SMLOUVA O DÍLO č. S170/2025/0075/OI

Zvýšení kybernetické bezpečnosti Městské části Praha 2

Městská část Praha 2
se sídlem: nám. Míru 600/20, 120 00 Praha 2
IČO: 00063461
DIČ: CZ00063461
zastoupena: Bc. Janem Kolářem., místostarostou
*dále jen „**zadavatel**“ na straně jedné*

a

Open Apps Development, a.s.
se sídlem: Kurta Konráda 2517/1, Libeň, 190 00 Praha 9
IČO: 116 49 275
DIČ: CZ11649275
č. účtu: [redacted]
zastoupena: Vlastou Šejvlovou, MBA, předsedkyní představenstva
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, pod sp. zn. B26495
*dále jen **„dodavatel“** na straně druhé*

*zadavatel a dodavatel dále též označováni jako „**smluvní strany**“ nebo „**účastníci smlouvy**“*

uzavřeli níže uvedeného dne, měsíce a roku tuto:

Smlouvu o dílo

(dále jen „***Smlouva***“)

Preambule a identifikace projektu

1. Tato smlouva je uzavírána na základě výsledku zadávacího řízení s názvem **„Zvýšení kybernetické bezpečnosti Městské části Praha 2“** uveřejněného ve Věstníku veřejných zakázek pod evidenčním číslem Z2025-045459 (dále jen **„veřejná zakázka"** nebo **„zadávací řízení").**

   Název projektu: Zvýšení kybernetické bezpečnosti Městské části Praha 2

   Registrační číslo projektu: CZ.31.2.0/0.0/0.0/24_145/0011560

   Informace o spolufinancování: Projekt je spolufinancován z EU

2. Cílem smlouvy je realizace kybernetických bezpečnostních opatření (produktů) vedoucích ke zvýšení bezpečnosti informační infrastruktury a informačních systémů zadavatele tak, aby byly naplněny požadavky na zajištění kybernetické bezpečnosti podle zákona č. 264/2025 Sb. o kybernetické bezpečnosti(dále jen „**zákon**“), včetně jeho prováděcích vyhlášek či nařízení, zejména vyhlášky č. 408/2025 Sb., regulovaných službách, vyhlášky č. 410/2025 Sb., o

bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, vyhlášky č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy, vyhlášky č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu a relevantních právních předpisů.(dále jen „**vyhlášky**“) ve spojení s implementací Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) – (dále jen „**NIS2**“) do českého právního řádu, a to v souladu s touto smlouvou, zadávací dokumentací a dotčenými právními předpisy.

3. Plnění této smlouvy bude spočívat v dodávce hardwarového vybavení, softwaru včetně příslušných licencí, zajištění řádné implementace, školení, zavedení ISMS, zajištění poskytování technické podpory výrobce a dalších činnostech, jak jsou popsány v zadávací dokumentaci a této smlouvě.

I.
Předmět smlouvy

1. Dodavatel se touto smlouvou zavazuje provést na svůj náklad a na své nebezpečí pro zadavatele dílo. Zadavatel se touto smlouvou zavazuje uhradit dodavateli za provedení díla a za zajištění jeho provozu a podpory dohodnutou cenu, to vše za podmínek v této smlouvě dále uvedených.
2. Dílem dle této smlouvy se rozumí:
    a) **dodávka hardware (dále „HW“) a software (dále SW) včetně základního nastavení prostředí,** která bude spočívat zejména v:
        i. vypracování cílového implementačního konceptu řešení
        ii. dodání HW zařízení do sídla zadavatele
        iii. instalaci HW v prostředí zadavatele, připojení do datové sítě LAN, zviditelnění a zpřístupnění zařízení pro provozní management,
        iv. dodávce a instalaci SW, včetně základního nastavení v prostředí zadavatele,
        v. poskytnutí licencí a předání licenčních klíčů dodávaného SW odpovědné osobě zadavatele,
        vi. ověření plné funkčnosti management konzolí HW zařízení a SW;

        (dále také jako „**etapa 1**“);
    b) **poskytnutí implementačních služeb a školení,** které budou spočívat zejména v:
        i. provedení kompletní konfigurace dodaných systémů podle této smlouvy a požadavků zadavatele,
        ii. integrace dodaných a stávajících systémů kybernetické bezpečnosti dle této smlouvy a požadavků zadavatele,
        iii. zaškolení administrátorů a klíčových uživatelů v potřebném rozsahu pro provádění provozního monitoringu systémů a aplikací jako celku i jednotlivě, osvojení detailní orientace v uživatelském prostředí managementu konzolí, osvojení schopností analýzy problémů v integračních nastaveních,

iv. předání základní provozní dokumentace, minimálně v rozsahu dle **Přílohy č. 6: *Obsah základní provozní dokumentace*,**

v. provedení 14denního testovacího provozu se zvýšenou podporou při nahlášení poruchy či provozního problému

(dále také jako „**etapa 2**“);

c) **zajištění poskytování technické podpory výrobce na 60 měsíců,** zadavatel předpokládá zahájení čerpání technické podpory výrobce od 1.4.2026

3. Ve vztahu k čl. I. odst. 2 písm. a) a b) shora se dodavatel se zavazuje dodat a provést dílo minimálně v rozsahu a v souladu s **Přílohou č. 1**: ***Cenová kalkulace*** *(včetně podrobného rozpisu dodávek)*, v rozsahu a souladu s požadavky stanovenými v **Příloze č. 2** této smlouvy***: Přehled produktů a jejich popis*** (v rozsahu produktů ID01 – ID07), jakož i v rozsahu a v souladu s **Přílohou č. 3** této smlouvy***: Technická specifikace*,** a způsobem, aby byly naplněny cíle dle čl. I. odst. 2 této smlouvy, což bude osvědčeno provedením výstupního auditu kybernetické bezpečnosti.

II.
Doba a místo plnění

1. Místem provádění díla je sídlo či určená pracoviště zadavatele.
2. Dodavatele se zavazuje dílo provést, tj. řádně dokončit a předat zadavateli **do 120 dní** ode dne účinnosti této Smlouvy, která je dána dnem zveřejnění v registru smluv.
3. Pro účely kontroly řádného a včasného provádění díla, jakož i pro účely plánování kapacit pro zajištění nezbytné součinnosti ze strany zadavatele je **Přílohou č. 4** této smlouvy: ***Harmonogram prací,*** zpracovaný dodavatelem, přičemž platí, že:
   a) dodavatel je povinen řádně provést **etapu 1** do 45 dní ode dne účinnosti této smlouvy,
   b) dodavatel je povinen řádně provést **etapu 2** do 120 dní ode dne účinnosti této smlouvy.
4. Před zahájením vlastních dodávek v rámci provádění díla předloží dodavatel zadavateli cílový implementační koncept řešení zpracovaný v souladu s požadavky uvedeným v Příloze č. 3: Technická specifikace. Cílový implementační koncept musí být předložen zadavateli nejpozději do 15 dní ode dne účinnosti smlouvy, s tím, že zadavatel je oprávněn uplatňovat připomínky, které je dodavatel povinen zapracovat. Oběma stranami odsouhlasená verze cílového implementační konceptu řešení je pro strany závazná a je nezbytnou podmínkou akceptace **etapy 1**.
5. K akceptaci díla či jeho etapy je dodavatel povinen vyzvat zadavatele nejméně 5 pracovních dnů před požadovaným dnem předání. Pro **etapu 2** platí, že lze k akceptaci vyzvat až po úspěšném absolvování testovacího provozu, který osvědčí funkčnost díla a způsobilost sloužit svému účelu.
6. Provedení **etapy 1** je podmíněno předáním této části díla a podpisem akceptačního protokolu stvrzujícího provedení **etapy 1** bez vad a nedodělků oběma smluvními stranami. V případě zjištění vad a nedodělků dohodnou smluvní strany lhůty pro jejich odstranění. Tehdy platí, že se **etapa 1** nepovažuje za řádně dokončenou a předanou, a to až do doby podpisu akceptačního protokolu stvrzujícího provedení díla bez vad a nedodělků, resp. stvrzující odstranění vytýkaných vad či nedodělků.
7. Provedení **etapy 2** je podmíněno předáním dokončeného díla a podpisem akceptačního

protokolu oběma smluvními stranami stvrzujícího provedení díla bez vad a nedodělků. Podpisem akceptačního protokolu se dílo považuje za předané. To neplatí pro případ, že bude akceptační protokol podepsán s výhradou, že je dílo provedeno s vadami a nedodělky, kdy pro tento případ dohodnou strany lhůty pro jejich odstranění. Dílo se považuje za řádně provedené, tj. dokončené a předané, až podpisem akceptačního protokolu potvrzujícího odstranění vad a nedodělků.

