Ev. č. smlouvy kupujícího: VZ1295

Aktualizovaná Příloha č. 3C zadávací dokumentace

SMLOUVA NA DODÁVKU A IMPLEMENTACI SW SYSTÉMU PRO ZABEZPEČENÍ KONCOVÝCH ZAŘÍZENÍ

uzavřená dle ustanovení § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník ve znění pozdějších předpisů (dále jen „smlouva“)

Článek I.
Smluvní strany

Objednatel:	**Zdravotní ústav se sídlem v Ostravě**
Sídlem:	Partyzánské náměstí 2633/7, Moravská Ostrava, 702 00 Ostrava
IČO:	71009396
DIČ:	CZ71009396
	Státní příspěvková organizace nezapsaná ve veřejném rejstříku
Bankovní spojení:	ČNB
č. ú.:	3235761/0710
ID datové schránky:	pubj9r8
Zastoupený:	Ing. Eduardem Ježem, ředitelem

(dále jen jako *„objednatel“*)

a

Dodavatel:	DATA-INTER spol. s r. o.
Sídlem/místem podnikání:	U Fortny 50/1, 746 01 Opava
IČO:	14615754
DIČ:	CZ14615754 (plátce DPH)
zapsaný v obchodním rejstříku vedeném Krajským soudem v Ostravě , oddíl C, vložka: 307	
Bankovní spojení:	Česká spořitelna a. s.
č. ú.:	6240636339/0800
ID datové schránky:	5x8x6ax
Zastoupený:	Ing. Karlem Boženkem, jednatelem

(dále jen *„dodavatel“*)

Smluvní strany uzavírají níže uvedeného dne tuto smlouvu v souladu se zadávací dokumentací kupujícího ze dne 27.1.2025, a to na základě výsledku výběrového řízení na veřejnou zakázku s názvem **„ZÚOVA - Zvýšení kybernetické bezpečnosti“** v části 3. **„Pořízení systému pro zabezpečení koncových zařízení na úrovni EDR a vyšší a Patch Management“**, zadanou objednatelem v otevřeném nadlimitním řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpis (dále jen „veřejná zakázka“), realizovanou v rámci projektu **„ZÚOVA - Zvýšení kybernetické bezpečnosti“,** registrační číslo projektu **„CZ.31.2.0/0.0/0.0/23_095/0008634**“, který je financovaný z prostředků Evropské unie, konkrétně programu: „Národní plán obnovy“, výzvy: 31_23_095 „Výzva č. 43 - Kybernetická bezpečnost - subjekty zdravotní péče“ a nabídkou prodávajícího ze dne 13.03.2025 (dále jen „nabídka“).

Ev. č. smlouvy kupujícího: VZ1295

Prodávající touto smlouvou garantuje kupujícímu splnění „**Části 3. Pořízení systému pro zabezpečení koncových zařízení na úrovni EDR a vyšší a Patch Management**“ zadání veřejné zakázky „ZÚOVA - **Zvýšení kybernetické bezpečnosti**“, zadané kupujícím v otevřeném nadlimitním řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů a prohlašuje, že splňuje všechny podmínky a povinnosti podle zadávací dokumentace veřejné zakázky. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:

a) v případě jakékoliv nejistoty ohledně výkladu ustanovení této smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel veřejné zakázky vyjádřený zadávací dokumentací,
b) v případě chybějících ustanovení této smlouvy budou použita dostatečně konkrétní ustanovení zadávací dokumentace,
c) prodávající je vázán svou nabídkou ze dne 13.03.2025 předloženou kupujícímu v rámci zadávacího řízení na veřejnou zakázku v Části 3., která se pro úpravu vzájemných vztahů vyplývajících z této smlouvy použije subsidiárně.

Článek II.
Základní ustanovení

1. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu se skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
2. Je-li dodavatel plátcem DPH, prohlašuje, že bankovní účet uvedený v čl. I odst. 2 této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“). V případě změny účtu dodavatele je dodavatel povinen doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu; je-li dodavatel plátcem DPH, musí být nový účet zveřejněným účtem ve smyslu předchozí věty.
3. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.
4. Dodavatel prohlašuje, že je odborně způsobilý k zajištění předmětu plnění podle této smlouvy.

Článek III.
Předmět smlouvy

1. Předmětem této smlouvy je dodávka a implementace dodávka nové a nepoužité (nikoliv repasované) ochrany koncových bodů pro 700 zařízení včetně virtualizačních platforem splňující níže uvedené minimální požadavky zadavatele včetně příslušenství či souvisejících technologií potřebných k plnému využití jejich vlastností a funkcionalit v rutinním provozu (dále jen „systém“) a umožnění jeho bezproblémového provozu (dále jen „plnění“) Podrobná specifikace plnění dle této smlouvy je uvedena v příloze č. 1C této smlouvy.
2. Systém bude instalován a provozována na HW prostředcích umístěných v budově sídla objednatele.
3. Plnění je strukturováno do následujících částí:
    a) Část 1 – Dodávka a implementace systému včetně dokumentace;
    b) Část 2 – Školení uživatelů a administrátorů;
    c) Část 3 – Zkušební provoz;
    d) Část 4 – Akceptační testy a předání plnění;
    e) Část 5 – Poskytování záruky

4. Předmětem této smlouvy je dále odpovídající závazek objednatele poskytnout dodavateli takovou součinnost, aby při plnění jeho povinností vyplývajících z této smlouvy tak, aby smlouva mohla být řádně realizována.
5. Předmětem této smlouvy je také závazek objednatele převzít od dodavatele plnění ve sjednané době plnění a zaplatit za něj dohodnutou cenu ve výši a způsobem dle této smlouvy.
6. Součástí předmětu plnění dodávaného dodavatelem je též poskytnutí licencí k SW specifikovanému v příloze č. 1C této smlouvy, včetně všech dokladů a návodů v českém jazyce, které se k software vztahují. Licencí se rozumí oprávnění objednatele k výkonu práva duševního vlastnictví k software a užití software pro potřeby objednatele a uživatele. Objednatel nebo uživatel je oprávněn na základě udělené licence software užít v územně neomezeném rozsahu po dobu trvání majetkových práv autora software. Odměna za poskytnutí licence je součástí ceny uvedené v čl. IV této smlouvy. Odpovědnost za neoprávněný zásah do autorských i jiných práv třetích osob nese výlučně dodavatel.
7. V případě, že v rámci plnění vznikne autorské dílo dodavatel poskytuje touto smlouvou objednateli a objednatel touto smlouvou přijímá nevýhradní oprávnění k užití takového autorského díla, a to všemi způsoby uvedenými v § 12 odst. 4 zákona č. 121/2000 Sb., o právu autorském o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Článek IV.
Cena

1. Celková cena za plnění dle této smlouvy činí:
   - 3.980.000 Kč bez DPH,
   - sazba DPH 21 %,
   - celková výše DPH 835.800 Kč,
   - 4.815.800 Kč včetně DPH.

