zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci odměňování, pracovní doby, doby odpočinku mezi směnami, atp.), zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci zaměstnávání cizinců), a to vůči všem osobám, které se na předmětu plnění podílejí, a bez ohledu na to, zda jsou práce prováděny bezprostředně dodavatelem či jeho poddodavateli.

13. Dodavatel je povinen zajistit řádné a včasné plnění finančních závazků svým případným poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem řádně vystavených a doručených faktur za plnění poskytnutá k plnění veřejné zakázky, a to vždy do 5 pracovních dnů od obdržení platby ze strany objednatele za konkrétní plnění.

14. Dodavatel je povinen zajistit sjednání a dodržování smluvních podmínek se svými případnými poddodavateli srovnatelnými s podmínkami sjednanými v této smlouvě, a to zejména v rozsahu výše smluvních pokut a délky záruční doby. Smluvní podmínky se považují za srovnatelné, bude-li výše smluvních pokut a délka záruční doby shodná se zněním této smlouvy.

15. Dodavatel se zavazuje při plnění předmětu této smlouvy dodržovat povinnosti stanovené v odst. 12., 13. a 14. tohoto článku smlouvy. Objednatel je oprávněn plnění těchto povinností kdykoliv kontrolovat, a to i bez předchozího ohlášení dodavateli. Je-li k provedení kontroly potřeba předložení dokumentů, zavazuje se dodavatel k jejich předložení nejpozději do 2 pracovních dnů od doručení výzvy objednatele.

X.
Licenční ujednání

1. Dodavatel poskytuje objednateli jako součást předmětu plnění dle této smlouvy licenci k software (dále jen „licence“), který podléhá ochraně dle zákona č. 121/2000 Sb., o právu autorském, o ochraně práv souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

2. Dodavatel poskytuje objednateli nevýhradní licenci k veškerým známým způsobům užití software, zejména, nikoliv však výlučně, k účelu, ke kterému byl vytvořen v souladu se smlouvou, a to v rozsahu minimálně nezbytném pro řádné užívání předmětu plnění dle této smlouvy objednatelem. Jedná se o licenci neomezenou územním rozsahem a dále způsobem nebo rozsahem užití.

3. Licenci je převoditelná a postupitelná, tj. je udělena s právem udělení bezúplatné podlicence či postoupení třetí osobě. Objednatel není povinen licenci využít.

4. Součástí poskytnutého rozsahu licenčních oprávnění je i právo objednatele předmět plnění provozovat za využití osob (dodavatelů) dalších odlišných od dodavatele.

5. Objednatel a dodavatel se výslovně dohodli, že odměna za užití licence je již zahrnuta v ceně za předmět plnění uvedené v čl. VI. odst. 1 této smlouvy.

XI.
Smluvní sankce a náhrada škody

1. Bude-li objednatel v prodlení s úhradou sjednané ceny, je dodavatel oprávněn účtovat objednateli úrok z prodlení ve výši 0,05 % z dlužné částky v Kč bez DPH za každý započatý den prodlení až do doby zaplacení dlužné částky, a objednatel se zavazuje takto účtovaný úrok z prodlení zaplatit.
2. Bude-li dodavatel v prodlení s termínem plnění dle čl. V. odst. 2 písm. a) této smlouvy, je objednatel oprávněn požadovat po dodavateli zaplacení smluvní pokuty ve výši 1.500, - Kč za každý započatý den prodlení a dodavatel se zavazuje takto požadovanou smluvní pokutu zaplatit.
3. Objednatel je oprávněn požadovat po dodavateli za porušení povinnosti stanovené v čl. XVI. odst. 1 této smlouvy (povinnost ochrany informací a mlčenlivosti) nebo za porušení povinnosti stanovené v čl. IX. odst. 1 této smlouvy (povinnost provádět plnění předmětu smlouvy prostřednictvím realizačního týmu ve složení stanoveném touto smlouvou) zaplacení smluvní pokuty ve výši 50.000,- Kč za každý jednotlivý případ porušení povinnosti a dodavatel se zavazuje takto požadovanou smluvní pokutu zaplatit.
4. Smluvní pokuty sjednané touto smlouvou zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé straně škoda, kterou lze vymáhat samostatně.
5. Smluvní pokuty a úroky z prodlení jsou splatné do 15 dnů ode dne, kdy povinná strana obdrží písemnou výzvu k zaplacení smluvní pokuty nebo úroku z prodlení, která bude obsahovat jejich vyčíslení. Zaplacením smluvní pokuty nebo úroku z prodlení nejsou dotčena práva na náhradu škody v plné výši.
6. Smluvní strany se zavazují jednat tak, aby nedocházelo ke škodám. Smluvní strany se zároveň dohodly, že ustanovení § 2050 občanského zákoníku se nepoužije. Objednateli náleží i přes sjednání smluvní pokuty právo na náhradu škody vzniklé porušením povinnosti, ke které se smluvní pokuta vztahuje.

XII.
Pojištění

1. Dodavatel se zavazuje uzavřít pojistnou smlouvu mezi pojišťovnou a dodavatelem v postavení pojištěného na pojištění rizik a odpovědnosti za škody způsobené vlivem vadného plnění dodaného dle této smlouvy s jednorázovým pojistným plněním minimálně ve výši 5.000.000 Kč za jednu pojistnou událost. Dodavatel se zavazuje udržovat uvedené pojištění v platnosti po celou dobu trvání této smlouvy, jakož i po celou dobu trvání závazků z této smlouvy vyplývajících (tj. i po dobu trvání technické podpory, i v případě využití opčního práva).
2. Náklady na pojištění nese dodavatel a jsou zahrnuty ve sjednaných cenách dle této smlouvy.
3. Prostou kopii dokladu o uzavření pojistné smlouvy je dodavatel povinen předložit objednateli nejpozději do 3 dnů ode dne účinnosti této smlouvy. V případě změny pojištění předloží dodavatel bezodkladně objednateli nový doklad prokazující uzavření příslušné pojistné smlouvy.
4. Skutečnost, že dodavatel řádně a včas neuzavře nebo neprodlouží pojistnou smlouvu nebo řádně a včas objednateli nepředloží doklad o jejím uzavření, jak je požadováno touto smlouvou, bude považována za podstatné porušení smlouvy na straně dodavatele.
5. Dodavatel se zavazuje uplatnit veškeré pojistné události související s poskytováním plnění dle této smlouvy u pojišťovny bez zbytečného odkladu.

XIII.
Záruka a odpovědnost za vady, podpora provozu předmětu plnění

1. Dodavatel poskytuje záruku za funkčnost dodaného systému po celou dobu platnosti smlouvy.
2. Dodavatel odpovídá za vady, které má předmět plnění v době převzetí a za vady, které se projeví v záruční době, popřípadě v důsledku škody, za kterou odpovídá dodavatel.

3. Veškeré vady předmětu plnění je objednatel oprávněn reklamovat u dodavatele kdykoliv po zjištění vady během záruční doby, a to formou písemného oznámení, obsahujícího specifikaci zjištěné vady nebo popis, jak se vada projevuje.

4. Objednatel je oprávněn uplatnit veškerá zákonná práva z vadného plnění. Volba práva z vadného plnění je věcí objednatele. Neuvede-li objednatel, jaké právo v souvislosti s vadou předmětu plnění uplatňuje, má se za to, že požaduje odstranění vady, tj. provedení opravy předmětu plnění nebo jeho části.

5. Dodavatel je povinen zahájit proces vedoucí k odstranění vady nejpozději druhý pracovní den od doručení oznámení o vadě.