III.
Cena a platební podmínky

1. Celková cena díla činí **54 887 294 Kč včetně DPH**, tj. částku 45 361 400 bez DPH. Bližší rozklad dohodnuté ceny díla je obsažen v **Příloze č. 1** této smlouvy: ***Cenová kalkulace.***
2. Cena díla je dohodnuta jako nejvýše přípustná. Cenu díla je možné překročit pouze v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude k ceně připočtena DPH ve výši stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen **„zákon o dani z přidané hodnoty"**).
3. Cena díla zahrnuje veškeré náklady dodavatele spojené s provedením díla, ať již jsou touto smlouvou či cenovou nabídkou předpokládány či nikoliv.
4. Cena díla bude hrazena ve 3 splátkách, a to následovně:
    a) Cena za **etapu 1** díla bude hrazena po řádném provedení a akceptaci, tj. předání **etapy 1** díla.
    b) Cena za **etapu 2** díla bude hrazena po řádném provedení a akceptaci, tj. předání **etapy 2** díla.
    c) Cena za Technickou podporu výrobce na 60 měsíců bude hrazena po řádném předání **etapy 2** díla.
5. Podmínkou vzniku nároku na úhradu příslušné části ceny díla je vždy (a) podpis akceptačního protokolu zadavatelem, kterým bude potvrzeno, že byla příslušná etapa provedena bez vad a nedodělků, případně akceptačního protokolu stvrzujícího úplné odstranění vad a nedodělků, a současně (b) doručení příslušné faktury zadavateli v souladu s podmínkami stanovenými níže.
6. Splatnost každé faktury činí 30 dní od jejího prokazatelného doručení zadavateli.
7. Všechny faktury musí obsahovat náležitosti řádného daňového dokladu ve smyslu zákona o dani z přidané hodnoty a současně uvádět číslo smlouvy, slovní identifikaci díla: „Zvýšení kybernetické bezpečnosti Městské části Praha 2“, registrační číslo projektu: CZ.31.2.0/0.0/24_145/0011560 a označení fakturované etapy díla. Projekt je spolufinancován z EU.
8. V případě, že faktura bude obsahovat věcné či formální nesprávnosti, popřípadě nebude obsahovat všechny zákonné či dohodnuté náležitosti, je zadavatel oprávněn ji vrátit ve lhůtě splatnosti zpět dodavateli k doplnění či opravě, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury zadavateli.
9. Dodavatel není oprávněn požadovat úhradu jakýchkoliv záloh či požadovat fakturování díla po jiných částech, než jak je dohodnuto výše.
10. Příslušná faktura se považuje za uhrazenou dnem odepsání fakturované částky z bankovního účtu zadavatele.

11. Dodavatel prohlašuje, že není veden v registru nespolehlivých plátců, a zavazuje se po dobu trvání této smlouvy řádně a včas platit DPH. Pokud příslušný finanční úřad vyzve zadavatele k placení DPH nezaplacené dodavatelem při realizaci této smlouvy, dodavatel se zavazuje uhradit zadavateli smluvní pokutu ve výši odpovídající nezaplacené DPH. Pokuta je splatná ve lhůtě do 30 dnů ode dne doručení vyúčtování o smluvní pokutě.

IV.
Práva a povinnosti stran

1. Dodavatel je povinen dodat zadavateli úplné a funkční dílo, v množství, jakosti, provedení a termínu dohodnutých touto smlouvou.
2. Dodavatel výslovně prohlašuje, že má detailní obsahovou znalost zákona o kybernetické bezpečnosti 264/2025 Sb. a vyhlášek s ním souvisejících za účelem implementace směrnice NIS2 do českého právního řádu, jakož i výslovně potvrzuje a zavazuje se, že dílo bude již při předání splňovat všechny relevantní legislativní požadavky pro zajištění kybernetické bezpečnosti (i) podle právních předpisů platných a účinných ke dni podpisu této smlouvy a (ii) podle těch ustanovení budoucích právních předpisů vydaných v souvislosti s implementací směrnice NIS2, které se vztahují či budou vztahovat k funkčnímu rozsahu Díla**.**
3. Dodavatel se zavazuje provést na svůj náklad a na své nebezpečí všechna související plnění a práce potřebné k včasnému a řádnému provedení díla.
4. Zadavatel je povinen poskytovat dodavateli součinnost potřebnou pro řádné provádění díla. Provozní dokumentace zadavatele bude dodavateli zpřístupněna po podpisu této Smlouvy. Dodavatel je povinen respektovat a řídit se provozní dokumentací zadavatele tak, aby nedošlo k ohrožení/přerušení činnosti zadavatele.
5. Dodavatel je, nad rámec základní provozní dokumentace, povinen poskytnout zadavateli další nezbytné podklady s dílem související, a to zejména záruční listy a návody v českém jazyce a další dokumentaci vyplývající z platné legislativy, zejména zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.
6. Dodavatel prohlašuje, že ke dni uzavření této smlouvy má uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti dodavatele za škodu způsobenou jeho činností do výše limitu pojistného plnění v částce minimálně 20.000.000 Kč z každé pojistné události. Kopie pojistné smlouvy dodavatele, resp. pojistný certifikát byl předán zadavateli před podpisem této smlouvy, jako jedna z podmínek pro uzavření smlouvy. Dodavatel se zavazuje na žádost zadavatele bezodkladně, nejpozději však ve lhůtě do 5 pracovních dnů od doručení písemné výzvy zadavatele, předložit mu pojistný certifikát prokazující existenci a účinnost této pojistné smlouvy. Dodavatel se zavazuje, že pojistná smlouva dle věty první tohoto článku zůstane v účinnosti v tomto rozsahu po celou dobu trvání záruky dle této smlouvy.
7. Dodavatel je povinen neprodleně písemně vyrozumět zadavatele o případném ohrožení doby řádného splnění díla a o všech skutečnostech, které mohou řádné a včasné plnění díla znemožnit, a to nejpozději do 3 dnů ode dne, kdy se dodavatel o takových skutečnostech dozví.
8. Obě smluvní strany odpovídají za škodu, kterou způsobí druhé straně porušením svých povinností dohodnutých touto smlouvou nebo stanovených zákonem při poskytování plnění dle této smlouvy.
9. Dodavatel není oprávněn postoupit jakákoliv práva anebo povinnosti vyplývající z této smlouvy na třetí osoby bez předchozího písemného souhlasu zadavatele. Uplatní-li třetí osoba své

právo k dílu nebo jeho části, zavazuje se dodavatel bez zbytečného odkladu a na vlastní náklady učinit potřebná opatření k ochraně výkonu práv zadavatele.

10. Množství a rozsah v rámci díla poskytovaných, resp. převáděných licencí k příslušnému SW, vyplývá z Přílohy č. 3: *Technické parametry*. Odměna za poskytnutí licenčních oprávnění je zahrnuta v celkové ceně díla.

11. Dodavatel se zavazuje, že k HW a SW komponentám zajistí technickou podporu garantovanou výrobcem či poskytovatelem (dále jako „**výrobce**“) na 60 měsíců, což je povinen doložit potvrzením příslušného výrobce HW či SW. Technická podpora výrobce spočívá zejména v garanci schopnosti HW a SW plnit funkce a účel předpokládané touto smlouvou, včetně zajištění kompatibility s příslušnými operačními systémy, poskytování bezplatných aktualizací (nových verzí SW) tak, aby byla zajištěna jejich podpora do výše uvedeného data, aj.

12. Je-li součástí díla další plnění, které je předmětem ochrany práv podle autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění, poskytuje dodavatel zadavateli licenci, která zahrnuje právo užívat dílo či jeho část tak, aby mohlo dílo sloužit svému účelu. Tato licence je územně neomezená a poskytována minimálně po dobu trvání majetkových práv autora k autorskému dílu.

13. Zadavatel nabývá vlastnické právo k dílu dnem řádného předání a převzetí díla bez vad a nedodělků na základě podpisu akceptačního protokolu oběma smluvními stranami.

14. Smluvní strany sjednávají, že dodavatel není oprávněn jakékoliv jeho pohledávky za zadavatelem, které vzniknou na základě této smlouvy, započítat vůči pohledávkám zadavatele za dodavatelem jednostranným právním jednáním.

15. Dodavatel zajistí, že dílo nebude zatíženo právy třetích osob, ze kterých by pro zadavatele plynuly jakékoliv další finanční nebo jiné nároky třetích stran. Pokud by taková práva přesto existovala či v průběhu plnění vznikla, je dodavatel je povinen zajistit jejich bezplatný převod na zadavatele, a to v plném rozsahu a na vlastní náklady, respektive na vlastní náklady zajistit vypořádání nároků třetích stran.

16. Zadavatel je povinen zajistit aktuálnost veškerých přístupových oprávnění potřebných k softwarovým a hardwarovým produktům dodaným na základě této smlouvy (přístupová jména a hesla). To platí i o přístupových oprávnění k registracím licencí a služeb prostřednictvím internetu u jednotlivých výrobců či poskytovatelů, a to zejména jsou-li nezbytné pro aktualizace a údržbu daného SW a HW minimálně po dobu poskytování technické podpory jednotlivými výrobci.