   Podrobný rozpis ceny za plnění je uveden v příloze č. 2 této smlouvy.
2. Cena podle odst. 1 tohoto článku smlouvy zahrnuje veškeré náklady dodavatele spojené se splněním jeho závazků vyplývajících z této smlouvy, včetně nákladů na poskytnuté licence a všech dalších souvisejících nákladů. Cena je stanovena jako nejvýše přípustná a není ji možno překročit.
3. Je-li dodavatel plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, bude dodavatel k ceně za plnění bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny za plnění v důsledku změny sazby DPH není nutno ke smlouvě uzavírat dodatek. V případě, že dodavatel stanoví sazbu DPH či DPH v rozporu s platnými právními předpisy, je povinen uhradit objednateli veškerou škodu, která mu v souvislosti s tím vznikla.

Článek V.
Místo a doba plnění

1. Místem plnění je: Zdravotní ústav se sídlem v Ostravě
   Partyzánské náměstí 2633/7
   Moravská Ostrava
   70200 Ostrava
2. Dodavatel se zavazuje provést kompletní plnění dle této smlouvy provést a odevzdat objednateli nejpozději do **3 měsíců** od nabytí účinnosti této smlouvy.
3. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami, a účinnosti okamžikem jejího uveřejnění v registru smluv podle zákona č. 340/2015 Sb., ve znění pozdějších předpisů.

Ev. č. smlouvy kupujícího: VZ1295

VI.
Akceptace plnění

1. Objednatel převezme plnění jako celek, a to bez vad a nedodělků po dokončení akceptační procedury (akceptačních a funkčních testů).
2. Plnění jako celek bude objednatelem převzato na základě finálního předávacího protokolu.
3. Ve finálním předávacím protokolu a v dílčím předávacím protokolu objednatel či uživatel prohlásí, zda plnění přejímá nebo jeho příslušnou část či nikoli. Pokud příslušná část plnění nebude převzata, protože obsahuje vady či nedodělky, potvrdí tuto skutečnost objednatel či uživatel v dílčím předávacím protokolu, včetně specifikace vad či nedodělků. Objednatel nebo uživatel je povinen vznést své výhrady nebo připomínky do 5 pracovních dnů. Dodavatel je povinen do 5 pracovních dnů provést veškeré potřebné úpravy dle výhrad a připomínek a předat příslušnou část plnění uživateli či objednateli k opětovné akceptaci.
4. Plnění jako celek se považuje za dokončené, pokud došlo k akceptaci a protokolárnímu převzetí, za předpokladu, že proběhl zkušební provoz, systém je plně funkční bez vad a nedodělků. Finální akceptace bude provedena na základě finálního předávacího protokolu.
5. Finální předávací protokol dle odst. 3 a 4 tohoto článku smlouvy bude obsahovat alespoň tyto náležitosti:
   a) číslo příslušného předávacího protokolu a datum jeho vyhotovení, místo vyhotovení,
   b) číslo této smlouvy, číslo veřejné zakázky,
   c) označení předmětu plnění
   d) označení objednatele a dodavatele,
   e) prohlášení objednatele či uživatele, že plnění či jeho část přejímá či nikoliv,
   f) jména a podpisy zástupců objednatele, uživatele a dodavatele, včetně kontaktních telefonů a e-mailů.

VII.
Platební podmínky

1. Právo na zaplacení ceny vzniká dodavateli řádným a včasným splněním jeho závazku poskytnout plnění, které je prosté vad, v místě plnění, a to na základě objednatelem potvrzeného předávacího protokolu.
2. Objednatel zaplatí cenu na základě faktury, kterou dodavatel vystaví po dodání zboží na základě kopie předávacího protokolu.
3. Dodavatel se zavazuje, že jím vystavená faktura bude obsahovat všechny náležitosti, které jsou stanoveny obecně závaznými právními předpisy (např. náležitosti daňového dokladu) a smluvními ujednáními a bude na ní uvedena touto smlouvou stanovená lhůta splatnosti. Adresa pro doručení daňového dokladu: Zdravotní ústav se sídlem v Ostravě, Partyzánské náměstí 2633/7, Moravská Ostrava, 702 00 Ostrava. V případě elektronického zaslání faktury je prodávající povinen doručit fakturu na adresu elektronické pošty kupujícího fakturace@zuova.cz
4. Faktura musí dále obsahovat:
   a) ev. číslo smlouvy kupujícího: VZ1295 a datum vystavení faktury,
   b) název projektu: „ZÚOVA – Zvýšení kybernetické bezpečnosti“, reg. č.: CZ.31.2.0/0.0/0.0./23_095/0008634,
   c) nedílnou součástí faktury bude vždy kopie předávacího protokolu s výčtem předávaných položek podepsaného oprávněnými zaměstnanci prodávajícího a kupujícího,
   d) předmět plnění a jeho přesnou specifikaci,
   e) číslo dodacího listu,
   f) lhůtu splatnosti faktury.

5. Celková cena musí být na faktuře uvedena v české měně.
6. Faktura je splatná do 60 kalendářních dnů ode dne prokazatelného doručení faktury objednateli.
7. Doba splatnosti faktury začíná běžet ode dne řádného doručení daňového dokladu objednateli. Za uhrazení faktury se považuje den, kdy byla předmětná částka odepsána z účtu objednatele.
8. Jestliže faktura nebude obsahovat náležitosti stanovené právními předpisy a touto smlouvou nebo jestliže údaje v ní uvedené nebudou správné, budou přepisované nebo jinak opravované, je objednatel oprávněn vrátit ji ve lhůtě splatnosti dodavateli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě se přeruší lhůta splatnosti a počne běžet znovu, ve stejné délce doručením opravené faktury do sídla objednatele.
9. V případě, že se dodavatel stane nespolehlivým plátcem ve smyslu § 106a zákona o DPH, je povinen o tom neprodleně písemně informovat objednatele. Neučiní-li tak, bude tato skutečnost smluvními stranami považována za podstatné porušení této smlouvy. Bude-li dodavatel ke dni uskutečnění zdanitelného plnění veden jako nespolehlivý plátce nebo číslo bankovního účtu prodávajícího uvedené na faktuře nebude zveřejněno způsobem umožňujícím dálkový přístup podle § 96 zákona o DPH, je objednatel oprávněn část ceny odpovídající dani z přidané hodnoty uhradit přímo na účet správce daně v souladu s ust. § 109a zákona o DPH. O tuto částku bude snížena celková cena a prodávající obdrží cenu bez DPH. Dodavatel souhlasí a bere na vědomí, že shora uvedeným postupem je zcela splněn závazek objednatele uhradit vyfakturovanou cenu. V případě, že z důvodu porušení povinností vyplývajících ze zákona o DPH prodávajícím bude objednatel jako ručitel vyzván příslušným správcem daně k zaplacení dlužné částky DPH za dodavatele, a to z jakéhokoliv důvodu, a tuto dlužnou částku DPH za něj uhradí, zavazuje se dodavatel uhradit objednateli tuto dlužnou částku do 30 dní ode dne, kdy byl k tomu objednatelem písemně vyzván. V případě, že se dodavatel stane nespolehlivým plátcem ve smyslu tohoto odstavce, má objednatel současně právo od této smlouvy odstoupit s účinky do budoucna.
10. Zálohy nebudou dodavateli poskytovány.
11. Dodavatel není oprávněn jednostranně započíst jakoukoli pohledávku vzniklou na základě této smlouvy nebo v souvislosti s ní.