6. Záruční doba neběží po dobu, po kterou nemohl objednatel předmět plnění užívat pro vady, za které dodavatel zodpovídá.

7. Uplatněním práva z vadného plnění není dotčen nárok objednatele na náhradu škody.

XIV.
Vyšší moc

1. Pro účely této smlouvy se za vyšší moc považují okolnosti, které objektivně znemožňují některé ze smluvních stran dočasně či trvale plnit některou z povinností podle této smlouvy, nejsou závislé na vůli smluvních stran a ani nemohou být smluvními stranami ovlivněny či překonány, přičemž smluvní strany nemohly s vynaložením odborné péče takovou okolnost zjistit ani předvídat před uzavřením smlouvy.

2. Za mimořádné nepředvídatelné a nepřekonatelné okolnosti smluvní strany považují zejména válečný či ozbrojený konflikt, akty či hrozby terorismu, občanské nepokoje, povstání, mobilizaci, přírodní katastrofy (např. povodně, přílivové vlny, požáry, výbuchy, zemětřesení), masivní výpadek elektrické energie nebo dodávek ropy, embargo, epidemie nebo jinak významné události, v jejichž důsledku bude smluvní strana z faktických důvodů, ze zákona či na základně opatření orgánu veřejné moci nucena zastavit, přerušit či podstatně omezit plnění smluvních povinností.

3. Pokud v důsledku vyšší moci nemůže smluvní strana plnit své smluvní povinnosti, je povinna o tom informovat druhou smluvní stranu neprodleně poté, co se o vzniku této okolnosti dozvěděla nebo se mohla dozvědět s vynaložením odborné péče. Současně je taková smluvní strana povinna specifikovat smluvní povinnosti, v jejichž plnění jí v důsledku vyšší moci je nebo bude bráněno, a prokázat příčinnou souvislost mezi překážkou vyšší moci a neplněním smluvní povinnosti.

4. Smluvní strana, které vyšší moc zabránila v řádném a včasném plnění smluvní povinnosti, je povinna učinit vše, co je v jejích silách, aby odvrátila či minimalizovala újmu vzniklou druhé smluvní straně z důvodu, že smluvní strana odvolávající se na vyšší moc není schopna plnit svou povinnost.

5. Za vyšší moc se pro účely této smlouvy nepovažuje překážka vzniklá z poměrů smluvní strany, která se překážky vyšší moci dovolává, nebo překážka vzniklá v době, kdy byla tato smluvní strana v prodlení s plněním smluvní povinnosti, ani překážka, kterou byla tato smluvní strana podle této smlouvy povinna překonat.

6. Brání-li smluvní straně v řádném a včasném splnění smluvní povinnosti vyšší moc a tato smluvní strana splnila své povinnosti podle odstavce 3. tohoto článku smlouvy, je oprávněna se domáhat prodloužení lhůty ke splnění smluvní povinnosti o dobu prokázaného trvání překážky vyšší moci. Smluvní strany se zavazují o změně doby plnění uzavřít písemný dodatek k této smlouvě. Má-li se však lhůta ke splnění smluvní povinnosti prodloužit v důsledku překážky vyšší moci o více než 30 dnů oproti původně sjednanému termínu, má smluvní strana, na jejíž straně překážka vyšší moci není, právo od smlouvy odstoupit.

7. Brání-li smluvní straně v řádném a včasném splnění smluvní povinnosti vyšší moc a tato smluvní strana splnila své povinnosti podle odstavce 3. tohoto článku smlouvy, nemá druhá smluvní strana po dobu trvání překážky vyšší moci právo uplatňovat smluvní pokuty či úroky z prodlení podle této smlouvy.

XV.
Ukončení smlouvy

1. Tuto smlouvu lze ukončit dohodou smluvních stran. Dohoda o ukončení smluvního vztahu musí být písemná, jinak je neplatná.
2. Od této smlouvy lze odstoupit v případě podstatného porušení smlouvy, jestliže je toto porušení smlouvy označeno za podstatné touto smlouvou nebo zákonem. Odstoupení je účinné dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
3. Smluvní strany se dohodly, že za podstatné porušení smlouvy považují zejména:
   a. nedodržení dohodnutého předmětu plnění dodavatelem,
   b. prodlení dodavatele s dodáním plnění v termínu stanoveném v čl. V. odst. 2 písm. a) této smlouvy,
   c. poskytnutí předmětu plnění dodavatelem i přes písemné upozornění objednatele s nedostatečnou odbornou péčí v rozporu s obecně závaznými právními předpisy, technickými normami, případně v rozporu s pokyny objednatele,
   d. dodavatel změní člena realizačního týmu i přes vyjádřený nesouhlas objednatele
   e. prodlení objednatele s úhradou ceny po dobu delší než 30 dní po lhůtě splatnosti.
4. Je-li zřejmé již v průběhu plnění této smlouvy, že právní, technické, finanční či organizační změny na straně dodavatele budou mít podstatný vliv na plnění této smlouvy, může objednatel od smlouvy odstoupit.
5. Objednatel si vyhrazuje právo od smlouvy odstoupit, pokud zjistí, že dodavatel při podání nabídky na veřejnou zakázku, na základě které je uzavřena tato smlouva, uvedl nepravdivá prohlášení nebo informace za účelem získat zakázku nebo jiný majetkový prospěch.
6. Odstoupením od smlouvy nejsou dotčena ustanovení týkající se smluvních pokut, úroků z prodlení a ustanovení týkající se těch práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení (např. povinnost poskytnout peněžitá plnění za plnění poskytnutá před účinností odstoupení).

XVI.
Ochrana informací a mlčenlivost

1. Smluvní strany se zavazují, že během trvání této smlouvy i po jejím ukončení budou chránit důvěrné informace druhé smluvní strany a zachovávat mlčenlivost o všech důvěrných informacích, o kterých se dozví od druhé smluvní strany v souvislosti s plněním smlouvy.
2. Důvěrné informace na straně objednatele jsou veškeré technické informace o jeho vnitřním prostředí a technické detaily týkající se technické infrastruktury a dále takové informace, které budou za důvěrné objednatelem výslovně označeny.

XVII.
Vzdálený přístup do prostředí objednatele

1. Vzdálený přístup je poskytován výhradně konkrétním osobám dodavatele, po odsouhlasení vedoucím KOC. Seznam osob, které budou mít do systému vzdálený přístup, bude uložen v dokumentaci KOC. Dodavatel zajistí, že v případě ukončení spolupráce s osobou, která bude mít přidělen vzdálený přístup, nahlásí tuto skutečnost vedoucímu KOC a přístup bude zneplatněn. Oprávnění ke vzdálenému přístupu nelze převádět na jinou osobu. Porušení této povinnosti je podstatným porušením smlouvy.

2. Dodavatel se zavazuje, že vzdálený přístup k informačním systémům v prostředí počítačové sítě KOC na základě této smlouvy bude užívat jen za účelem dodávky a implementace předmětu plnění. Porušení této povinnosti bude považováno za podstatné porušení smlouvy.

3. Dodavatel se zavazuje postupovat při realizaci předmětu plnění tak, aby v počítačové síti KOC nezpůsobil poškození, ztrátu nebo odcizení dat. Pokud by k výše uvedenému došlo, zavazuje se dodavatel takto vzniklé závady neprodleně odstranit a nahradit objednateli veškerou škodu.