17. Dodavatel je oprávněn využít pro realizaci díla poddodavatele uvedené v Příloze č. 7: Seznam poddodavatelů. Dodavatel je oprávněn změnit poddodavatele, pouze za předpokladu, že jeho změna byla zadavatelem předem odsouhlasena, a to i tehdy, pokud pomocí daného poddodavatele neprokazoval splnění kvalifikace. Zadavatel udělí souhlas se změnou poddodavatele, pokud k jeho neudělení nebude mít objektivní důvody. Pokud však dodavatel prokazoval splnění části kvalifikace pomocí poddodavatele, je oprávněn ho nahradit pouze takovým poddodavatelem, který splňuje požadovanou část kvalifikace ve stejném nebo větším rozsahu, což je povinen doložit a prokázat.

18. Dodavatel se dále zavazuje při realizaci této smlouvy dodržovat následující povinnosti:

    a) dodavatel zajistí dodržování veškerých právních předpisů vůči svým pracovníkům, zejména odměňování, pracovní dobu, dobu odpočinku mezi směnami, placené

přesčasy. Dále se zavazuje zajistit, že všechny osoby, které se na plnění zakázky budou podílet, jsou vedeny v příslušných registrech, například v registru pojištěnců ČSSZ;

a) s ohledem na ochranu životního prostředí, se dodavatel zavazuje k minimální produkci všech druhů odpadů, vzniklých v souvislosti s realizací díla. V případě jejich vzniku bude přednostně a v co největší míře usilovat o jejich další využití, recyklaci a další ekologicky šetrná řešení, a to i nad rámec povinností stanovených zákonem č. 541/2020 Sb., o odpadech;

b) při plnění předmětu veřejné zakázky zajistí legální zaměstnávání, férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby, které se na plnění veřejné zakázky podílejí, a to i u svých poddodavatelů,

19. Dodavatel se zavazuje udržovat a průběžně zlepšovat svůj systém řízení bezpečnosti informací (ISMS) v souladu s normou ISO/IEC 27001 nebo ekvivalentním rámcem tak, aby pokrýval veškeré plnění poskytované dle této smlouvy. Současně dodavatel prohlašuje jeho provozní procesy splňují požadavky zákona 264/2025 Sb., včetně prováděcích předpisů. a požadavky NIS2 směrnice (EU) 2022/2555 a navazující požadavky plynoucí z její implementace do českého právního řádu na řízení (pod)dodavatelského řetězce.

20. Dodavatel je povinen poskytnout na žádost zadavatele poskytovateli provozní, servisní a uživatelské podpory a užívání díla veškerou nezbytnou součinnost v souvislosti se zajištěním těchto činností.

21. Dodavatel prohlašuje, že on, jeho statutární orgán, majitel, konečný vlastník není uveden v žádných mezinárodních sankčních seznamech a že jeho majitel či konečný vlastník není občanem Ruské federace nebo Běloruské republiky a nevztahují se na něj žádné ekonomické sankce. Zejména v souladu s nařízením Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině dodavatel prohlašuje, že není Sankcionovanou osobou a neporušuje jakékoli Sankce. Dodavatel zejména prohlašuje, že:

    a) není osobou nebo subjektem, který je určeným cílem nebo který je jinak předmětem sankcí, včetně, ale nejen, v důsledku toho, že je takový subjekt vlastněn nebo jinak ovládán, přímo či nepřímo, jakoukoli fyzickou nebo právnickou osobou, která je určeným cílem sankcí nebo která je jinak předmětem sankcí (dále jen **„Sankcionovaná osoba");**

    b) neporušuje jakékoli zákony, předpisy, obchodní embarga nebo jiná omezující opatření týkající se hospodářských nebo finančních sankcí (zejména, ale nikoli výlučně, opatření týkající se financování terorismu) přijatá, spravovaná, prováděná a/nebo vynucená některým z následujících způsobů: (a) Organizací spojených národů a jakoukoli agenturu nebo osobu, která je řádně jmenována, zmocněna nebo oprávněna Organizací spojených národů k přijímání, správě, provádění a/nebo uplatňování těchto opatření; (b) Evropskou unií a jakoukoli agenturu nebo osobu, která je řádně jmenována, zmocněna nebo oprávněna Evropskou unií k přijímání, správě, provádění a/nebo uplatňování těchto opatření; a (c) vládou Spojených států amerických, ministerstvem, divizí, agenturou nebo kanceláří, včetně Úřadu pro kontrolu zahraničních aktiv (OFAC) ministerstva financí USA, ministerstva zahraničí USA a/nebo ministerstvo obchodu USA.

Dodavatel je současně povinen zajistit, aby jakýkoliv jeho poddodavatel splňoval podmínky učiněného prohlášení.

22. Dodavatel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a dále prohlašuje, že takovou obchodní společností není ani žádný z jeho poddodavatelů (dále jen **„Střet zájmů").**

23. Zjistí-li zadavatel, že dodavatel či poddodavatel je Sankcionovanou osobou, porušil či porušuje Sankce, je ve Střetu zájmů či jakýmkoliv jiným způsobem porušil či porušuje prohlášení uvedená v tomto článku smlouvy, je zadavatel oprávněn od této Smlouvy odstoupit.

V.
Oprávněné osoby, realizační tým

1. Oprávněnými osobami při provádění díla jsou za zadavatele:
   a) ve věcech smluvních: Bc. Jan Kolář, místostarosta, mail: jan.kolar@praha2.cz, tel.: +420 236 044 470
   b) ve věcech technických: Ing. Petr Štěpán, vedoucí odboru informatiky, mail: petr.stepan@praha2.cz, tel.: +420 236 044 225
2. Oprávněnými osobami při provádění díla jsou za dodavatele:
   a) ve věcech smluvních: [redacted]
   b) ve věcech technických: [redacted]
3. **V příloze č. 5:** ***Realizační tým*** je identifikováno složení realizačního týmu, tj. osob, které jsou pověřeny a oprávněny přímo se zúčastnit provádění díla a vystupovat a jednat za dodavatele, včetně jejich kontaktních údajů. Dodavatel prohlašuje, že veškeří členové realizačního týmu splňují a budou splňovat veškeré požadavky kladené na jejich roli při realizaci díla.
4. Pro účely uplatnění vad, záruk či jiných relevantních požadavků dle této Smlouvy je možné kontaktovat dodavatele prostřednictvím helpdesku/hot-line dodavatele:
   a) Mail: [redacted]
   b) Tel.: [redacted]
5. Dodavatel je povinen zajistit plnění smlouvy za přímé účasti osob (členů realizačního týmu), pomocí kterých byla prokázána kvalifikace v rámci veřejné zakázky, a to po celou dobu jejího trvání, a lze je vyměnit pouze s předchozím písemným souhlasem zadavatele. Tento souhlas bude dán, obdobně jako v případě dle odst. 17 shora, za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikační požadavky kladené na jejich roli dle Přílohy č. 5: *Realizační tým*. Účinnost změny v obsazení člena realizačního týmu nastává okamžikem udělení souhlasu s jeho změnou. Změna kontaktní osoby nebo člena realizačního týmu není důvodem k uzavření dodatku.
6. Veškerá korespondence, pokyny, oznámení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém jazyce a doručují se buď osobně, doporučenou poštou na adresu sídla smluvní strany, uvedenou v záhlaví smlouvy, e-mailem na adresy oprávněných osob

nebo prostřednictvím datové schránky na ID datové schránky smluvní strany, uvedené v záhlaví této smlouvy. Smluvní strany se v případě doručování zásilek formou doporučených dopisů dohodly tak, že zásilka je považována za doručenou 3. pracovní den bezprostředně následující po dni jejího odeslání prostřednictvím držitele poštovní licence na adresu příslušné smluvní strany dle záhlaví této smlouvy.