Článek VIII.
Práva a povinnosti smluvních stran

1. Není-li stanoveno touto smlouvou výslovně jinak, řídí se vzájemná práva a povinnosti smluvních stran přiměřeně ustanoveními § 2586 a následujícími občanského zákoníku.
2. Dodavatel je zejména povinen:
   a) Provést plnění řádně a včas za použití postupů odpovídajících platným právním předpisům, technickým normám ČR nebo jiné dokumentaci vztahující se k provedení služby a umožňovat užívání, k němuž bylo určeno.
   b) Řídit se při provádění plnění pokyny objednatele.
   c) Umožnit objednateli kontrolu provádění plnění, a to kdykoliv po dobu jeho realizace. Pokud objednatel zjistí, že dodavatel nerealizuje plnění řádně či jinak porušuje svou povinnost, poskytne dodavateli lhůtu k nápravě; neučiní-li tak dodavatel ve stanovené lhůtě, je objednatel oprávněn od smlouvy odstoupit.
   d) Odstranit zjištěné vady a nedodělky plnění na své náklady.
   e) Dbát při realizaci plnění dle této smlouvy na ochranu životního prostředí a dodržovat platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí.
   f) Postupovat při realizaci plnění s odbornou péčí.
3. Smluvní strany se pro vyloučení pochybností výslovně dohodly, že veškerá data, která vzniknou v rámci plnění této smlouvy, náležejí objednateli, a to bez ohledu na to, zda případně budou v rámci plnění ze strany dodavatele upravována.

4. Dodavatel je povinen neprodleně písemně vyrozumět objednatele o případném ohrožení doby plnění a o všech skutečnostech, které mohou řádné a včasné plnění předmětu této smlouvy znemožnit, a to neprodleně od okamžiku, kdy se dodavatel dozví o takové skutečnosti.
5. Dodavatel není oprávněn postoupit jakákoliv práva anebo povinnosti vyplývající z této smlouvy na třetí osoby bez předchozího písemného souhlasu objednatele.
6. Smluvní strany sjednávají, že dodavatel není oprávněn jakékoliv jeho pohledávky za objednatelem, které vzniknou na základě této smlouvy, započítat vůči pohledávkám objednatele za dodavatelem jednostranným právním jednáním.
7. Dodavatel odpovídá objednateli za škodu způsobenou porušením povinnosti podle této smlouvy nebo povinnosti stanovené obecně závazným platným právním předpisem.
8. Dodavatel se zavazuje na realizaci této smlouvy alokovat pracovní kapacitu osob realizačního týmu uvedeného v nabídce dodavatele podané ve veřejné zakázce a k plnění této smlouvy využít výhradně těchto osob. Jakákoliv dodatečná změna osoby realizačního týmu musí být předem písemně schválena objednatelem. Dodavatel se v takovém případě zavazuje nahradit osobu realizačního týmu takovou osobou, která disponuje alespoň požadovanými minimálními znalostmi a odbornou kvalifikací dle požadavků objednatele uvedených v zadávací dokumentaci veřejné zakázky. Dodavatel i osoby podílející se na realizaci této smlouvy musí po celou dobu trvání této smlouvy splňovat kvalifikační kritéria stanovená v zadávací dokumentaci veřejné zakázky. Při porušení této podmínky má objednatel právo odstoupit od smlouvy.
9. Dodavatel je povinen předat objednateli do 5 měsíců od nabytí účinnosti této smlouvy rozpis ceny za plnění s určením samostatných majetků, souborů majetků nebo samostatných funkčních celků za účelem evidence majetku a jeho odepisování dle zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů. U odepisování dlouhodobého hmotného a nehmotného majetku bude uveden klasifikační kód CZ-CPA za účelem odepisování dlouhodobého hmotného a nehmotného majetku.

Článek IX.
Záruka za jakost

1. Dodavatel objednateli na hmotné věci, které byly dodány v rámci plnění poskytuje záruku za jakost (dále jen „záruka“) ve smyslu § 2113 a násl. občanského zákoníku, a to v délce 60 měsíců (dále též „záruční doba“).
2. Záruční doba začíná běžet dnem převzetí příslušné věci objednatelem. Záruční doba se staví po dobu, po kterou nemůže objednatel věc řádně užívat pro vady, za které nese odpovědnost dodavatel.
3. Během záruky má objednatel oprávnění k používání aktuální verze SW systému (nejvyšší verze software, která je pro používanou platformu právě komerčně dostupná a opravné verze software, včetně jejich aktualizace, budou-li dostupné).
4. Pro nahlašování a odstraňování vad v rámci záruky platí podmínky uvedené v odst. 9 a násl. tohoto článku smlouvy.
5. Specifikace požadované záruky je uvedena v příloze č. 1C této smlouvy.
6. Záruční požadavky bude objednatel či uživatel zadávat primárně prostřednictvím rozhraní Service Desk provozovaného objednatelem, do kterého bude dodavateli zřízen přístup.
7. V záruční době se prodávající zavazuje zajistit řešení záručních požadavků v časovém režimu 8x5.

Ev. č. smlouvy kupujícího: VZ1295

Práva z vadného plnění

8. Objednatel má právo z vadného plnění z vad, kterou má věc, která je součástí plnění při převzetí dodavatelem, byť se vada projeví až později. Objednatel má právo z vadného plnění také z vad vzniklých po převzetí věci objednatelem, pokud je dodavatel způsobil porušením své povinnosti. Projeví-li se vada v průběhu 6 měsíců od převzetí věci objednatelem, má se zato, že dodaná věc byla vadná již při převzetí.
9. Vady věcí, dodaných v rámci plnění dle a vady, které se projeví během záruční doby, budou dodavatelem odstraněny bezplatně.
10. Veškeré vady věcí dodaných v rámci plnění je objednatel povinen uplatnit u dodavatele bez zbytečného odkladu poté, kdy vadu zjistil, a to formou písemného oznámení (popř. emailem), obsahujícím co nejpodrobnější specifikaci zjištěné vady. Objednatel bude vady oznamovat na:
    - e-mail: support@datainter.cz
    - adresu: https://helpdesk.datainter.cz/
    - do datové schránky ID: 5x8x6ax

    K uplatňování vad dle tohoto odstavce jsou oprávněni kromě objednatele také uživatelé. Každé takovéto nahlášení vady se považuje za řádné uplatnění vady objednatelem ve smyslu této smlouvy.
11. Objednatel má právo na odstranění vady dodáním nové věci nebo opravou; je-li vadné plnění podstatným porušením smlouvy, má také právo od smlouvy odstoupit. Právo volby plnění má objednatel.
12. Servis za účelem odstraňování vad bude probíhat v místech instalace, tj. u uživatelů. V případě výměny nebo opravy v servisním středisku dodavatele nebo autorizovaném servisním středisku výrobce zabezpečí dodavatel bezplatně dopravu vadné věci od objednatele nebo uživatele do servisu a dopravu opravené nebo vyměněné věci zpět.
13. Dodavatel je povinen uhradit objednateli škodu, která mu vznikla vadným plněním, a to v plné výši. Dodavatel rovněž objednateli uhradí náklady vzniklé při uplatňování práv z vadného plnění.