XVIII.
Závěrečná ujednání

1. Dodavatel prohlašuje, že neporušuje etické principy, principy společenské odpovědnosti ani základní lidská práva.

2. Tato smlouva a práva a povinnosti z ní vzniklé, i výslovně touto smlouvou neupravené, se řídí příslušnými ustanoveními občanského zákoníku.

3. Vzhledem k veřejnoprávnímu charakteru objednatele dodavatel výslovně souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů [zejména ZZVZ, zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**zákon o registru smluv**"), a zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů].

4. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení této smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak. Smluvní strany si současně potvrzují, že si nejsou vědomy žádných doposud mezi nimi zavedených obchodních zvyklostí či praxe.

5. Změnit nebo doplnit tuto smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány výslovně prohlášeny za dodatek této smlouvy a podepsány oprávněnými zástupci smluvních stran. Za písemnou formu pro tento účel nebude považována výměna e-mailových zpráv.

6. V případě plurality osob na straně dodavatele se tyto osoby zavazují, že budou vůči objednateli a třetím osobám z jakýchkoliv právních vztahů vzniklých v souvislosti s plněním předmětu této smlouvy zavázáni společně a nerozdílně, a to po celou dobu plnění této smlouvy, i po dobu trvání jiných závazků vyplývajících z této smlouvy.

7. Smlouva podléhá uveřejnění v registru smluv dle zákona o registru smluv. Smluvní strany se dohodly, že návrh na uveřejnění smlouvy v registru smluv podá objednatel.

8. Smlouva je uzavřena okamžikem jejího podpisu oběma smluvními stranami a nabývá účinnosti okamžikem jejího zveřejnění v registru smluv.

9. Nedílnou součást této smlouvy tvoří její přílohy:

   Příloha č. 1 – **Technická specifikace – popis řešení dodavatele**,

   Příloha č. 2 – **Technické podmínky**

   Příloha č. 3 - **Rozpočet**.

   V případě rozporu mezi přílohou č. 1 smlouvy a přílohou č. 2 smlouvy platí, že přednost mají informace uvedené v příloze č. 2 smlouvy – Technických podmínkách.

10. Tato smlouva je vyhotovena v jednom elektronickém vyhotovení podepsaném zaručenými elektronickými podpisy zástupců smluvních stran, popřípadě je vyhotovena ve dvou listinných vyhotoveních a podepsána vlastnoručně zástupci smluvních stran; každé vyhotovení má platnost originálu, přičemž každá ze smluvních stran obdrží po jednom vyhotovení.

11. Smluvní strany se s obsahem smlouvy seznámily, souhlasí s ním a po přečtení prohlašují, že byla sepsána dle jejich pravé, dobrovolné a svobodně projevené vůle v souladu s veřejným pořádkem a dobrými mravy, na důkaz čehož připojují na konec smlouvy své podpisy.

Doložka podle § 23 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů:

Tato smlouva byla schválena Radou Jihomoravského kraje usnesením č. 9932/24/R135 ze dne 17.07.2024.

Objednatel:	Dodavatel:
V Brně dne 30.07.2024	V Brně dne 24.07.2024
_____	_____
Jihomoravský kraj	**AXENTA a.s.**
Mgr. Jan Grolich	Ing. Lukáš Přibyl
hejtman Jihomoravského kraje	předseda představenstva

Příloha č. 1 smlouvy – Technická specifikace – popis řešení dodavatele

Nasazená technologie

Vulnerability management od společnosti Rapid7, a to konkrétně Rapid7 InsightVM.

Jedná se o on-premise hybridní řešení, které umožňuje nasazení on-premise, ale umožňuje taktéž využití funkcionalit, které poskytuje cloudová konzole, tak jak požaduje objednatel. Nasazení centrální správy a scaneru zranitelností je on-premise.

HW, na němž bude nasazená technologie provozována

Scan engine bude provozován na stávajícím HW. Bez rozšíření. Management konzole bude provozována na stávajícím HW v KOC, tak jej objednatel popsal.

Operační systém, na němž bude nasazená technologie provozována

UBUNTU SERVER 22.04 LTS

Bude třeba povolit následující prostupy z/do vnitřní sítě:

- KOC > PO 40814/TCP (Console to Scanner communication)
- PO > KOC 40815/TCP (Scanner to Console communication)
- KOC > public pro komunikaci řešení s update a licenčními servery výrobce je zapotřebí port 443, 80.

Jednotný přístup z/do KOC bude řešen:

SSH 22 port pro přístup na všechny PO ze strany dodavatele pro instalaci scanneru

Komunikace z/do KOC bude řešena:

Ze strany dodavatele budou použity stávající přístupové účty, které jsou využívány pro správu infrastruktury JMK KOC. Samotný produkt bude komunikovat prostřednictvím stávajících IPSEC mezi PO JMK, který je použit pro transport logů.

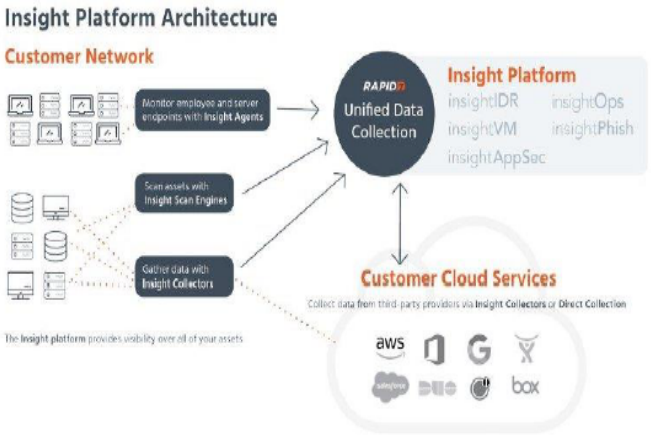
COMGUARD

RAPID7 insightVM

Rapid7 Vulnerability Management

Zneužití známé zranitelnosti je pro útočníka nejjednodušší cesta, jak proniknout do dané společnosti. S kvalitním vulnerability managementem by firmy dokázaly bezpečnostnímu incidentu plně předejít. Vulnerability Management od Rapid7 sbírá a dává v reálném čase do souvislostí rozsáhlé množství korelovaných dat a poskytuje tak podrobný přehled o zranitelnostech. Na rozdíl od tradičních skenů zranitelností nebo správy incidentů, se Rapid7 dívá na síť optikou útočníka a donutí společnost rychleji zasáhnout proti zranitelnostem, které jsou opravdovým rizikem, nejen teoretickou hrozbou.

Celé portfolio Rapid7 je spojeno do unikátní centralizované bezpečnostní platformy **Insight Platform**. Spojuje celé portfolio produktů – Xtended Detection and Response (XDR), SIEM, Threat Intelligence, ochrana cloudových aplikací a management zranitelností, včetně webových a mobilních aplikací. Insight Platform sbírá data z celého IT ekosystému a umožňuje bezpečnostním IT týmům efektivně spolupracovat při analýze sdílených dat. Produkty z řady Insight využívají jednotného agenta a kolektory a díky tomu je škálování celého řešení velmi snadné.



Rapid7 InsightVM

Rapid7 InsightVM vyhledává zranitelnosti v prostředí společnosti a pomáhá určit jejich prioritu díky tzv. Real Risk Score. Na základě pravděpodobnosti jejich zneužití navrhne optimální harmonogram aplikace záplat. Dokáže velmi úzce spolupracovat s nástrojem pro penetrační testování – Metasploit, který uchovává podrobnou znalost exploitů a pomocí něj dokáže ověřit, zda je hrozba stále aktuální. InsightVM poskytuje live management zranitelností, stejně jako analýzu koncových bodů za účelem sledování hrozeb v reálném čase. InsightVM dokáže nasbírat informace o zranitelnostech a exportovat je do jiných nástrojů v rámci Insight Platform, čímž zvyšuje bezpečnostní inteligenci celého prostředí. Poskytuje také ucelené a přehledné reporty, které mohou sloužit pro management organizace.