VI.
Záruky, vady, reklamace

1. Dodavatel se zavazuje dodat zadavateli pouze nový (ne starší 12 měsíců ode dne výroby) hardware. Dodávaný hardware a software musí být originální, nepoužitý ani nerepasovaný a musí být dodán s veškerými doklady, které se k němu vztahují, jsou potřebné k nabytí vlastnického práva a k jeho řádnému užívání. V databázi výrobce, pokud taková existuje, musí být zadavatel veden jako první uživatel zboží. Soulad s výše uvedenými skutečnostmi dodavatel doloží prohlášením o původu dodávaného zboží (včetně sériových čísel). Zadavatel si vyhrazuje právo kdykoli v průběhu plnění (nebo po podpisu) této smlouvy vyžádat si od dodavatele prokázání výše uvedených skutečností, a to prohlášením výrobce, eventuálně znaleckým posudkem či jiným srovnatelným způsobem.
2. Dodavatel se zavazuje, že dílo bude funkční a prosté vad a že bude mít vlastnosti a bude způsobilé sloužit účelu předpokládanému touto smlouvou a zadávací dokumentací. Dodavatel k dílu, jeho HW a SW komponentám, poskytuje záruku za jakost v délce trvání 60 měsíců od předání díla bez vad a nedodělků dle čl. II. odst. 6.
3. Dodavatel odpovídá za vady, které má dílo v době jeho předání zadavateli a dále poskytuje zadavateli záruku na vady díla, které vzniknou nebo se objeví v průběhu trvání záruční doby dle předchozího odstavce s výjimkou, že bude vada způsobena nesprávnou obsluhou, vyšší mocí nebo třetími osobami.
4. Zadavatel je povinen informovat dodavatele o jakékoliv vadě díla bez zbytečného odkladu po jejím vzniku.
5. Zadavatel je oprávněn reklamovat vady předmětu díla u dodavatele, a to písemnou formou po celou dobu trvání záruční doby. V reklamaci musí být popsána vada předmětu díla, určen nárok zadavatele z vady předmětu díla, případně požadavek na způsob odstranění vad, a to včetně termínu pro odstranění vad dodavatelem, který bude činit alespoň 3 dny, nedohodnou-li se smluvní strany jinak; vždy však platí, že je dodavatel povinen zahájit činnosti směřující k odstranění vady následující pracovní den od oznámení vady. Za písemnou formu uplatnění reklamace je považováno také nahlášení standardními prostředky technické podpory provozu, např. e-mailem nebo prostřednictvím HelpDesku/ hot-line uvedeným v čl. V smlouvy.
6. Smluvní strany ujednávají, že zadavatel má právo volby způsobu odstranění reklamované vady.
7. Dodavatel se zavazuje zajistit odstranění vad díla ve lhůtě stanovené zadavatelem, a to i tehdy, neuznává-li dodavatel odpovědnost za vady či příčiny, které ji vyvolaly a současně zahájit reklamační řízení v místě provádění předmětu díla. Odstranění vady není zadavatel oprávněn podmiňovat jakoukoliv předchozí úhradou či odsouhlasením takové úhrady. O reklamačním řízení budou dodavatelem pořizovány písemné zápisy ve dvojím vyhotovení, z nichž jeden stejnopis obdrží každá ze smluvních stran. Bude-li v reklamačním řízení vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno bezúplatně.

8. V případě, že dodavatel bude v prodlení s odstraněním vady, je zadavatel oprávněn zajistit odstranění vady třetí osobou, a to na náklady dodavatele, s čímž dodavatel výslovně souhlasí.
9. Za vady díla se nepovažují poruchy funkčnosti, které jsou důsledkem: (a) použití díla či jeho části pro jiné účely, než pro jaké je určen či jeho použití v rozporu s jeho účelem a poskytnutou dokumentací, (b) provedení změny díla či jeho části bez souhlasu zadavatele, (c) změny SW či HW, pokud tyto změny provedl zadavatel bez předchozí konzultace s dodavatelem, (d) vady či poruchy SW či HW, které nebyly předmětem díla, ale funkčnost díla je na nich závislá.
10. Reklamaci uplatní zadavatel u dodavatele nejpozději poslední den záruční doby. I reklamace odeslaná zadavatelem poslední den záruční doby se považuje za uplatněnou včas.
11. Záruční doba se prodlužuje o dobu, po kterou byly vady odstraňovány, a to ve vztahu k dílu jako celku.

VII.
Sankční ujednání

1. Pro případ prodlení dodavatele s provedením díla zaplatí dodavatel zadavateli smluvní pokutu ve výši 0,1 % z celkové ceny bez DPH za každý i započatý den prodlení s provedením díla.
2. Pro případ prodlení dodavatele s odstraněním vad či nedodělků uvedených v akceptačním protokolu zaplatí dodavatel zadavateli smluvní pokutu ve výši 20.000 Kč za každou vadu a každý, byť i započatý den prodlení, maximálně však do výše odpovídající polovině ceny díla.
3. Pro případ prodlení dodavatele s odstraněním vad uplatněných dle čl. VI. této smlouvy zaplatí dodavatel zadavateli smluvní pokutu ve výši 20.000 Kč za každou vadu a každý, byť i započatý den prodlení, maximálně však do výše odpovídající polovině ceny díla.
4. Smluvní strany sjednávají pro případ porušení povinnosti o ochraně informací čl. IX této Smlouvy smluvní pokutu ve výši 50.000 Kč za každý případ porušení.
5. V případě, že bude zadavatel v prodlení se zaplacením faktury dodavateli, je zadavatel povinen zaplatit dodavateli zákonný úrok z prodlení z fakturované částky dle aktuálně platné legislativy.
6. Za porušení povinnosti doložit pojistný certifikát prokazující existenci a účinnost pojistné smlouvy dle čl. IV. odst. 6 této Smlouvy zaplatí dodavatel zadavateli smluvní pokutu ve výši 0,05 % z minimální výše limitu pojistného plnění uvedeného tamtéž, a to za každý, byť jen započatý den, v němž bude dodavatel v prodlení s doložením pojistného certifikátu.
7. Za porušení povinnosti dodavatele provádět dílo za přímé účasti osob realizačního týmu, resp. osob u kterých je prokázána jejich kvalifikace (dle Přílohy č. 5: Realizační tým), je dodavatel povinen uhradit zadavateli smluvní pokutu ve výši 20.000 Kč za každý takový případ porušení a každou osobu, a to i opakovaně.
8. Smluvní pokuty stanovené dle tohoto článku jsou splatné do třiceti (30) dnů ode dne doručení výzvy k zaplacení smluvní pokuty povinné smluvní straně.
9. Zaplacením smluvní pokuty není dotčeno právo smluvní strany na náhradu škody vzniklé porušením smluvní povinnosti, které se smluvní pokuta týká, a to v plné výši.
10. Smluvní pokuty dle této smlouvy může zadavatel požadovat kumulativně. Smluvní pokutu je zadavatel oprávněn započíst oproti splatným pohledávkám dodavatele.

VIII.
Platnost a účinnost smlouvy

1. Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti okamžikem jejího uveřejnění v registru smluv. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona o č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, a s tímto uveřejněním souhlasí.
2. Platnost této smlouvy může být předčasně ukončena:
    a) písemnou dohodou smluvních stran;
    b) odstoupením zadavatele od smlouvy v případě jejího podstatného porušení ze strany dodavatele;
    c) výpovědí dodavatele, pokud bude zadavatel přes písemné upozornění dodavatele déle než 60 dnů od písemného upozornění v prodlení s plněním své platební povinnosti vůči dodavateli.
3. Za podstatné porušení smlouvy ze strany dodavatele se považuje zejména prodlení dodavatele s předáním díla delší než 30 dnů, porušení jakékoliv povinnosti dodavatele vyplývající ze smlouvy a její nesplnění ani v dodatečné lhůtě (alespoň 10 dnů), kterou zadavatel dodavateli poskytl a písemně jej na možnost odstoupení v případě nesplnění povinnosti upozornil. Odstoupení od smlouvy ze strany zadavatele není spojeno s uložením jakékoliv sankce k jeho tíži.
4. Výpovědní lhůta činí v případě výpovědi jeden měsíc a počíná běžet prvním dnem měsíce následujícího po měsíci, ve kterém byla písemná výpověď doručena druhé smluvní straně.
5. Odstoupení od smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně na adresu jejího sídla uvedené v záhlaví této smlouvy.
6. V případě odstoupení od smlouvy zadavatelem se tato smlouva zrušuje od počátku. V případě již poskytnutého plnění ze strany dodavatele se smlouva zrušuje co do zbytku nesplněné části plnění, ledaže by zadavatel prohlásil, že částečné plnění pro něj nemá význam. Dojde-li k předčasnému ukončení smlouvy jiným způsobem, je dodavatel oprávněn požadovat pouze uhrazení částky za již poskytnutá plnění, která jsou pro zadavatele samostatně využitelná a byla poskytnuta v souladu s podmínkami stanovenými touto smlouvou.
7. Odstoupením od této smlouvy zanikají všechny závazky smluvních stran z této smlouvy. V případě odstoupení od této smlouvy však nezanikají nároky smluvních stran na náhradu škody a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklé před skončením účinnosti této smlouvy, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví občanský zákoník.
8. Podstatným porušením této smlouvy, zakládajícím právo zadavatele na odstoupení od smlouvy, se rozumí rovněž případ, kdy příslušný orgán veřejné moci zjistí svým pravomocným rozhodnutím v souvislosti s plněním této smlouvy porušení obecně závazných právních předpisů.

IX.
Ochrana informací

1. Dodavatel a zadavatel se zavazují zachovávat mlčenlivost ve vztahu k důvěrným informacím, které získají či jim budou zpřístupněny v průběhu poskytování plnění dle této smlouvy. Za

důvěrné informace se považují zejména zprávy týkající se vnitřních záležitostí smluvních stran a předmětu plnění smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou stranu, zejména veškeré informace, které se týkají obsahu, struktury a zabezpečení informačních a komunikačních systémů zadavatele či jeho provozní dokumentace a také informace výslovně jako důvěrné označené.