Článek X.
Oznámení a komunikace, kontaktní osoby

1. Veškerá oznámení, tj. jakákoliv komunikace na základě této smlouvy, bude probíhat v souladu s tímto článkem. Kromě jiných způsobů komunikace dohodnutých mezi smluvními stranami se za účinné považují osobní doručování, doručování doporučenou poštou, zprávou do datové schránky, elektronickou poštou, a to na adresy smluvních stran, nebo na takové adresy, které si smluvní strany vzájemně písemně oznámí.
2. Oznámení správně adresovaná se považují za uskutečněná v případě osobního doručování anebo doručování doporučenou poštou okamžikem doručení, v případě posílání elektronickou poštou okamžikem obdržení potvrzení o doručení od druhé smluvní strany při použití stejného komunikačního kanálu.
3. Informace a materiály, které obsahují osobní údaje a důvěrné informace budou doručovány buď osobně, nebo zasílány elektronickou poštou a v případě požadavku objednatele šifrovány.
4. Pověřenými kontaktními osobami objednatele v souvislosti s plněním předmětu smlouvy jsou
    a) ve věcech technických:
    [redacted]
5. Pověřenými kontaktními osobami dodavatele v souvislosti s plněním předmětu smlouvy jsou:
    b) ve věcech obchodních:
    [redacted]

Ev. č. smlouvy kupujícího: VZ1295

c) ve věcech technických:
[redacted]

Článek XI.
Odpovědnost za škodu

1. Dodavatel bude povinen nahradit objednateli v plné výši škodu, která vznikla při realizaci služeb z důvodů na straně dodavatele nebo jako důsledek porušení povinností a závazků dodavatele dle této smlouvy.
2. Dodavatel prohlašuje, že po celou dobu trvání této smlouvy bude mít na vlastní náklady sjednánu pojistnou smlouvu pro případ způsobení škody třetí osobě s limitním plněním na jednu pojistnou událost minimálně 50 mil. Kč, s maximální spoluúčastí 500.000 Kč. Pojištění musí obsahovat krytí škod způsobené na majetku, zdraví třetích osob včetně krytí odpovědnosti za finanční škody.
3. V případě, že při činnosti prováděné dodavatelem dojde ke způsobení škody objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu odstavce 2 tohoto článku, bude dodavatel povinen tyto škody uhradit z vlastních prostředků.
4. Dodavatel předložil objednateli před podpisem této smlouvy doklad o sjednání pojistné smlouvy na požadované pojištění dle odstavce 2 tohoto článku smlouvy a je dále na výzvu objednatele povinen předložit doklad o trvání pojištění, včetně všech dodatků nebo certifikáty příslušných pojišťoven prokazující existenci pojištění (dobu trvání pojištění, jeho rozsah, pojištěná rizika, pojistné částky, roční limity a sublimity plnění a výši spoluúčasti). Doklad dle předchozí věty nesmí být starší 1 měsíce. Dodavatel je povinen předložit, po celou dobu plnění této smlouvy, do 5 pracovních dnů od vyžádání objednatelem, kopie pojistných smluv či certifikát prokazující existenci pojištění dle odstavce 2 tohoto článku smlouvy.

Článek XII.
Ochrana osobních údajů a důvěrných informací

1. Není-li stanoveno touto smlouvou či jejími přílohami výslovně jinak, je ustanoveními tohoto článku smlouvy mezi smluvními stranami upravena zejména bezpečnost informací, ochrana a zpracování osobních údajů a bezpečnostní procesy a postupy objednatele, které souvisejí s plněním této smlouvy.
2. Dodavatel objednateli odpovídá za to, že dokumenty a soubory dat, které mu při plnění této smlouvy předá:
   a) jsou kopiemi originálů příslušných dokumentů a souborů dat dodavatele,
   b) neobsahují žádné infiltrační prostředky,
   c) že k nim má práva na jejich šíření, instalaci, konfiguraci a správu, která mu umožňují s nimi nakládat a dále je poskytovat tak, jak je sjednáno v této smlouvě.
3. Veškeré skutečnosti obchodní, ekonomické a technické povahy související se smluvními stranami, které nejsou běžně dostupné v obchodních kruzích a se kterými se smluvní strany seznámí při realizaci předmětu smlouvy nebo v souvislosti s touto smlouvou, jsou považovány za neveřejné. V případě, že budou dodavateli zpřístupněny osobní údaje, jsou pro účely této smlouvy považovány za neveřejné.
4. Dodavatel se zavazuje, že neveřejné informace jiným subjektům nesdělí, nezpřístupní, nezkopíruje a neumožní jejich zkopírování ani nevyužije pro sebe nebo pro jinou osobu. Zavazuje se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Dodavatel se zavazuje zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost.

5. Povinnost plnit ustanovení tohoto článku smlouvy ohledně neveřejných informací se nevztahuje na informace, které:
   a) mohou být zveřejněny bez porušení této smlouvy,
   b) byly písemným souhlasem obou smluvních stran zproštěny těchto omezení,
   c) jsou známé nebo byly zveřejněny jinak než následkem porušení povinnosti jedné ze smluvních stran,
   d) příjemce je zná dříve, než je sdělí smluvní strana,
   e) jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem na základě zákona, popřípadě, jejichž uveřejnění je stanoveno zákonem,
   f) smluvní strana sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv.
6. Dodavatel je povinen zlikvidovat veškeré neveřejné informace, které se dověděl v průběhu plnění této smlouvy poté, co bude plnění z této smlouvy ukončeno, ať už splněním anebo jiným způsobem zániku této smlouvy.
7. Dodavatel je povinen přijmout veškerá potřebná opatření, která jsou nutná k zajištění plnění předmětu této smlouvy a která vyplývají z této smlouvy anebo z interních předpisů a postupů objednatele, se kterými bude dodavatel seznámen.
8. Povinnost ochrany neveřejných informací trvá bez ohledu na ukončení účinnosti této smlouvy. Neveřejné informace jsou považovány za důvěrné údaje ve smyslu § 1730 odst. 2 občanského zákoníku.
9. Dodavatel prohlašuje, že při plnění této smlouvy bude docházet ke zpracování osobních údajů (dále jen „zpracování“) ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů a ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „obecné nařízení“).
10. Smluvní strany prohlašují, že v při plnění této smlouvy není objednatel v pozici správce ani zpracovatele osobních údajů dle čl. 4 odst. 7 a 8 obecného nařízení.
11. Dodavatel prohlašuje, že zajistí bezpečnost zpracování a naplnění veškerých požadavků, které se na zpracování zejména ve smyslu obecného nařízení vztahují. Dodavatel si je vědom své odpovědnosti za dodržování veškerých zákonných povinností v souvislosti se zpracováním a rovněž si je vědom své odpovědnosti za škodu vzniklou v případě porušení těchto povinností. V případě potřeby je dodavatel povinen uzavřít s objednatelem či jednotlivými uživateli smlouvu o zpracování osobních údajů, případně jinou smlouvu, která zajistí soulad prováděného zpracování s platnými právními předpisy.