Real Risk Score

Real Risk Score je vlastní metodika od Rapid7, která posuzuje rizika podle teoretických hrozeb CVSS a existence reálné hrozby, např. zda již existuje exploit nebo nikoliv. Výsledkem této metriky je výrazné snížení počtu zranitelností k řešení.

Skenování

Rapid7 InsightVM usnadňuje správu zranitelností bez ohledu na to, zda spravujete tisíc nebo milion IP adres každý den. Díky skenování pomocí DHCP umožní skenování zařízení, jakmile se připojí k síti. Skenování automaticky proběhne na základě nových hrozeb s vysokou závažností. Před samotným skenováním je možné si specifikovat kritické stroje v infrastruktuře.

COMGUARD
communication security

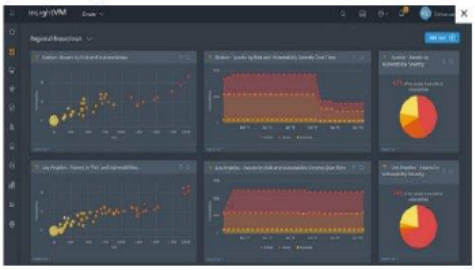
COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel: +420 513 035 400
info@comguard.cz | www.comguard.cz

COMGUARD

RAPID7

Integrace

InsightVM je velmi užitečným a bohatým zdrojem dat při kombinaci se SIEM a Firewally. Pomocí otevřeného API se dokáže snadno integrovat s více než 50 bezpečnostními technologiemi – LogRhythm, ManageEngine, McAfee Nitro Security, Amazon Web Services, ArcSight, Cisco, FireEye, Google Apps, Microsoft, Office 365, VMware a další. Integrace s Metasploit, nejpoužívanějším Frameworkem na penetrační testování na světě, poskytuje real-time detekci, které zranitelnosti systémů jsou aktuální, a u kterých se pracuje na jejich odstranění.



Klíčové vlastnosti Rapid7 InsightVM

- **Real Risk Score** – prioritizace nalezených zranitelností
- **Asset Management** – informace o nejzranitelnějších strojích
- **Remediation planning** – souhrn jednoduchých kroků, které pomohou při nápravě
- **Cílené skenování a reportování** – skenování a reportování zaměřené na určité oblasti (interní a externí síť, webové aplikace, databáze atd.)
- **Dívá se na síť z pohledu útočníka** a donutí vás zasáhnout proti hrozbě, která je opravdovým rizikem, a ne pouze teoretickou hrozbou
- **Lehký agent** pro koncové body
- **Pravidelné hodnocení sítě** – pravidelné audity zaměřené na specifické oblasti infrastruktury
- **Holistický pohled** – Poskytuje podrobné informace o nainstalovaných aplikacích na koncových zařízeních.
- Lze pořídit jak ve verzi **on-premise**, tak i pro **cloud**

	InsightVM	Nexpose
Počet administrátorů	Neomezeno	Neomezeno
Počet scanovacích enginů	Neomezeno	Neomezeno
Automatic vulnerability updates and Microsoft Patch Tuesday vulnerability updates	✓	✓
Scan scheduling and alerting	✓	✓
Basic web application scanning	✓	✓
Policy assessment (PCI, CIS, DISA, and more)	✓	✓
Advanced report and scan customization	✓	✓
RESTful API, OpenAPI, and third-party integrations	✓	✓
Dynamic discovery scanning (VMware, Mobile)	✓	✓
Dynamic, live dashboards with 50+ cards	✓	X
Endpoint agents	✓	X
Live data querying	✓	X
AWS and Microsoft Azure Support	✓	✓
Dynamic asset groups and tagging	✓	✓
Real Risk Score	✓	✓
Report templates and uploading	✓	✓
Integrated vulnerability validation with Metasploit	✓	✓
Custom tags and system criticality tags	✓	✓
Access to public and proprietary threat feeds	✓	X
Remediate		
Executive and remediation reporting	✓	✓
User role customization	✓	✓
Remediation Projects	✓	X
Automation-Assisted Patching	✓	X
Ticketing integrations (API)	✓	✓
Deployment options		
Software installation	✓	✓
Virtual appliance	✓	✓
Physical appliance	✓	✓
Private cloud	✓	✓
Managed Service	✓	✓

Tabulka: Srovnání verze InsightVM a Nexpose

Vulnerability management lze pořídit ve verzi onpremise, která je pod názvem Nexpose. A hybridní verzi InsightVM, kdy samotné nasazení agentů a skenovacího engine je on premise a live management zranitelností je napojen do cloudu.

Unikátní kombinace Rapid7 Metasploit a Real Risk Score dělá z vulnerability managementu jednotné řešení pro správu rizik a umožní organizacím **být v souladu s bezpečnostními předpisy** a audity pro Risk Management, Vulnerability a Configuration Management, jako jsou ISO 27002, PCI DSS, SNS, HIPAA, HITECH, FISMA (USGCB/FDCI a včetně SCAP shody), Sarbanes-Oxley (SOX), Top 20 CSC a NERC CIP.

insightAppSec

Rapid7 InsightAppSec je cloud-based řešení zabezpečující dynamic application security testing (DAST). Skenuje jak jednoduché, tak komplexní, interní i externí webové aplikace s cílem otestovat jejich rizikovost a poskytnout informace potřebné k případné rychlejší nápravě. Identifikuje XSS, CSRF, SQL injections a mnoho dalších zranitelností z Rapid7 knihovny, která obsahuje více než 90 typů útoků. Generuje interaktivní HTML reporty prostřednictvím Attack Replay a sdílí je s vaším vývojovým týmem a zainteresovanými stranami. DAST řešení je možné také pořídit v on-prem verzi – AppSpider Enterprise/Pro.

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel: +420 513 035 400
info@comguard.cz | www.comguard.cz

Příloha č. 2 smlouvy – Technické podmínky

Popis výchozího stavu

Jihomoravský kraj (objednatel) je zřizovatelem více než 230 příspěvkových organizací s nejrůznějším zaměřením činnosti, s různou velikostí a s dislokací po území celého kraje. Od roku 2017 jsou vybrané příspěvkové organizace postupně připojovány do bezpečnostního dohledového centra, které provozuje oddělení **Kybernetické operační centrum** odboru kancelář ředitele Krajského úřadu Jihomoravského kraje (dále jen „KOC"). KOC zajišťuje pro připojené příspěvkové organizace Jihomoravského kraje služby bezpečnostního dohledového centra.

V síti každé připojené příspěvkové organizace (dále jen „PO") je integrován server pro sběr a odesílání bezpečnostně relevantních informací z infrastruktury. Logy jsou přes VPN tunel přenášeny do KOC k automatizovanému i ručnímu vyhodnocení. Nasazení jak stávajících technologií, tak poptávané technologie skeneru zranitelností běží v distribuovaném nasazení, kde v PO dochází jenom ke sběru/skenu a předání/odeslání dat do centrálního bodu, tedy do KOC, k e zpracování.