2. Dodavatel je povinen zabezpečit veškeré podklady poskytnuté mu zadavatelem, které mají charakter či obsahující důvěrné informace proti krádeži, odcizení či jakémukoliv zneužití.
3. Dodavatel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv zadavatele nejméně ve stejném rozsahu, v jakém je v závazkovém vztahu zavázán sám.
4. Smluvní strany se zavazují, že neuvolní třetí osobě informace druhé strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací.
5. V souvislosti s důvěrností informací bere dodavatel na vědomí, že je zákonnou povinností zadavatele uveřejnit celé znění této smlouvy včetně všech jejich případných dodatků a seznamu poddodavatelů v souladu se zákonem o registru smluv. Splnění této, jakož i dalších zákonných povinností zadavatele (např. poskytnutí smlouvy dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů), není porušením důvěrnosti informací.
6. Povinnost zachovávat mlčenlivost se dále nevztahuje na informace:
    a) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak než porušením ustanovení tohoto odstavce ze strany dodavatele,
    b) které jsou smluvní straně známy a byly ji volně k dispozici ještě před přijetím těchto informací od druhé smluvní strany,
    c) které je smluvní strana povinna poskytnout na základě zákona či rozhodnutí příslušného orgánu státní správy.
7. Po ukončení účinnosti této smlouvy je každá ze smluvních stran povinna bez zbytečného odkladu vrátit druhé smluvní straně všechny poskytnuté materiály obsahující důvěrné informace včetně jejich případně pořízených kopií. O předání a převzetí se sepíše protokol podepsaný oběma smluvními stranami (jejich zástupci ve věcech technických, případně smluvních).
8. Za prokázané porušení ustanovení v tomto článku má druhá smluvní strana právo požadovat náhradu takto vzniklé škody. Práva a povinnosti uvedené v tomto článku zůstávají v platnosti po dobu 5 let po ukončení tohoto smluvního vztahu, a to i v případě, že by došlo k předčasnému ukončení smlouvy.

X.
Závěrečná ustanovení

1. Vztahy mezi smluvními stranami se řídí českým právním řádem. Ve věcech smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními občanského zákoníku a ostatními obecně závaznými právními předpisy.
2. Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu písemně oznámit druhé smluvní straně a vyvolat

jednání zadavatele a dodavatele.

3. Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují, že bezodkladně nahradí neplatné ustanovení této smlouvy jiným platným ustanovením svým obsahem podobným neplatnému ustanovení.
4. Tato smlouva je uzavřena v souladu s usnesením Rady Městské části Praha 2 číslo 598 ze dne 6.10. 2025.
5. Tato smlouva nabývá platnosti podpisem oběma zástupci smluvních stran a účinnosti zveřejněním v registru smluv, které po dohodě smluvních stran provede zadavatel.
6. Obě smluvní strany se dohodly, že budou smlouvu podepisovat elektronicky prostřednictvím kvalifikovaného elektronického podpisu.
7. Nedílnou součástí této smlouvy jsou následující přílohy
    a) Příloha č. 1: *Cenová kalkulace (včetně podrobného rozpisu dodávek)*
    b) Příloha č. 2: *Přehled produktů a jejich popis*
    c) Příloha č. 3: *Technická specifikace*
    d) Příloha č. 4: *Harmonogram prací*
    e) Příloha č. 5: *Realizační tým*
    f) Příloha č. 6: *Obsah základní provozní dokumentace*.
    g) Příloha č. 7: *Seznam poddodavatelů*
8. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

V Praze dne dle data el. podpisu

V Praze dne dle data el. podpisu

za zadavatele
Bc. Jan Kolář, místostarosta

za dodavatele
Vlasta Šejvlová, MBA, předsedkyně představenstva

Příloha č. 1: Cenová kalkulace (včetně podrobného rozpisu dodávek)

CENOVÁ KALKULACE

		Cena v Kč bez DPH		
ID produktu	**Název produktu**	**Etapa 1 - Dodávka HW, SW licencí**	**Etapa 2 - Služby implementace a školení**	**Technická podpora výrobce na 60měsíců**
01	Nástroj na detekci kybernetických bezpečnostních událostí (EDR,XDR,NDR)	7 729 400,00 Kč	400 000,00 Kč	4 454 000,00 Kč
		Cena v Kč s DPH		
		9 352 574,00 Kč	484 000,00 Kč	5 389 340,00 Kč

		Cena v Kč bez DPH		
ID produktu	**Název produktu**	**Etapa 1 - Dodávka HW, SW licencí**	**Etapa 2 - Služby implementace a školení**	**Technická podpora výrobce na 60měsíců**
02	MFA (Vícefaktorové ověřování)	1 540 000,00 Kč	100 000,00 Kč	996 000,00 Kč
		Cena v Kč s DPH		
		1 863 400,00 Kč	121 000,00 Kč	1 205 160,00 Kč

		Cena v Kč bez DPH		
ID produktu	**Název produktu**	**Etapa 1 - Dodávka HW, SW licencí**	**Etapa 2 - Služby implementace a školení**	**Technická podpora výrobce na 60měsíců**
03	Kompletní správa životního cyklu logů	2 289 000,00 Kč	200 000,00 Kč	1 379 000,00 Kč
		Cena v Kč s DPH		
		2 769 690,00 Kč	242 000,00 Kč	1 668 590,00 Kč

		Cena v Kč bez DPH		
ID produktu	**Název produktu**	**Etapa 1 - Dodávka HW, SW licencí**	**Etapa 2 - Služby implementace a školení**	**Technická podpora výrobce na 60měsíců**
04	Bezpečnostní Dasboard	2 650 000,00 Kč	413 000,00 Kč	1 542 000,00 Kč
		Cena v Kč s DPH		
		3 206 500,00 Kč	499 730,00 Kč	1 865 820,00 Kč

ID produktu	Název produktu	Cena v Kč bez DPH		
		Etapa 1 - Dodávka HW, SW licencí	Etapa 2 - Služby implementace a školení	Technická podpora výrobce na 60měsíců
05	DLP (data loss prevention)	1 690 000,00 Kč	100 000,00 Kč	860 000,00 Kč
		Cena v Kč s DPH		
		2 044 900,00 Kč	121 000,00 Kč	1 040 600,00 Kč

ID produktu	Název produktu	Cena v Kč bez DPH		
		Etapa 1 - Dodávka HW, SW licencí	Etapa 2 - Služby implementace a školení	Technická podpora výrobce na 60měsíců
06	Zavedení systému ISMS a dodávka nástroje na risk management, zajištění kompatibility s legislativou	2 290 000,00 Kč	341 600,00 Kč	1 320 000,00 Kč
		Cena v Kč s DPH		
		2 770 900,00 Kč	413 336,00 Kč	1 597 200,00 Kč

ID produktu	Název produktu	Cena v Kč bez DPH		
		Etapa 1 - Dodávka HW, SW licencí	Etapa 2 - Služby implementace a školení	Technická podpora výrobce na 60měsíců
07	Zabezpečené datové úložiště (provozní a bezpečnostní logy, archivace a zálohování)	9 880 400,00 Kč	200 000,00 Kč	4 987 000,00 Kč
		Cena v Kč s DPH		
		11 955 284,00 Kč	242 000,00 Kč	6 034 270,00 Kč

Cena celkem – hodnotící kritérium (stanovená jako součet položky za ID01-ID07)

Položka	Cena v Kč bez DPH	Cena v Kč s DPH
Celkem Etapa 1 - Dodávka HW, SW licencí (ID01+ID02+ID03+ID04+ID05+ID06+ID07)	28 068 800,00 Kč	33 963 248,00 Kč
Celkem Etapa 2 - Služby implementace a školení (ID01+ID02+ID03+ID04+ID05+ID06+ID07)	1 754 600,00 Kč	2 123 066,00 Kč
Celkem Technická podpora výrobce na 60 měsíců (ID01+ID02+ID03+ID04+ID05+ID06+ID07)	15 538 000,00 Kč	18 800 980,00 Kč
Cena celkem – hodnotící kritérium (Etapa 1 + Etapa 2 + Technická podpora výrobce na 60 měsíců)	**45 361 400,00 Kč**	**54 887 294,00 Kč**

ROZPIS DODÁVEK

Seznam dodaných HW a SW komponent – dodávka ID 01-07

Produkt ID	Typ (HW nebo SW)	Název výrobce	Označení (model nebo název používaný výrobcem)	Množství
1	SW	[redacted]		1
1	SW			450
1	SW			501
2	SW			450
3	HW			1
4	SW			1
5	SW			450
6	SW			1
7	HW			2
7	SW			1
7	HW			4