Článek XIII.
Sankce

1. V případě prodlení dodavatele s provedením plnění dle čl. V. odst. 2. této smlouvy, je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 10.000,- Kč, a to za každý započatý den prodlení.
2. V případě porušení povinnosti dodavatele dle článku XI. odst. 2 této smlouvy, je dodavatel povinen zaplatit objednateli smluvní pokutu ve výši 100.000,- Kč za každý i započatý měsíc, v němž nebude mít uzavřenou pojistnou smlouvu se stanovenými parametry.
3. V případě porušení povinnosti k ochraně osobních údajů a důvěrných informací dle čl. XII této smlouvy je dodavatel povinen zaplatit objednateli smluvní pokutu ve výši 50.000,- Kč za každý jednotlivý případ.
4. Pro případ prodlení se zaplacením ceny za plnění sjednávají smluvní strany úrok z prodlení ve výši stanovené občanskoprávními předpisy.

5. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně vedle smluvní pokuty, a to v plné výši.

Článek XIV.
Zánik smlouvy

1. Tato smlouva zaniká:
   a) písemnou dohodou smluvních stran,
   b) jednostranným odstoupením od smlouvy pro její podstatné porušení druhou smluvní stranou, s tím, že podstatným porušením smlouvy se rozumí zejména
      - neprovedení plnění ve sjednané době,
      - opakované nedodržení (nejméně 2x) pokynů objednatele, právních předpisů nebo technických norem, které se týkají poskytování plnění,
      - nedodržení smluvních ujednání o záruce za jakost nebo o právech z vadného plnění.
      - neuhrazení ceny za plnění objednatelem po druhé výzvě dodavatele k uhrazení dlužné částky, přičemž druhá výzva nesmí následovat dříve než 30 dnů po doručení první výzvy.
2. Objednatel je oprávněn smlouvu vypovědět bez uvedení důvodů ve vztahu k části 6 plnění (dle čl. III odst. 6 písm. f) této smlouvy).
3. Objednatel je dále oprávněn od této smlouvy odstoupit v těchto případech:
   a) bylo-li příslušným soudem rozhodnuto o tom, že dodavatel je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);
   b) podá-li dodavatel sám na sebe insolvenční návrh.
4. Odstoupením od smlouvy není dotčeno právo oprávněné smluvní strany na zaplacení smluvní pokuty ani na náhradu škody vzniklé porušením smlouvy. Dodavatel bere na vědomí, že vzniklá škoda na straně objednatele může zahrnovat ztrátu veškerých dotačních prostředků přiznaných objednateli v rámci všech částí projektu „ZÚOVA - Zvýšení kybernetické bezpečnosti“, registrační číslo projektu „CZ.31.2.0/0.0/0.0/23_095/0008634“.
5. Pro účely této smlouvy se pod pojmem „bez zbytečného odkladu“ dle § 2002 občanského zákoníku rozumí „nejpozději do 3 týdnů“.

Článek XV.
Závěrečná ustanovení

1. Doplňování nebo změnu této smlouvy lze provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, postupně číslovaných a takto označených dodatků.
2. Dodavatel nemůže bez souhlasu objednatele postoupit svá práva a povinnosti plynoucí z této smlouvy třetí osobě.
3. Tato smlouva je vyhotovena v elektronické podobě, přičemž každá ze smluvních stran obdrží její elektronický originál opatřený elektronickými podpisy smluvních stran.
4. Dodavatel prohlašuje, že souhlasí a je srozuměn se skutečností, že objednatel na základě zákona č. 340/2015 Sb., o registru smluv znění pozdější předpisů, je povinen uveřejnit tuto smlouvu v registru smluv a dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, o této smlouvě a právním vztahu jí založeném může být povinen zpřístupnit či poskytnout všechny informace, které citované zákony nebo jiné právní předpisy z uveřejnění nebo zpřístupnění nevylučují.
5. Smluvní strany se shodují, že zveřejnění této smlouvy v registru smluv podle zákona č. 340/2015 Sb., zajistí objednatel.
6. Nedílnou součástí této smlouvy jsou následující přílohy:

Ev. č. smlouvy kupujícího: VZ1295

Příloha č. 1C: Požadavky na pořízení systému pro zabezpečení koncových zařízení na úrovní EDR a vyšší a Patch Management

Příloha č. 2: Položkový rozpočet

Příloha č. 3: Technická specifikace

7. Smluvní strany prohlašují, že tato smlouva vyjadřuje jejich vážnou a svobodnou vůli, že smluvní projevy jsou dostatečně určité a srozumitelné a že smlouva nebyla uzavřena v tísni ani za nápadně nevýhodných podmínek. Na důkaz souhlasu s celým obsahem smlouvy ji podepisují oprávnění zástupci obou smluvních stran.

V Ostravě, dne .....

za kupujícího:

Ing. Eduard Ježo

Digitálně podepsal Ing. Eduard Ježo
Datum: 2025.05.05 13:11:28 +02'00'

Ing. Eduard Ježo
ředitel Zdravotního ústavu se sídlem v Ostravě

V Opavě, dne 05.05.2025

za prodávajícího:

Ing. Karel Boženek

Digitálně podepsal Ing. Karel Boženek
Datum: 2025.05.05 10:02:54 +02'00'

Ing. Karel Boženek
jednatel
DATA-INTER spol. s r. o.

Ev. č. smlouvy kupujícího: VZ1295

Příloha č. 1C: Požadavky na pořízení systému pro zabezpečení koncových zařízení na úrovní EDR a vyšší a Patch Management

Předmětem plnění této části veřejné zakázky je dodávka nové a nepoužité (nikoliv repasované) ochrany koncových bodů pro 700 zařízení včetně virtualizačních platforem splňující níže uvedené minimální požadavky zadavatele včetně příslušenství či souvisejících technologií potřebných k plnému využití jejich vlastností a funkcionalit v rutinním provozu (tzn. např. veškeré napájecí a datové kabely, software, atd.) (dále také „vybavení“).