U každé PO, na serveru (taktéž zvaném kolektor) běží KVM virtualizace a jsou tam virtualizovány jednotlivé komponenty/sběrače/analyzátory. Pro dodávku skeneru zranitelnosti je na každém kolektoru alokován prostor pro běh virtuálního serveru s OS CENTOS 7.x, na kterém bude instalována aplikace VA skeneru. Maximální výkonové parametry alokovatelné pro VA skener v PO jsou:

- 4x CORE
- 8 GB RAM
- 100 GB disk space
- OS CENTOS 7.x
- KVM virtualizace

Jestli dodavatelem navrhované řešení není možné provozovat v rámci této specifikace je možné dodat vlastní HW (i s případným podkladovým SW, jako je OS apod.) pro distribuované řešení kolektorů. V tomto případě jsou kladeny následující minimální požadavky na HW:

- 1/2U RACK server
- 2x PSU
- 4x LAN
- ILO/DRAC/IPMI mgmt + GUI console
- HDD 7200+ rpm v RAID1

Pro nasazení centrálního managementu (detektor zranitelnosti) bude poskytnut virtuální prostor v prostředí KOC na platformě VMware. Jakékoli další SW požadavky (OS, Databáze apod.) zajistí dodavatel.

Specifikace poptávaného technického řešení

Poptávané je řešení Vulnerability Managementu (v tomto dokumentu také „skener zranitelností") s podporou interního i externího (cloudového) skenování a řízení zranitelností. Požadované řešení je v podobě distribuované architektury – centrální konzola v KOC a skenovací kolektory pro PO.

V tabulce 1 je uveden seznam PO, pro které objednatel požaduje nasazení skenu zranitelnosti. Pokud bude dále popisována některá organizace, bude dále použit jen kód.

KÓD	Celkový počet assetů	Název	Adresa

NEMBV	59	Nemocnice Břeclav, příspěvková organizace	U Nemocnice 3066/1, 690 74 Břeclav
NEMHO	140	Nemocnice TGM Hodonín, příspěvková organizace	Purkyňova 11, 695 26 Hodonín
NEMHU	76	Nemocnice Hustopeče, příspěvková organizace	Brněnská 716/41, 693 01 Hustopeče
NEMIV	322	Nemocnice Ivančice, příspěvková organizace	Široká 401/16, 664 91 Ivančice
NEMKY	243	Nemocnice Kyjov, příspěvková organizace	Strážovská 1247/22, 697 01 Kyjov
NEMLE	76	Nemocnice Letovice, příspěvková organizace	Pod Klášterem 55/17, 679 61 Letovice
NEMTI	70	Nemocnice Tišnov, příspěvková organizace	Purkyňova 279, 666 01 Tišnov
NEMVY	103	Nemocnice Vyškov, příspěvková organizace	Purkyňova 235/36, 682 01 Vyškov
NEMZN	72	Nemocnice Znojmo, příspěvková organizace	MUDr. Jana Janského 2675/11, 669 02 Znojmo
ZZS	157	Zdravotnická záchranná služba Jihomoravského kraje, příspěvková organizace	Kamenice 798/1d, 625 00 Brno
SUS	515	Správa a údržba silnic Jihomoravského kraje, příspěvková organizace	Žerotínovo náměstí 449/3, 602 00 Brno
VIDA	525	Moravian Science Centre Brno, příspěvková organizace	Křížkovského 554/12, Pisárky, 603 00 Brno
KrÚ JMK	150	Krajský úřad Jihomoravského kraje	Žerotínovo náměstí 449/3, 602 00 Brno
KOC	130	Kybernetické operační centrum	Žerotínovo náměstí 449/3, 602 00 Brno
Celkem	**2638**		

Tabulka 1 – Seznam organizací pro nasazení skenu zranitelností

Dodavatel zajistí nekonfliktní instalaci na centrální server, na koncová zařízení kolektory (servery) a technické prostředky pro běh centrální serverové části. Bude zajištěn sběr dat v rámci skenů zranitelností a obousměrná komunikace mezi KOC a jednotlivými PO. Součástí služby jsou tedy všechny práce a aktivity (i s podporou produktivního provozu) pro plnohodnotné a funkční nasazení skeneru zranitelností do prostředí KOC.

Technické požadavky na řešení skenu zranitelností

Řešení musí být dodáno ve variantě on-premise (implementace na centrální server) bez nutnosti využití cloudových služeb, ale s podporou/možností provádět externí skeny z cloudového prostoru výrobce produktu (tedy externí sken je součástí řešení, ale jako služba). Tedy správa skeneru zranitelností i

aktualizace databáze zranitelností a produktu samotného musí být možné provádět z on-prem konzole bez nutnosti připojení skenerů k internetu.

Zásadním požadavkem je zajištění tzv. multitenantního provozu, kdy se všechny informace vyhodnocují v jednom centru, ale vzájemně se jednotlivé tenanty (zákazníci) neovlivňují i pokud mají stejné IP rozsahy.

Objednatel požaduje, aby nabízené řešení mělo minimálně tyto funkcionality (všechny parametry jsou povinné):

Obecné požadavky

1. Řešení musí být realizované produkty s integrovaným uživatelským rozhraním včetně dostupnosti výsledků testování, systémově a administrativně snadno ovladatelným aplikačním prostředím.
2. Řešení musí být možno provozovat centrální správu a databázi pro důvěrná data on-premise, vlastní funkcionalita sběru a vyhodnocení zranitelností musí probíhat čistě v rámci on-premise architektury.
3. Řešení musí být flexibilní = bezagentní řešení, tj. bez nutnosti instalace SW kódu na infrastrukturu ICT. Současně s možností využití agentů pro zařízení mimo síť organizace.
4. Řešení musí podporovat oddělení dat do jednotlivých tenantů a jejich separátní vyhodnocení
5. Řešení musí umožňovat periodické automatické aktualizace databáze zranitelností a testovací aplikace (scanning engine) na všech skenovacích zařízení (interních i externích v internetu) garantovaná dodavatelem s 24hod reakcí na nově popsané zranitelnosti například na stránkách výrobců SW, nebo online databází zranitelností - cve.mitre.org apod.
6. Řešení musí být integrovatelné se systémem SIEM ArcSight ESM (výstupy skenů zranitelností per asset, compliance a konfigurační policy) a VMware (dynamické discovery assetů v rámci virtuálního prostředí, součást security service NSX, pro přímý vulnerability assessments přes hypervisor, asset management, tagování VM strojů na základě úrovně zranitelnosti apod).
7. Požadujeme shodu s bezpečnostními nařízeními (ISO 27001 a ZoKB)
8. Řešení musí umožňovat přenášení dat mezi jednotlivými komponenty řešení, především mezi centrálním managementem a skenery např. o zjištěných zranitelnostech a informace o testovaných zařízeních, pouze s použitím silného šifrování a pouze v rámci LAN objednatele (včetně poboček).
9. Řešení musí umožňovat periodické automatické aktualizace databáze zranitelností a testovací aplikace (scanning engine) na všech skenovacích zařízení (interních i externích v internetu) garantovaná dodavatelem s 24hod reakcí na nově popsané zranitelnosti například na stránkách výrobců SW, nebo online databází zranitelností - cve.mitre.org apod.