Příloha č. 2: Přehled produktů a jejich popis

POPIS PRODUTŮ

Produkt	Popis	Funkce
ID01 Nástroj pro detekci kybernetických bezpečnostních událostí (EDR/XDR)	Požadujeme nástroj pro aktivit koncových zařízení, který dokáže identifikovat a reagovat na nestandardní nebo nežádoucí chování zařízení na počítačové síti. Typicky je požadována automatizovaná detekce a reakce na incidenty a zajištění maximální ochrany před šířením škodlivých kódů přes počítačovou síť v reálném čase. Požadované pokrytí je min. 300 koncových zařízení a min. 80 serverů (fyzické i virtualizované prostředí). Očekáváme implementaci technologií pro zabezpečení sítě v rozsahu (Network Detection Response) zahrnující hloubkovou inspekci datových paketů, sandboxing a detekci malwaru. Systém ochrany koncových zařízení musí poskytnout informace pro forenzní vyšetřování incidentů. Součástí řešení by měly být síťové pasti (Honeypots) pro identifikaci útoků a mechanismy pro jejich včasnou detekci a následnou analýzu v sandboxu. Zadavatel již část těchto technologií vlastní a provozuje.	Monitoring provozu datové sítě a komunikace koncových zařízení s identifikací nestandardního chování
ID02 MFA (Vícefaktorové ověřování)	Systém vícefaktorového ověřování musí podporovat kombinaci několika metod ověření identity uživatele (450 uživatelů) pro zvýšení bezpečnosti přístupu k aplikacím a uživatelským účtům na koncových zařízeních. Systém by měl být kompatibilní s běžně používanými operačními systémy (Windows, Linux, MacOS). Systém musí být uživatelsky přívětivý, minimalizovat dopad na běžné pracovní procesy a zároveň zachovat vysokou úroveň zabezpečení. Systém by měl umožňovat nastavení různých časových intervalů pro vynucení opětovného ověření a měl by umožňovat nastavit nevynucované ověření v případě připojení uživatele z lokální sítě úřadu. Kromě zadání tradičního hesla nebo PIN kódu musí systém umožnit vyžádání druhého faktoru ověření. Systém musí podporovat alespoň následující metody ověření: • SMS kód • Autentizační aplikace • Kvalifikovaný certifikát na čipové kartě	Vícefaktorové ověřování podporující několik metod ověření identity uživatele

Produkt	Popis	Funkce
ID03 Nástroj na sběr a vyhodnocování logů	Požadujeme systém log-management s neomezeným sběrem logů (provozní a bezpečnostní logy), který dokáže zpracovávat události z různých zdrojů – aplikace, operační systémy, zařízení počítačové sítě, další hw zařízení připojená do počítačové sítě. Systém musí umožnit dopsání komunikačních analyzátorů (parser) pro zařízení přímo nepodporované výrobcem systému log-managementu bez nutnosti spolupráce s ním (otevřená architektura). Požadujeme standardizaci přijatých logů do jednotného formátu a jejich automatické indexování pro snadné a rychlé vyhledávání. Data uložená v log-management systému musí být chráněna před modifikací, smazáním nebo jiným poškozením, systém musí podporovat jejich konsolidaci na centrálním úložišti. Očekáváme snadné ad hoc vyhledávání událostí bez nutnosti programování (přes uživatelské rozhraní) a grafické znázornění klíčových statistik, včetně GeoIP, DNS informací a dalších informací nutných pro forenzní vyšetřování incidentů. Předpokládá se průběžné uchování a zpracování logů za období min. 12 měsíců a nativní podpora virtualizace.	Neomezený sběr logů a událostí z různých zdrojů s plně autonomním provozem
ID04 Bezpečnostní Dashboard	Požadujeme jednotnou platformu pro technologický a bezpečnostní monitoring, která zajistí viditelnost incidentů ze všech zařízení a součástí KB řešení a poskytne detailní a strukturovaný pohled na provoz IT infrastruktury a agendových a podpůrných aplikací. Systém musí být schopen kontinuálně shromažďovat a analyzovat data z různých KB systémů a zařízení, jako je log-management, SIEM, XDR a provozního dohledu Zabbix, Nagios aj. a umožnit rychlé vyhodnocení aktuálního stavu IT infrastruktury a dostupnosti/funkčnosti monitorovaných aplikací. Očekáváme možnost definovat závislosti mezi jednotlivými hw a sw prvky IT provozu, což usnadní identifikaci rozsahu případných problémů a závislostí v řetězci zdrojů. Pracovníci dohledu musí mít možnost snadno identifikovat příčinu problémů a rychle na ně reagovat. Systém by měl uchovávat data za	Integrační platforma pro zobrazování, hodnocení incidentů a korelaci informací z provozních a security řešení

Produkt	Popis	Funkce
	zvolené období a generovat pravidelné management reporty, které poskytnou klíčové informace pro řízení IT infrastruktury a její optimalizaci. Požadujeme podporu nástrojů pro sledování/vyhodnocovaní historických dat s cílem zlepšit efektivitu a dlouhodobý rozvoj IT prostředků.	
ID05 DLP (data loss protection nástroj)	Nástroj pro monitoring práce s daty a soubory a ochranou před ztrátou. Systémový přístup k monitorování a ochraně citlivých dat díky nástroji DLP zabezpečuje proti únikům, krádeži a neoprávněnému sdílení. Hlavní funkce • Klasifikace a identifikace citlivých dat • Monitorování činností uživatelů s daty • Prevence úniku dat (Data Leak Prevention) • Nastavení pravidel a politik • Blokování rizikových aktivit v reálném čase • Audit a protokolování aktivit • Soulad s legislativou a standardy	Monitoring práce s daty, soubory a nastavení pravidel/politik pro jejich ochranu před ztrátou nebo zneužitím.
ID06 Zavedení systému ISMS dle zákona o kybernetické bezpečnosti (systém řízení bezpečnosti informací) a dodání platformy pro řízení kybernetické bezpečnosti se schopností automatizovaného reportingu o stavu organizace v rámci zavedeného ISMS	Opatření bude realizováno dodavatelským zajištěním role osoby odpovědné za kybernetickou bezpečnost/managera kybernetické bezpečnosti. Ten v rámci své činnosti vytvoří systém řízení bezpečnosti informací odpovídající povinnostem stanovených novelizací zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Vytvořená dokumentace musí jasně definovat odpovědnosti, jak pro organizační opatření (např. řízení přístupu, bezpečnost dodavatelského řetězce, správu změn a konfigurací), oblast lidských zdrojů (např. změna pracovního poměru, práce na dálku), tak opatření technická – fyzická bezpečnost (např. fyzický vstup, zabezpečení kanceláří, místností a vybavení) a technologická oblast (např. logování, oddělení sítí, kryptografie). Součástí musí být také vytvoření základních metodických pokynů pro zaměstnance, dodavatele a třetí strany, které stanoví závazné postupy a pravidla pro bezpečné nakládání s informacemi a aktivy organizace. Výsledkem bude ucelený systém řízení bezpečnosti informací, podpořený odpovídající dokumentací, který zajistí soulad s požadavky NIS2 a umožní	V rámci realizace opatření dojde k vytvoření dokumentace, nastavení procesů a rolí tak, aby byl žadatel plně v souladu se zákonem č. 264/2025 Sb. a prováděcími předpisy k implementaci směrnice NIS2. Systém bude implementován do online provozovaného standardního nástroje usnadňujícího následnou správu systému a plnění zákonných povinností včetně plného řízení

Produkt	Popis	Funkce
	efektivní řízení bezpečnostních rizik. Součástí dodávky bude implementace systému do standardizovaného softwarového prostředí/platformy, které bude propojovat obecné výsledky a vytvořené postupy s reálnými daty z monitorovacích systémů provozovaných v prostředí zadavatele (např. servisdesk, logmanagement nebo monitoring). Vytvořený systém v rámci online platformy musí podporovat provádění těchto činností v souladu s vybranými EU normami a jejich implementacemi do národních prostředí tedy standardy ISO 27001, NIS2, DORA, TISAX. V případě NIS a NIS2 bude podporovat jejich implementace národní legislativy v podobě zákona o kybernetické bezpečnosti včetně prováděcích předpisů. Systém umožní automatizovaně a dynamicky definovat nové normy formou katalogů hrozeb, zranitelností a opatření. Součástí řešení musí být mapa aktiv a jejich souvztažností. V případě kontroly ze strany NÚKIB bude systém obsahovat veškerou nutnou dokumentaci a záznamy v rámci dané úrovně povinností, včetně ad hoc generovaných záznamů v oblasti řízení aktiv a rizik např. plán opatření a aktivit (PoA), plán zvládání rizik (PZR) či zhodnocení rizik (ZHR).	aktiv a rizik a možnosti automatizovaně a dynamicky definovat případné nové normy formou katalogů hrozeb, zranitelností a opatření. Součástí opatření bude dodavatelské zajištění výkonu role osoby odpovědné za kybernetickou bezpečnost v organizaci žadatele.
ID07 Zabezpečené datové úložiště pro provozní a bezpečnostní logy včetně aplikačních dat ISMS	I. HW pro lokalitu ÚMČ Praha 2 1. Diskový systém typu All flash s ochranou proti modifikaci dat ransomwarem a zaručenou nesmazatelností a autenticitou dat s primárním využitím pro ukládání a analýzu bezpečnostních logů o kapacitě min. 100 TB bez single point of Failure 2. Diskový systém s ochranou proti modifikaci dat ransomwarem a zaručenou nesmazatelností a autenticitou dat s primárním využitím pro zálohování a archivaci o kapacitě min. 200 TB bez single point of failure II. SW licence a předplatné pro provoz úložiště ve virtualizovaném prostředí cloudu ÚMČ Praha 2 1. Virtualizovaná verze úložiště dat s ochranou proti modifikaci dat ransomwarem a zaručenou nesmazatelností a autenticitou dat s primárním	Bezpečné izolované datové úložiště pro provozní a bezpečnostní logy a další kritická data