Název	**CPV**
Balík programů pro zabezpečení	48730000-4
Balík antivirových programů	48761000-0
Dodávka programového vybavení	72268000-1
Systémová podpora	72253200-5
Systémové poradenství	72246000-1
Implementace programového vybavení	72263000-6
Počítačová školení	80533100-0

Minimální požadavky na vlastnosti předmětu plnění této části veřejné zakázky – parametry vyjadřující požadavky na výkon nebo funkci:

1. Počet zařízení

- Předmětem plnění dodávka ochrany koncových bodů pro 700 zařízení z toho minimálně 100 serverů a 600 pracovních stanic,
- Součástí dodávky jsou veškeré potřebné licence na 5 let.

2. Požadavky pro centrální správu

Požadovaná funkce
Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů
Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí
Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení
Konzole pro centrální správu je kompletně multi-tenantní
Podpora produktů výrobcem nástroje bude poskytována v českém jazyce
Základní vlastnosti

Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu
Aktualizace pro dodávaný produkt po dobu 5 let
Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem
Možnost zasílat upozornění napojením na Syslog server
Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce
Úlohy správy bezpečnosti
Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.
Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery
Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity
Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy
Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy
Možnost restartovat serveru nebo desktopu přímo z konzole centrální správy
Centralizované místo pro záznam všech úloh
Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)
Nastavení úrovně bezpečnosti
Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD
Reportování
Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě
Možnost zasílání vygenerovaných reportů e-mailem
Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv
Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen
Karanténa
Vzdálená obnova či smazání souboru v karanténě
Možnost automaticky přidat soubor do výjimky při obnově z karantény
Uživatelé
Více předdefinovaných rolí:

Root, administrátor, reportér 1. Root: spravuje komponenty řešení 2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení 3. Reportér: spravuje a vytváří reporty
Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)
Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny
Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení
Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat
Logy
Zaznamenávání uživatelských akcí
Detailní log pro každou akci
Komplexní vyhledávání v logách
Správa a instalace ochrany
Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány
Instalace může být provedena několika způsoby, alespoň: 1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 3. Distribuce instalačního balíčku pomocí GPO či SCCM
Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN
Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou
Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci
Konzole správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích
Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů
Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou
Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat
Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti
Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)
Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body
Možnost spustit Network discovery z kteréhokoli již instalovaného klienta

Ev. č. smlouvy kupujícího: VZ1295

3. Požadavky na vlastnosti a funkce ochrany fyzických koncových bodů

Požadovaná funkce
Podpora operačních systémů: Windows 11 Windows 10 Windows 8.1 Windows 8 Windows 7 Windows Server 2022 Windows Server 2022 Core Windows Server 2019 Windows Server 2019 Core Windows Server 2016 Windows Server 2016 Core Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Ubuntu 14.04 LTS a vyšší CentOS 6.0 a vyšší Debian 8.0 a vyšší Mac OS X El Capitan (10.11) a vyšší
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
Detekce na základě virových definicí (tzn. signatur)
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
Detekce 0-day útoků na základě odhalování anomálního chování

Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
Detekce 0-day bezsouborových útoků
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
Možnost automatického spuštění podezřelých souborů v Sandboxu
Možnost nastavení Sandboxu – délka pozorování po spuštění, počet opakování spuštění, přístup k internetu během detonace ano/ne
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
Možnost ručního vložení vzorku do Sandboxu
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
Řešení generuje detekce na základě automatizovaného hledání IoCs v datech sbíraných EDR senzorem
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
Řešení umožňuje analýzu vektoru útoku
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní
Možnost prověřovat http provoz
Možnost prověřovat provoz šifrovaný pomocí SSL

Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
Ochrana proti podvodným a phishingovým webovým stránkám
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
Patch management
Součástí nástroje musí být možnost bezdotykové a vzdálené distribuce patchů
Distribuce konkrétní záplaty pro definovanou zranitelnost automaticky
Distribuce konkrétní záplaty pro definovanou zranitelnost z konzole na vyžádání administrátorem
Řešení musí mít možnost definovat úložiště v lokální síti pro snížení dopadů na konektivitu do internetu
Možnost zobrazit stavu nainstalovaných / chybějících / nefunkčních záplat na koncovém zařízení
Součástí záplaty musí být informace (CVE, BuletinID)
Záplaty lze nástrojem distribuovat na fyzické a virtuální servery Windows, Golden image, pracovní stanice Windows a aplikace třetích stran.
Možnost odložení restartu pro záplaty.
Dostupné záplaty pro platformu Windows – desktopy a servery
Dostupné záplaty pro aplikaci MS Office
Dostupné záplaty pro aplikace výrobců: Adobe Acrobat, Adobe Reader, Google Chrome, Mozilla Firefox, Opera, Zoom client, WinZIP, VMware tools, Cisco WebEx
Firewall
Možnost blokovat skenování portů
Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS
Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb
Možnost vypnout IDS
Možnost nastavit profily známých sítí
Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu
Karanténa
Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě
Možnost obnovy souboru do originální či do nově zadané lokality

Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní)
Kontrola přístupu k internetu
· Zablokování přístupu na internet pro specifické stanice / skupiny stanic · Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic · Zablokování přístupu k internetu v určený čas · Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné) · Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)

4. Požadavky na vlastnosti a funkce ochrana virtualizovaných koncových bodů

Požadovaná funkce
Podpora operačních systémů: Windows 11 Windows Server 2022 Windows Server 2022 Core Windows Server 2019 Windows Server 2019 Core Windows Server 2016 Windows Server 2016 Core Ubuntu 16.04 LTS a vyšší
Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen
„Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením
„Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže
Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení
Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)

Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
Detekce na základě virových definicí (tzn. signatur)
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
Detekce 0-day útoků na základě odhalování anomálního chování
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
Detekce 0-day bezsouborových útoků
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
Možnost automatického spuštění podezřelých souborů v Sandboxu
Možnost nastavení Sandboxu – délka pozorování po spuštění, počet opakování spouštění, přístup k internetu během detonace ano/ne
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
Možnost ručního vložení vzorku do Sandboxu
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP
Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy

Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
Řešení umožňuje analýzu vektoru útoku
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
Možnost prověřovat http provoz
Možnost prověřovat provoz šifrovaný pomocí SSL
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic
Modul pro ochranu mailboxů lokálně provozované Microsoft Exchange proti malwaru, spamu a phishingovým útokům
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
Ochrana proti podvodným a phishingovým webovým stránkám
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)

5. Implementační služby

a. Obecné požadavky

- Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Účastník je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:
    (a) Dodávku nabízeného řešení,
    (b) Nastavení bezpečnostních politik dle nejlepších postupů,
    (c) Implementaci řešení,
    (d) Implementace ochrany Exchange Serveru 2019,
    (e) Implementace ochrany Actice direktory,
    (f) Provedení školení,
    (g) Zajištění zkušebního provozu,

(h) Provedení akceptačních testů,

(i) Předání do ostrého provozu.

- Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.
- Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office, pdf).

b. Harmonogram realizace

- Součástí nabídky dodavatele bude detailní harmonogram implementace systému včetně klíčových milníků a termínů.
- Maximální doba realizace jsou 3 měsíce od okamžiku nabytí účinnosti Smlouvy.

c. Požadavky na školení

- Účastník zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.
- Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- Školení administrátorů – minimální rozsah školení je 16 hodin, předpokládá se účast max. 10 účastníků, školení bude probíhat v sídle Zadavatele. Zadavatel může změnit místo školení dle potřeby.
- Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

d. Požadavky na provedení akceptačních testů a přechod do zkušebního provozu

- Účastník navrhne způsob a provedení akceptačních testů. Akceptační testy musí vždy zahrnovat minimálně:
  (a) Prokázání kompletnosti dodávky a splnění povinných požadavků.
  (b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
  (c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
  (d) Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná.
- O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol.
- Účastník zajistí zkušební (testovací) provoz v délce minimálně 30 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení v pracovní den v době od 8h do 16h.

e. Požadavky na dokumentaci

- Účastník zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.
- Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

6. Požadavky na záruku

a. Obecné požadavky

- záruka na celý systém 5 let,
- dodavatel zajistí, aby dodaný systém byl po dobu záruky funkční a aktualizován,
- komunikace záručních oprav bude vedena v českém jazyce,
- pro hlášení záručních požadavků je dodavatel povinen zajistit provoz helpdeskové aplikace a telefonické podpory v režimu 24x7. Součástí helpdeskové aplikace musí být reporting o průběhu řešení záručních požadavků,
- časový režim aktivní záruční podpory 8x5.

Vybraný dodavatel je povinen v rámci plnění předmětu této části veřejné zakázky také na svůj náklad:

- zajistit dopravu do místa plnění, včetně pojištění v rámci dopravy, cla a balného,
- poskytovat bezplatný záruční servis,
- zadavateli předat předávací protokol – dodací list.

Ev. č. smlouvy kupujícího: VZ1295

Příloha č. 2: Položkový rozpočet

P.č.	Položka	Popis nabízené položky	Cena v Kč bez DPH
1	Ceny jednotlivých produktů s licencemi na 5 let	700 lic. Bitdefender GravityZone Business Security Enterprise (Ultra) - 5 let 700 lic. Bitdefender GravityZone Patch Management - 5 let	3 980 000,00 Kč
2	Nabídková cena za implementaci	Popis implementace včetně detailního harmonogramu a klíčových milníků a termínů: 1. Dodávka nabízeného řešení v trial verzi (D+5) 2. Implementace řešení, ochrany Exchange Serveru 2019 a ochrany Active directory (D+30) 3. Nastavení bezpečnostních politik dle nejlepších postupů (D+30) 4. Provedení školení (D+31 až 59 dle možností zadavatele) 5. Zahájení zkušebního provozu (D+59) 6. Provedení akceptačních testů (D+89), 7. Dodávka ostrých licencí na 5 let a předání do ostrého provozu (D+90) Výše uvedené lhůty jsou maximální možné. Údaj D značí datum účinnosti smlouvy, čísla značí počet kalendářních dnů. Náklady na implementaci jsou zahrnuty v nabídkové ceně produktů, ke kterým se vztahují a nevyčíslujeme je zvlášť.	- Kč
3	Ostatní náklady	veškeré náklady jsou obsaženy již ve výše uvedených položkách, ostatní náklady nejsou žádné	- Kč

Celková nabídková cena bez DPH:	3 980 000,00 Kč
Výše DPH v %:	21%
Výše DPH v Kč:	835 800,00 Kč
Celková nabídková cena včetně DPH:	4 815 800,00 Kč

Ing. Karel Boženek

Digitálně podepsal Ing. Karel Boženek
Datum: 2025.05.05 10:03:25 +02'00'

Ing. Karel Boženek, jednatel

Ev. č. smlouvy kupujícího: VZ1295

Příloha č. 3: Technická specifikace

PODROBNÁ SPECIFIKACE NABÍZENÉHO PLNĚNÍ

1. Počet zařízení

- Předmětem plnění je dodávka ochrany koncových bodů pro 700 zařízení (z tohoto počtu lze použít až pro 245 serverů; za server je považována i stanice s OS Linux):
  - 700 licencí Bitdefender GravityZone Business Security Enterprise (Ultra)
  - 700 licencí Bitdefender GravityZone Patch Management
- Součástí dodávky jsou veškeré potřebné licence na 5 let.

2. Centrální správa

Funkce
Všechny komponenty řešení jsou v českém jazyce – včetně konzole správy, klientské aplikace a manuálů
Konzole pro správu nasazena v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí
Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení
Konzole pro centrální správu je kompletně multi-tenantní
Podpora produktů výrobcem nástroje bude poskytována v českém jazyce
Základní vlastnosti
Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu
Aktualizace pro dodávaný produkt po dobu 5 let
Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem
Možnost zasílat upozornění napojením na Syslog server
Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce
Úlohy správy bezpečnosti
Řešení umožňuje integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.
Řešení je schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery

Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity
Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy
Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy
Možnost restartování serveru nebo desktopu přímo z konzole centrální správy
Centralizované místo pro záznam všech úloh
Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)
Nastavení úrovně bezpečnosti
Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD
Reportování
Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě
Možnost zasílání vygenerovaných reportů e-mailem
Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv
Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen
Karanténa
Vzdálená obnova či smazání souboru v karanténě
Možnost automaticky přidat soubor do výjimky při obnově z karantény
Uživatelé
Více předdefinovaných rolí: Root, administrátor, reportér 1. Root: spravuje komponenty řešení 2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení 3. Reportér: spravuje a vytváří reporty
Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)
Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny
Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení
Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat
Logy
Zaznamenávání uživatelských akcí

Detailní log pro každou akci
Komplexní vyhledávání v logách
Správa a instalace ochrany
Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány
Instalace může být provedena několika způsoby, alespoň: 1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 3. Distribuce instalačního balíčku pomocí GPO či SCCM
Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN
Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou
Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci
Konzole správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích
Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů
Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou
Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat
Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti
Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)
Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body
Možnost spustit Network discovery z kteréhokoli již instalovaného klienta

3. Vlastnosti a funkce ochrany fyzických koncových bodů

Funkce
Podpora operačních systémů: Windows 11 Windows 10 Windows 8.1 Windows 8 Windows 7 Windows Server 2022

Ev. č. smlouvy kupujícího: VZ1295

Windows Server 2022 Core Windows Server 2019 Windows Server 2019 Core Windows Server 2016 Windows Server 2016 Core Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Ubuntu 14.04 LTS a vyšší CentOS 6.0 a vyšší Debian 8.0 a vyšší Mac OS X El Capitan (10.11) a vyšší
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
Detekce na základě virových definicí (tzn. signatur)
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
Detekce 0-day útoků na základě odhalování anomálního chování
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
Detekce 0-day bezsouborových útoků
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně

Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
Možnost automatického spuštění podezřelých souborů v Sandboxu
Možnost nastavení Sandboxu – délka pozorování po spuštění, počet opakování spuštění, přístup k internetu během detonace ano/ne
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
Možnost ručního vložení vzorku do Sandboxu
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
Řešení obsahuje funkce EDR integrované do jedné klientské aplikace spolu s EPP
Řešení podporuje možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
Řešení je schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
Řešení generuje detekce na základě automatizovaného hledání IoCs v datech sbíraných EDR senzorem
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
Řešení umožňuje analýzu vektoru útoku
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní
Možnost prověřovat http provoz
Možnost prověřovat provoz šifrovaný pomocí SSL
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic
Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
Ochrana proti podvodným a phishingovým webovým stránkám
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
Patch management

Součástí nástroje musí být možnost bezdotykové a vzdálené distribuce patchů
Distribuce konkrétní záplaty pro definovanou zranitelnost automaticky
Distribuce konkrétní záplaty pro definovanou zranitelnost z konzole na vyžádání administrátorem
Řešení má možnost definovat úložiště v lokální síti pro snížení dopadů na konektivitu do internetu
Možnost zobrazit stavu nainstalovaných / chybějících / nefunkčních záplat na koncovém zařízení
Součástí záplaty musí být informace (CVE, BuletinID)
Záplaty lze nástrojem distribuovat na fyzické a virtuální servery Windows, Golden image, pracovní stanice Windows a aplikace třetích stran.
Možnost odložení restartu pro záplaty.
Dostupné záplaty pro platformu Windows – desktopy a servery
Dostupné záplaty pro aplikaci MS Office
Dostupné záplaty pro aplikace výrobců: Adobe Acrobat, Adobe Reader, Google Chrome, Mozilla Firefox, Opera, Zoom client, WinZIP, VMware tools, Cisco WebEx
Firewall
Možnost blokovat skenování portů
Modul je možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS
Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb
Možnost vypnout IDS
Možnost nastavit profily známých sítí
Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu
Karanténa
Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě
Možnost obnovy souboru do originální či do nově zadané lokality
Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní)
Kontrola přístupu k internetu
· Zablokování přístupu na internet pro specifické stanice / skupiny stanic · Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic · Zablokování přístupu k internetu v určený čas · Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné) · Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)

Ev. č. smlouvy kupujícího: VZ1295

4. Vlastnosti a funkce ochrany virtualizovaných koncových bodů

Funkce
Podpora operačních systémů: Windows 11 Windows Server 2022 Windows Server 2022 Core Windows Server 2019 Windows Server 2019 Core Windows Server 2016 Windows Server 2016 Core Ubuntu 16.04 LTS a vyšší
Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen
„Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením
„Skenovací“ zařízení je možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže
Produkt umí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení
Řešení umožňuje optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)
Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů
Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru
Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
Detekce na základě virových definicí (tzn. signatur)
Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení

Detekce 0-day útoků na základě odhalování anomálního chování
Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
Detekce 0-day bezsouborových útoků
Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně
Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
Možnost automatického spuštění podezřelých souborů v Sandboxu
Možnost nastavení Sandboxu – délka pozorování po spuštění, počet opakování spouštění, přístup k internetu během detonace ano/ne
Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
Možnost ručního vložení vzorku do Sandboxu
Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
Řešení obsahuje funkce EDR integrované do jedné klientské aplikace spolu s EPP
Řešení podporuje možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
Řešení je schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
Řešení umožňuje analýzu vektoru útoku
Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
Možnost prověřovat http provoz
Možnost prověřovat provoz šifrovaný pomocí SSL
Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic
Modul pro ochranu mailboxů lokálně provozované Microsoft Exchange proti malwaru, spamu a phishingovým útokům

Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)
Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
Ochrana proti podvodným a phishingovým webovým stránkám
Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní
Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)

Nabízené produkty splňují veškeré technické požadavky definované zadavatelem v zadávací dokumentaci výběrového řízení.

5. Implementační služby

a. Obecné informace

- Do nabídky jsou zahrnuty veškeré další činnosti a prostředky, které jsou nezbytné v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Budou provedeny minimálně následující implementační práce:
  - (j) Dodávku nabízeného řešení,
  - (k) Nastavení bezpečnostních politik dle nejlepších postupů,
  - (l) Implementaci řešení,
  - (m) Implementace ochrany Exchange Serveru 2019,
  - (n) Implementace ochrany Active directory,
  - (o) Provedení školení,
  - (p) Zajištění zkušebního provozu,
  - (q) Provedení akceptačních testů,
  - (r) Předání do ostrého provozu.

- Veškerá dokumentace bude zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office, pdf).

b. Harmonogram realizace

- Dodávka nabízeného řešení v trial verzi (D+5)
- Implementace řešení, ochrany Exchange Serveru 2019 a ochrany Active directory (D+30)
- Nastavení bezpečnostních politik dle nejlepších postupů (D+30)

- Provedení školení (D+31 až 59 dle možností zadavatele)
- Zahájení zkušebního provozu (D+59)
- Provedení akceptačních testů (D+89),
- Dodávka ostrých licencí na 5 let a předání do ostrého provozu (D+90)
- Výše uvedené lhůty jsou maximální možné. Údaj D značí datum účinnosti smlouvy, čísla značí počet kalendářních dnů. Maximální doba realizace jsou 3 měsíce od okamžiku nabytí účinnosti Smlouvy.

c. Školení

- Bude zajištěno školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.
- Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- Školení administrátorů – minimální rozsah školení bud 16 hodin, předpokládaná účast max. 10 účastníků, školení bude probíhat v sídle Zadavatele. Zadavatel může změnit místo školení dle potřeby.
- Náklady na školení jsou zahrnuty v nabídkové ceně.

d. Akceptačních testy a přechod do zkušebního provozu

- Akceptační testy budou zahrnovat minimálně:
  (e) Prokázání kompletnosti dodávky a splnění povinných požadavků.
  (f) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
  (g) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
  (h) Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná.
- O provedení akceptace a jejím výsledku bude vyhotoven písemný akceptační protokol.
- Testovací provoz bude zajištěn v délce minimálně 30 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení v pracovní den v době od 8h do 16h.

e. Dokumentace

- Bude zpracována provozní dokumentace, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.
- Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Ev. č. smlouvy kupujícího: VZ1295

6. Záruka

Obecné informace

- záruka na celý systém 5 let,
- bude zajištěno, že dodaný systém bude po dobu záruky funkční a aktualizován,
- komunikace záručních oprav bude vedena v českém jazyce,
- pro hlášení záručních požadavků bude zajištěn provoz helpdeskové aplikace a telefonické podpory v režimu 24x7. Součástí helpdeskové aplikace bude reporting o průběhu řešení záručních požadavků,
- časový režim aktivní záruční podpory 8x5,
- je zajištěna doprava do místa plnění, včetně pojištění v rámci dopravy, cla a balného,
- záruční servis je poskytován bezplatně,
- zadavateli bude předán předávací protokol – dodací list.