Požadavky na vlastnosti skenování

1. Řešení musí umožňovat detekci zranitelností na vzdáleném ICT zařízení s podporou minimálně následujících operačních systémů:
    - Windows desktop 7+ a Windows Server 2008+, RHEL, GNU/Linux distribuce;
    - databází: Oracle, MS SQL Server, PostgreSQL;
    - routerů a switchů s podporou pro IOS, NX-OS, Comware 5 a 7 výrobců HP, Cisco;
    - aplikačních web serverů: Apache, WebSphere, MS IIS;
    - a virtualizační platformy VMware;
    - dále pak pro Simple Network Management Protocol (SNMP), Secure Shell (SSH) Public Key, Telnet, Web Site Form Authentication, Web Site HTTP Authentication, Web Site Session Authentication.
2. Řešení musí umožňovat pravidelné automatické, kontinuální (nepřetržité) i ad-hoc ruční spouštění testování zranitelností ICT zařízení v prostředí síťové infrastruktury, s možností výběru IP rozsahu nebo předdefinovaných skupin zařízení a s výběrem/úpravou profilu a zátěže testování – minimální požadovaná periodicita 1x denně přes celý IP rozsah v rámci dodávky. Řešení musí umožnit vizualizaci těchto rozvrhů v kalendáři v rámci GUI.

3. Řešení musí umožňovat autentizované skenovaní pro přesnější zjištění bežících služeb a automatizované inteligentní ověřování skutečných síťových služeb běžících na nalezených TCP/UDP portech (nikoliv pouze dle banneru a čísla portu).
4. Řešení musí umožňovat volbu intenzity testování (např. kolik IP adres a TCP/UDP portů testovat paralelně), rychlosti testování (např. port mapping speed, packet delay time) s minimalizací zátěže testovaných zařízení a síťové infrastruktury.
5. Řešení musí umožňovat nastavení minimalizace rizika výpadku testovaného zařízení nebo síťové služby, minimálně zákazem provádění invazivních testů, zákazem aplikace exploitů, DoS i DDoS útoků a password brute forcingu.
6. Řešení musí umožňovat automatické predikce nových zranitelností dle relevantních atributů: verze OS, verze síťových protokolů a verze aplikací na dříve testovaných systémech bez potřeby jejich nového otestování po zveřejnění nových typů zranitelností.
7. Řešení musí umožňovat konfigurovatelný reporting a filtrování výsledků testování webových aplikací s možností třídění a filtrování výsledků testování dle všech kategorií zranitelností aktuální verze OWASP TOP-10 a filtrování výsledků testování dle zvolené topologie (logických větví) webových aplikací.
8. Řešení musí umožňovat provádět automatizované testy zranitelností zařízení, systémů i aplikací anonymně (bez přihlášení uživatele) a autentizovaně (pod účtem vybraného uživatele aplikace).
9. Řešení musí umožňovat testování dynamicky přidělovaných IP adres přes DHCP službu a sledování její historie a reportování pomocí „DNS name“ nebo „Host name“.
10. Řešení musí umožňovat testování překrývajících se IP adres a jejich individuálního sledování a reportování dle různých lokalit.
11. Řešení musí paraleně pracovat s IPv4 i IPv6, jedná se především o schopnost detekovat IPv6 systémy při skenování pomocí IPv4.
12. Řešení musí detekovat zranitelnosti v celém „IT stacku“. Například po objevení defaultního hesla, toto heslo využít pro další hlubší skeny a detekci souvisejících zranitelností.
13. Řešení musí podporovat automatické zjišťování aktiv (asset management), přičemž musí minimálně zvažovat následující parametry IP adresy, MAC adresy a hostname, tak aby bylo zamezeno duplicitám. Systém musí umožňovat načítání logů z DHCP serveru a dynamicky upravovat údaje o strojích, tj. řešení musí umožňovat discovery scan, tedy zrychlené pravidelné automatické, kontinuální (nepřetržité) i ad-hoc ruční spouštění mapování síťové infrastruktury s identifikací i OS, TCP a UDP portů a služeb a vyznačením nových, potvrzených a nepotvrzených zařízení. Minimální požadovaná periodicita 1x denně přes celý IP rozsah v rámci dodávky. VM při autentifikovaném skenu dokáže vytvořit i seznam běžících služeb, dle něj se dá pak groupovat, vyhledávat apod (např verze OS, firmware, běžící služby, databáze aj)

Požadavky na scoring, značkování a filtraci

1. Řešení musí umožňovat automatickou aktualizaci tagů v Asset databázi dle dynamických tagovacích pravidel.
2. Řešení musí umožňovat automatickou centralizaci všech nalezených aktivních systémů a jejich atributů: verze OS, verze aplikací, otevřené TCP a UDP porty a síťové protokoly do jednotné Asset databáze s možností definovat statické a dynamické hierarchické tagy (nálepky) a dle těchto tagů provádět filtrování aktiv, jejich testování i reportování výsledků.
3. Řešení musí podporovat tzv Real Risk skóre, zahrňující do priorizace akcí a kritičnosti zranitelnosti i informace o existenci exploitu a informaci již o použití daného exploitu (nebo jiného zneužití zranitelnosti) včetně zahrnutí informace o obtížnosti zneužití (dokáže i začátečník nebo jen zkušený profesionál apod).

4. Řešení musí umožňovat definici pravidel pro automatické a dynamické tagování aktivních systémů dle nalezených atributů po každém testu zranitelností, minimálně pro:
    - verzi operačního systému;
    - verzi instalovaných aplikací;
    - otevřené TCP a UDP porty;

- verzi síťových protokolů;
- verzi nalezených zranitelností.

5. Řešení musí umožňovat centralizované úpravy v databázi zranitelností, a to tak aby pro celý rozsah implementace bylo možné měnit hodnotu rizikovosti zranitelností, popis hrozeb, popis negativního dopadu a odstranění zranitelností nebo bylo možné vyjmout určité zranitelnosti z testování, a dále editovat CVSS Scoring (Common Vulnerability Scoring System).
6. VM pro každou zjištěnou zranitelnost uvádět popis relevantních hrozeb, možného negativního dopadu na systém, odkazy na online zdroje nebo databáze zranitelnosti popisující danou zranitelnost (např. webovou stránku výrobce SW, cve.mitre.org apod.) a popis odstranění zranitelnosti s uvedením http linku na patch výrobce nebo postup změny konfigurace systému.
7. Řešení musí umožňovat automatizovanou identifikaci všech zjištěných zranitelností ve výsledcích testování, včetně míry jejich rizikovosti, popisu příslušných TCP/UDP portů, protokolů, síťových služeb a aplikací na kterých byly detekovány.

Požadavky na vizualizaci

1. Řešení musí umožňovat filtrování výsledků mapování síťové infrastruktury dle platformy OS, otevřených TCP-IP portů, potvrzených/nepotvrzených zařízení, automatizované srovnávání historických map s vyznačením rozdílů.
2. Řešení musí umožňovat automatické filtrování a reportování relevantních aktiv dotčených novou zranitelností s vyznačením pravděpodobnosti s využitím skóre reálného rizika.

Požadavky na shodu nastavení (Configuration Audit)

1. Řešení musí umožňovat definice a tvorbu i vlastních template bezpečnostní kontroly konfigurací operačních systémů Windows, Linux na základě vybraných parametrů uložených v registrech a souborových systémech a možnost kontrolovat integritu vybraných konfiguračních souborů.
2. Řešení musí umožňovat automatické provádění bezpečnostního auditu konfigurace minimálně následujících operačních systémů:
   - Windows desktop 7+ a Windows Server 2008+,
   - RHEL, GNU/Linux distribuce;
   - databází: Oracle 10+, MS SQL Server, Postgres, MySQL;
   - routerů a switchů s podporou pro IOS, NX-OS, Comware 5 a 7 výrobců HP, Cisco;
   - aplikačních web serverů: Apache, WebSphere, MS IIS;
   - a virtualizační platformy VMware;

   vůči šablonám technických bezpečnostních opatření.