Produkt	Popis	Funkce
	využitím pro ukládání a analýzu bezpečnostních logů o kapacitě min. 2x 10 TB bez single point of Failure	

Příloha č. 3: Technická specifikace

SPOLEČNÉ REALIZAČNÍ POŽADAVKY NA DODÁVKU ID 01 - 07
Cílový stav
Zadavatel poptává vždy hotový systém, ne vývoj na zakázku. Celý systém musí být nativně integrovatelný do IT infrastruktury zadavatele, po zaškolení obsluhovatelný a konfigurovatelný lidskými zdroji zadavatele bez nutnosti žádat o konfigurační úpravy dodavatele. Veškeré konfigurační nástroje musí být zadavateli dostupné bez nutnosti zapojení dodavatele.
Rozsah licence
Zadavatel požaduje u SW komponent stálou (tzv. perpetual) licenci, která bude pokrývat jeho IT infrastrukturu. Popis provozního prostředí na vyžádání a podpisu NDA. Součástí dodávky musí být i kompletní podpora výrobce v rozsahu dodávaných SW a HW komponent na dobu min. 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze systému, požadované funkce zařazené na tzv. roadmapu nebudou akceptovány.
Služby implementace a školení
Pokud není uvedeno jinak v technické specifikaci konkrétního ID pak se Službami implementace a školení rozumí zejména: - instalace všech HW a SW součástí řešení - provedení potřebných analýz v prostředí zadavatele za účelem co nejefektivnějšího nasazení HW a SW prostředků, splnění integračních požadavků na další systémy zadavatele - připojení HW zařízení do sítě LAN a jejich zpřístupnění pro sdílení a monitoring - nastavení pravidel komunikace a monitoringu IT zařízení v LAN - provedení specifické konfigurace podle role zařízení - iniciace licencí na portálu výrobce ve prospěch zadavatele - tvorba a realizace testovacích scénářů před uvedením systému do produkce - akceptované předání do produkce -. příprava požadovaných výstupů/reportů Zaškolení administrátorů a klíčových uživatelů aplikace nebo systémového rozhraní v rozsahu: - nutném pro běžný provozní monitoring a základní analýzu provozních problémů - ovládání a orientaci v uživatelském rozhraní - nastavení bezpečnostních pravidel a správu uživatelských rolí - popis nastavení integrací na další IT a KB systémy v prostředí zadavatele
Testovaní v prostředí zadavatele před uzavřením smlouvy
V případě, že si v průběhu hodnocení veřejné zakázky zadavatel nebude jistý hodnotami technických parametrů řešení nabízených uchazečem, zadavatel bude požadovat po uchazeči vytvoření testovacího prostředí v IT infrastruktuře zadavatele, na kterém bude účastník všechny požadované parametry schopen demonstrovat.
Cílový implementační koncept řešení
Cílový implementační koncept řešení bude obsahovat definici základních milníků realizace etapy 1 a etapy 2 v kontextu Přílohy č. 4 Harmonogram prací, návaznost jednotlivých kroků realizace řešení a definici případných závislostí, popis rozsahu integrace jednotlivých produktů do prostředí zadavatele v souladu s cíli předmětu smlouvy, specifikaci informací, které bude muset zadavatel poskytnout nad rámec zpřístupněné Provozní dokumentace a další relevantní informace.
Technická podpora výrobce na HW a SW komponenty

Je požadována technická podpora výrobce na 60 měsíců. Zadavatel předpokládá čerpání technické podpory od 1.4.2026.

ID 01 Nástroj pro detekci kybernetických bezpečnostních událostí (EDR/XDR/NDR)

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
EDR (End Point Detection and Response)		
DETEKČNÍ FUNKCE/SCHOPNOSTI		
Systém je cíleně navržen jako nástroj pro bezpečnostní specialisty a SOC týmy pro podporu jejich práce a poskytuje detailní síťovou vizibilitu na dění na koncových bodech a implementuje detekční metody relevantní známým i novým bezpečnostním hrozbám.	ANO	Fidelis Endpoint je cíleně vytvořen a vyvíjen jako bezpečnostní platforma pro podporu práce SOC a CIRT týmů a implementuje několik detekčních metod, pro rozpoznání nových i známých hrozeb na koncových bodech.
Pokročilá detekce hrozeb: - detekce škodlivého kódu jeho rozpoznáním podle vzorů pro obsah - detekce škodlivého kódu pomocí pravidel popisující chování, - detekce projevů činnosti útočníka na koncovém bodě, - analýza běžících procesů na stanici a jejich ohodnocení z hlediska činností, které provádějí nebo by mohly provádět.	ANO	Všechny uvedené detekční metody jsou podporovány.
Systém musí klasifikovat události podle MITRE ATT&CK frameworku uvedením odpovídající techniky a/nebo taktiky útočníka.	ANO	Systém mapuje detekce na taktiky a techniky dle MITRE ATT@CK. Toto je možné využít i pro vlastní pravidla.
Systém bude možné napojit na vlastní nebo otevřené zdroje informací o hrozbách ve formátech JSON, CSV a STIX.	ANO	Vlastní popis hrozeb lze do systému dodat jako feed(y) a jsou podporovány všechny uvedené formáty.
Systém musí rozpoznat zranitelnosti nainstalovaného software na koncových bodech.	ANO	Systém získává seznam nainstalovaného software na koncovém bodě a porovnává jej s CVE databází. Výstupem jsou rozpoznané zranitelnosti pro každý koncový bod.
Systém bezpečnostního monitorování koncových zařízení (stanic a serverů) s integrovanou funkcionalitou EDR.	ANO	Systém Fidelis Endpoint je od počátku navržen jako EDR řešení.
Systém bude kontinuálně zaznamenávat činnosti na koncových bodech v podobě meta-dat v těchto oblastech: - spuštění a ukončení procesů,	ANO	Všechny uvedené činnosti na koncových bodech jsou monitorovány a sbírány v podobě tzv. Behaviors – prakticky jde o

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
- souborové manipulace, - manipulace s registry, - síťových spojení včetně URL pro http spojení, - DNS překladů, - Manipulace s USB médii a přenosy souborů na ně, - Windows události (Windows Events).		metadata popisující chování procesů.
Vlastní pravidla lze definovat tak, aby také používala kategorie MITRE ATT&CK frameworku.	ANO	Vlastní pravidla mohou také používat taxonomii MITRE ATT@CK.
Systém bude umožňovat import popisu IOC ve formátu OpenIOC a YARA.	ANO	Oba zmíněné formáty jsou podporovány.
VYŠETŘOVACÍ FUNKCE/SCHOPNOSTI		
Systém umožní zhodnocení hrozby integrací na službu Virus Total nebo obdobnou službu.	ANO	Systém využívá službu pro ohodnocení souborů dle hash s daty odpovídajícími Virus Total.
Systém musí umožnit přístup ke koncovému bodu pomocí sezení v reálném čase (konzolový přístup) pro účely vyšetřování a reakce.	ANO	Pokryto schopností vystavit terminálové sezení s koncovým bodem přímo z webového rozhraní systému. Využívá cmd.exe a bash na koncovém bodě.
Systém bude umožňovat vyhledávání souboru i pro smazané soubory.	ANO	Pokryto úlohou pro vyhledávání souboru s volbou pro hledání i mezi smazanými soubory.
Systém bude umožňovat vyhledávání v metadatech dle libovolného parametru události (například jméno procesu, jméno rodiče, PID, hash, jméno souboru, jméno klíče v registrech, IP adresa serveru, URL spojení).	ANO	Ale vytvořit sofistikovaný výraz obsahující relační podmínky spojené logickými operátory.
V případě potřeby musí být systém schopný spustit rozšířené úlohy zjišťující stav koncového bodu v oblasti: - získání historie navštívených stránek webového prohlížeče - získání záznamu síťového provozu koncového bodu - získání obrazu logického disku nebo fyzického disku - získání obrazu paměti	ANO	Pokryto úlohami