Požadavky na autentizaci, autorizaci a uživatelskou segregaci

1. Řešení musí umožňovat seskupování testovaných systémů do skupin s přiřazením vlastníků a hodnoty aktiv.
2. Řešení musí umožňovat katalogizaci rozsahu testovaných webových aplikací pod účtem uživatele a porovnání přístupových práv uvnitř webové aplikace mezi jednotlivými uživateli.
3. Řešení musí umožňovat provádět testování zranitelností bez nebo volitelně se vzdálenou autentizací na testovaná zařízení na úroveň operačních systémů a databází.
4. Řešení musí podporovat autentizaci uživatelů do centrální řídící aplikace a centrální databáze výsledků testování, pomocí externího LDAP, primárně AD s Kerberos.
5. Řešení musí umožňovat centralizované a vysoce zabezpečené šifrované úložiště všech výsledků mapování sítě a testování zranitelností systémů s řízením přístupových oprávnění na základě definovaných rolí a odpovědností k výsledkům a spouštění testování a auditů, dle principu need-to-know.
6. Řešení musí umožňovat změnu závažnosti zranitelnosti a modifikace testovaných skupin a typů testovaných zranitelností.

Požadavky na reporting

1. Řešení musí umožňovat centralizované, agregované ukládání všech výsledků testování zranitelností a auditů konfigurace všech systémů a webových aplikací do jednotné normalizované databáze s centrálním monitoringem stavu zranitelností (formou Dashboardu) a centralizovaným reportingem nad agregovanými výsledky všech realizovaných testů a auditů ze všech lokalit v rámci dodávky.
2. Řešení musí umožňovat automatické filtrování a reportování relevantních aktiv dotčených zvolenou „Zero-Day" zranitelností nebo hrozbou s vyznačením pravděpodobnosti úspěšného útoku.
3. Řešení musí umožňovat konfigurovatelný reporting a filtrování výsledků testování, zpracování trendů za libovolné časové období nad historií testování, porovnávání stavu zranitelností za zvolené časové období a oblast sítě a srovnávání výsledků vybraných historických testů.
4. Řešení musí umožňovat reporting výsledků mapování a testování zranitelností přes celou infrastrukturu v rámci dodávky, nezávislý reporting nad konkrétními realizovanými testy, reporting s automatickou korelací poslední známé informace a stavu zranitelností nad zvoleným rozsahem reportu.
5. Řešení musí umožňovat generování reportu nalezených zranitelností dle optimální logiky instalace patchů od nejnovějších po nejstarší patche a s vyřazením nahrazených patchů novějšími.
6. Řešení musí umožňovat podrobný technický reporting všech zjištěných zranitelností, informací a detailů o reportovaných systémech s možností filtrování zvolené úrovně a typu detailu.
7. Řešení musí umožňovat vytvořit sumární přehledový manažerský reporting o celkovém stavu a počtu zranitelností, trendem a vyplývající míře rizika nad zvoleným rozsahem reportu.
8. Řešení musí umožňovat konfigurovatelný reporting a filtrování výsledků testování webových aplikací s možností třídění a filtrování výsledků testování dle všech kategorií zranitelností aktuální verze OWASP TOP-10 a filtrování výsledků testování dle zvolené topologie (logických větví) webových aplikací.
9. Řešení musí umožňovat archivaci výsledků testů min. 12 měsíců s možností exportu minimálně ve formátech XML, CSV, HTM, PDF.
10. Řešení musí umožňovat automatickou centrální archivaci a korelaci všech výsledků historických testů zranitelností ze všech testovaných zařízení a oddělení reportingu od jednotlivých výsledků jednotlivých testů.
11. Řešení musí konsolidovat zranitelnosti odstranitelné stejným postupem a toto prezentovat formou remediačních plánů v rámci reportů.
12. Řešení musí identifikovat zranitelnosti pro které existuje exploit, případně asociované s konkrétním malware kitem. Řešení musí identifikovat známé typy malware a exploit kity související se zjištěnými zranitelnostmi a tyto skutečnosti zahrnout do rizikovosti zranitelnosti. Součástí popisu zranitelnosti musí být informace, zda je daná zranitelnost využívána útočníky.

Další požadavky

1. Hodnocení rizik musí vyjma parametru CVSS zahrnovat typ aktiva, jeho důležitost, dostupnost exploitů, zneužitelnost dané hrozby útočníkem, technická náročnost zneužití hrozby a další parametry. Výsledkem všech parametrů je ohodnocení dané zranitelnosti z hlediska její kritičnosti.
2. Řešení musí navrhovat kroky k odstranění hrozby a poskytovat nástroje pro optimalizace počtu kroků opatření s cílem udržet skóre rizikovosti na stanovené úrovni.
3. Řešení musí podporovat integraci se SIEM produkty ArcSight.
4. Řešení musí podporovat integraci s penetračními testovacími platformami, aby bylo možné potvrdit, že zranitelnosti lze využít, například integraci s Metasploit.
5. Řešení musí obsahovat mechanizmus pro nastavení minimálních politik pro jednotlivá aktiva a reportovat neshodu s politikami.
6. Řešení by mělo obsahovat automatický mechanizmus k označování strojů (např. dle parametrů) a na základě označení provádět další akce. Systém musí obsahovat také ruční značení strojů.
7. Řešení musí být schopno automaticky kategorizovat prostředky na základě více atributů (například nainstalovaný operační systém, IP rozsah) a stroje objevené při skenování automaticky třídit do dané skupiny.

8. Řešení lze rozšířit o další modul určený k automatizaci procesů bezpečnostních nástrojů (SOAR), není nyní součástí výberového řizení.
9. Řešení lze rozšířit o další modul určený pro testování zranitelnosti webových aplikací (DAST), není nyní součástí výběrového řízení.
10. V případě rozšíření řešení o další z výše uvedených modulů není třeba nainstalovat další typy agentů, lze využít jednotného agenta pro všechny technologie a tím zjednodušit proces případné implementace a správy.
11. Řešení musí umožňovat také autentizované (auditní) skenování. A systém musí pro autentizaci podporovat minimálně tyto systémy:
    - Concurrent Versioning System (CVS)
    - DB2; File Transfer Protocol (FTP); IBM AS/400; Lotus Notes/Domino
    - Microsoft SQL Server ; Sybase SQL Server
    - Microsoft Windows/Samba (SMB/CIFS); Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS)
    - MySQL Server; Oracle
    - Post Office Protocol (POP); PostgreSQL
    - Remote Execution; Simple Network Management Protocol (SNMP)
    - Secure Shell (SSH); Secure Shell (SSH) Public Key
    - Sybase SQL Server; Telnet; Web Site Form Authentication
12. Řešení musí disponovat funkcionalitou řízení procesu nápravy zranitelností. Toto musí obsahovat nejméně definici postižených zařízení, seznamu zranitelností, přidělení pracovníka zodpovědného za nápravu a pracovníka a požadovaný termín vyřešení. Opakované skeny zranitelností budou zobrazovat aktuální stav řešených zranitelností a postup daného projektu.

Požadavky na související plnění

Předávání dat do KOC

Veškerá komunikace mezi jednotlivými PO a KOC bude probíhat šifrovaně, aby nebylo možné komunikaci zachytit a zneužít. Dodavatel v nabídce popíše navrhovaný způsob zabezpečení.

Implementace

Implementací se rozumí zprovoznění řešení skeneru zranitelností v sítích všech uvedených subjektů a PO ve spolupráci s jednotlivými administrátory PO. Dále otestování obousměrné komunikace mezi PO a KOC, kdy součástí akceptačníchtestů implementace bude provedení skenu (dle vytvořených a odsouhlasených skenovacích polotik) na specifikovaném segmentu sítě či zařízeních PO.

Podpora produktivního provozu

Součástí dodávky – implementace bude intenzívní post-implementační podpora po dobu 3 měsíců v rozsahu 3MD/měsíc.

Školení

Součástí předmětu veřejné zakázky bude také zaškolení odpovědných osob objednatele pro zvládnutí obsluhy dodané technologie v minimálním rozsahu 8 hodin, rozdělených do dvou bloků po 4 hodinách. Dále pro administrátory PO budou zajištěny 3 termíny stejných školení online v délce min. 2 hodin, tak aby se administrátoři mohli připojit nejméně na jeden z daných termínů.

Dokumentace

Součástí dodávky bude dokumentace, a to minimálně v následujícím rozsahu:

- Provozní dokumentace – popis reálného nasazení + popis skenovacích politik
- Zanesení relevantních informací do provozní CMDB KOC (konfigurační databáze)

- Guides výrobce (v českém nebo anglickém jazyku)

Rozvoj a a související plnění

Objednatel předpokládá, že případný rozvoj bud poskytován v rozsahu cca 8MD/4 roky. V případě, že nastanou situace, které objednatel nezvládne vyřešit vlastními silami (například detekce zranitelností velkého rozsahu, přechod na novější verzi SW, rozsáhlé analýzy detekcí apod.), pro každý jednotlivý případ bude smluvními stranami předem dohodnut rozsah prací a objednatel vystaví objednávku.

Technická podpora

Objednatel předpokládá, že technická podpora bude poskytována v rozsahu cca 2MD/měsíc. **Technickou podporou** se rozumí činnosti spojené s diagnostikou, laděním, monitorováním, softwarovým vývojem, testováním, analyzováním, dokumentováním, implementací, nasazováním, projektovým řízením a podobně, za účelem řešení závad a chybových stavů, které jsou nebo se jeví jako závady nebo chybové stavy dodaného systému. Tyto činnosti též zahrnují činnosti související s infrastrukturou KOC nezbytně nutné pro efektivní řešení událostí (operační systémy, databázové systémy, integrovaný software, ovladače, komponenty a podobně), a dále zahrnují z toho vyplývající nezbytnou součinnost dodavatele pro zaměstnance objednatele a jeho ostatních dodavatelů.

Vymezení technické podpory

Popis minimálního rozsahu činností technické podpory požadovaných objednatelem

Dodavatel zajistí:

1. Pravidelné profylaxe dodané technologie a prostředí
2. Konfigurační úpravy – stejný postup jako níže u instalací nových verzí firmware
3. Instalace aktualizací firmware – veškeré aktualizace budou nejdříve testovány v testovacím prostředí dodavatele, aby nedošlo k narušení funkčnosti KOC.
4. Instalace aktualizací definic
5. Health check na měsíční bázi – kontrola stavu a provozuschopnosti HW
6. Zaškolení obsluhy při případném přechodu na novou verzi management konzole
7. Průběžná aktualizace dokumentace dle skutečného stavu

Evidence událostí a vykazování času

1. Události a úkoly zadává primárně objednatel. V odůvodněných případech zadává události a úkoly pracovník dodavatele.
2. Počáteční stanovení Kategorie a Priority provádí objednatel. Dodavatel je Kategorii události oprávněn změnit pouze po dohodě s objednatelem.
3. Čas strávený řešením událostí a požadavků pracovníci dodavatele zaznamenávají k příslušným událostem. Vykazovaný čas je zaokrouhlován na 30 minutové úseky nahoru.
4. Objednatel je oprávněn vykazovaný čas kontrolovat na základě předložených předávacích protokolů za daný měsíc a nejdéle do 5 dnů po doručení příslušné faktury s předávacím protokolem odsouhlasit výkaz prací. Objednatel je povinen oznámit dodavateli své námitky bez zbytečného odkladu po předložení dané faktury.

Kategorie události

Události jsou zařazeny do jedné z následujících kategorií podle závažnosti a pozorovaných nebo očekávaných důsledků události v případě, že nebude vyřešena:

1. Kategorie A: Úplná nedostupnost technologie nebo její kritické komponenty bez možnosti problém obejít jiným postupem práce nebo administračním zásahem; událost obecně způsobuje závažné ztráty objednateli.
2. Kategorie B: Závada nebo chybový stav technologie, který nezpůsobuje nedostupnost KOC nebo její kritické komponenty, avšak závažným způsobem omezuje či znemožňuje provádění některých činností; lze jej obejít jiným způsobem nebo administračním zásahem, resp. nezpůsobuje závažné ztráty objednateli.
3. Kategorie C: Všechny ostatní události s nižší závažností, které nejsou kategorizovány jako A nebo B.

4. Kategorie D: Požadavky na konzultaci nebo rozvoj provozovaných technologií

Vyřešení události je stav, kdy:

1. bylo dosaženo odstranění příčiny závady nebo chybového stavu; nebo
2. závada nebo chybový stav se přestal projevovat přes úsilí vynaložené k odhalení příčiny; nebo
3. byl navržen a zaveden náhradní postup práce, který alespoň o jeden stupeň snižuje Kategorii události; to vede na vznik nové události s nižší Kategorií a novou Prioritou; nebo
4. objednatel událost odvolal; nebo
5. po dohodě s objednatelem byla událost uzavřena z jiných důvodů; nebo
6. objednatelem byl zamítnut servisní zásah na místě, aniž by byla k dispozici jiná možnost řešení události (např. vzdáleným přístupem); nebo
7. byla prokázána příčina, jejíž odstranění není v kompetenci dodavatele ve smyslu rozsahu poskytované Technické podpory; to nevylučuje poskytování další součinnosti.

Poskytování technické podpory bude uhrazeno na základě faktury pouze za odvedenou/vykázanou práci.

Příloha č. 3 smlouvy – Rozpočet

Rozpočet - Skener zranitelností

CENÍK						
Název účastníka:			...			
Řádek		**Jednotka**	**Cena za jednotku v Kč bez DPH**	**Cena za všechny organizace, na 1 rok**		**Cena za všechny organizace, na 4 roky**
1.	**Licence na 1 organizaci a na dobu 12 měsíců (kategorie A - do 100 assetů)**	1 organizace/12 měsíců	[redacted]			
	Licence na 1 organizaci a na dobu 12 měsíců (kategorie B - 101 - 300 assetů)	1 organizace/12 měsíců				
	Licence na 1 organizaci a na dobu 12 měsíců (kategorie C - 301 - 600 assetů)	1 organizace/12 měsíců				
2.	**Implementace v 1 organizaci**	1 organizace/jednorázově				
3.	**Upgrade HW v 1 organizaci**	1 organizace/jednorázově				
4.	**Technická podpora (1MD)**	1MD				
5.	**Případný rozvoj a související plnění (1MD)**	1MD				
6.	**Maintenance na 1 organizaci**	1 organizace/12 měsíců				
			Celková nabídková cena			**10 656 600,00 Kč**

Počet organizací celkem:	14
Kategorie A - do 100 assetů	[redacted]
Kategorie B - 101 - 300 assetů	
Kategorie C - 301 - 600 assetů	
Doba plnění (roky)	
Technická podpora - předpoklad ve 14 organizacích/48 měsíců (2MD/měsíc)	
Případný rozvoj a související plnění - předpoklad ve 14 organizacích/48 měsíců	