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém musí být schopný zobrazit činnosti určitého procesu ve vztahu k: - souborovým manipulacím - manipulacím s registry - síťovým spojením - spuštěným podprocesům - to vše graficky na časové ose.	ANO	Pokryto úlohami
Systém bude pro běžící procesy schopen zaznamenat: - otevřené sokety - souborové manipulace - informace o DLL, které byly dynamicky přilinkovány včetně informace, zda byly injektovány - obsazený virtuální adresní prostor - identitu, pod kterou byl proces spuštěn.	ANO	Pokryto úlohami
Systém musí být schopen na vyžádání – nebo jako součást automatické reakce – získat informace o okamžitém stavu koncového bodu minimálně v oblastech: - přihlášení uživatelé - vystavená síťová spojení - běžící procesy - seznam zavedených lokálních správců - seznam nainstalovaného software - seznam nainstalovaných důvěryhodných certifikátů - čas od spuštění počítače - stav antiviru - stav firewallu - seznam do paměti nahraných ovladačů - seznam klíčů a hodnot autorun v registrech - výpis obsahu DNS a ARP vyrovnávacích pamětí - HW inventář - obsah směrovací tabulky - seznam aktivních síťových rozhraní.	ANO	Pokryto úlohami
Systém musí být schopen nalézt soubor na disku koncového bodu dle: - obsahu - hashe - názvu - velikosti - koncovky	ANO	Pokryto úlohami

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
- času vytvoření/modifikace - kombinace výše uvedeného.		
Události budou zaznamenávány do centrálního úložiště v reálném čase a budou zpětně dostupné s časovou retencí požadovanou Zadavatelem.	ANO	Události jsou zaznamenávány do tzv Datastore, což je databáze, ve které lze vyhledávat historické události.
REAKČNÍ FUNKCE/SCHOPNOSTI		
Systém umožní provedení akce na koncovém bodě nebo bodech odesláním úlohy k provedení a také interakcí s koncovým bodem v reálném čase.	ANO	Úlohy a terminálové sezení pokrývají tento požadavek.
Systém musí umožnit na stanici: - smazat soubor - ukončit proces - síťová izolace koncového bodu (při zachování komunikace systému s EDR řešením) - modifikace/mazání obsahu registrů - instalace a odinstalace aplikací a záplat - odhlášení uživatele - zapnutí a vypnutí firewallu - restartování, vypnutí a hibernace koncového bodu.	ANO	Pokryto úlohami
Ochrana koncového bodu zabráněním spuštění procesu dle hash nebo výrazu YARA.	ANO	Pokryto mechanismy Process Blocking a Process Termination, které umí využívat feedy (hash) a složitější podmínky (včetně YARA).
Systémová správa podporovaná na koncovém bodu prostřednictvím nástroje EDR: - správa uživatelů (přidání, odebrání, povolení, zablokování, - instalace a odinstalace aplikací, - změna nastavení operačního systému (například zapnutí firewallu a antivirového systému).	ANO	Pokryto úlohami
Forenzní analýza: - vzdáleně – získáním obrazu paměti určitého procesu - vzdáleně – získáním obrazu celé paměti - vzdáleně – získáním obrazu disku	ANO	Pokryto úlohami
Automatizace reakce na incidenty automatickým nebo polo-automatickým spouštěním akcí (nachystaných výrobcem i uživatelem definovaných) na koncových	ANO	Pokryto Playbooky (pro složitější situace a detekce učiněné i NDR a pastmi) a schopností navázat na

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
bodech v případě výskytu určitého alarmu, který se ke koncovému bodu vztahuje.		EDR behaviorální pravidlo přímo úlohu v EDR.
Systém musí být schopen automatického spuštění vybrané akce jako automatické odpovědi na určitý alert.	ANO	Pokryto Playbooky (pro složitější situace a detekce učiněné i NDR a pastmi) a schopností navázat na EDR behaviorální pravidlo přímo úlohu v EDR.
Schopnost agenta systému provádět více akcí současně.	ANO	Agent je schopen provádět své činnosti (sběr behaviour, vyhodnocování pravidel, spouštění úloh, terminálové sezení) současně.
Systém musí umožnit zobrazení běžících procesů na koncovém bodě v reálném čase a základní manipulaci s nimi – například jejich ukončení a získání obrazu paměti procesu.	ANO	Je k dispozici pohled na běžící procesy na koncovém bodě s možností jejich ukončení nebo provedení memory dump.
Automatizace vybraných reakcí na incidenty (dle definovaných a schválených scriptů).	ANO	Pokryto Playbooky (pro složitější situace a detekce učiněné i NDR a pastmi) a schopností navázat na EDR behaviorální pravidlo přímo úlohu v EDR.
Systém musí umožnit zobrazení vzdáleného souborového systému koncového bodu a základní manipulace se soubory – například získání souboru, smazání souboru.	ANO	Je k dispozici pohled na souborový systém na koncovém bodě s možností základní manipulace se soubory (smazání, kopírování, stažení).
Automatickým spouštěním akcí (nachystaných i uživatelem definovaných) na koncových bodech v případě výskytu určitého alarmu, který se ke koncovému bodu vztahuje.	ANO	Pokryto Playbooky (pro složitější situace a detekce učiněné i NDR a pastmi) a schopností navázat na EDR behaviorální pravidlo přímo úlohu v EDR.
OSTATNÍ FUNKČNÍ POŽADAVKY		
Alerty generované systémem musí být zobrazovány v centrální konzoli řešení.	ANO	Systém EDR je integrovaný s NDR a pastmi a lze zobrazit všechny alerty v jednom pohledu.
Před-připravené integrační vazby na aplikace typu SIEM.	ANO	Předpřipraveny jsou vazby na Qradar a ArcSight, případně další systémy využívající CEF nebo LEEF formát.
Systém musí podporovat integraci s: - komponenty pro detekci APT útoků na síťovém provozu (NDR), způsobem plné integrace v řešení Extended Detection and Response (XDR).	ANO	Fidelis Endpoint je integrovanou součástí bezpečnostní platformy Fidelis Elevate, která je dále tvořena NDR částí Fidelis Network a síťovými pastmi Fidelis Deception

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		a dohromady tvoří Aktivní XDR (AXDR).
Jednotné uživatelské rozhraní pro analytiku, vyšetřování a reakci společnou pro prostředí sítě i koncových bodů.	ANO	Platforma Fidelis Elevate poskytuje jednotné rozhraní vytvořené datovou integrací a propojením pohledů na NDR/pasti a EDR.
Dokumentované standardizované aplikační rozhraní pro zákaznické integrace s dalšími bezpečnostními komponentami. Preferujeme http & XML nebo JSON API rozhraní.	ANO	K dispozici je dokumentované a bohaté API založené na HTTPS a JSON.
Systém disponuje jednotným rozhraním pro správu, detekci, vyšetřování a reakci, které je součástí poptávaného řešení Extended Detection and Response.	ANO	Fidelis Endpoint je integrovanou součástí bezpečnostní platformy Fidelis Elevate, která je dále tvořena NDR částí Fidelis Network a síťovými pastmi Fidelis Deception a dohromady tvoří Aktivní XDR (AXDR).
Systém bude napojen na zdroj aktualizovaných informací o hrozbách (threat-intelligence) a bude z toho zdroje provádět pravidelně aktualizace.	ANO	Součástí služeb podpory (maintenance) je i poskytování aktualizací threat-intel - tedy feedů, pravidel a signatur.
Systém je kompletně nasaditelný do prostředí zákazníka	ANO	Systém lze kompletně realizovat on-premise, dokonce případně zcela bez nutnosti komunikace do internetu.
Systém je shopen být plně funkční i bez konektivity do internetu	ANO	Systém lze kompletně realizovat on-premise, dokonce případně zcela bez nutnosti komunikace do internetu.
Systém musí být schopný zaznamenávat metadata o chování koncových bodů, alerty a výsledky úloh i pro koncové body, které jsou dočasně mimo síť, jejich uchováním na koncovém bodě až do jejich odeslání do systému alespoň po dobu 5 dní.	ANO	Výsledky úloh i události na koncových bodech jsou ukládány do mezipaměti, pokud nemá koncový bod konektivitu na server Fidelis Endpoint. Dobu retence těchto dat lze nastavit.
Na koncových stanicích musí agentská část využívat zanedbatelnou část zdrojů - agent by neměl překročit po většinu času jednotky (max. 4%) využití CPU.	ANO	Výrobce udává využití asi 2% CPU.
Agent systému musí být odolný proti odinstalování a pokusům jej zastavit nebo poškodit.	ANO	Agent je schopen bránit pokusům o jeho zastavení nebo odinstalování.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém musí uchovávat metadata a události po dobu minimálně 30 dní s možností rozšíření až na 90 dní formou volitelné licence.	ANO	V případě Fidelis Endpoint dokonce není nutné ani navýšení licence, postačuje navýšení úložné kapacity Datastore.
Odinstalace agentů musí vyžadovat zvláštní autentizaci (např. heslo pro odinstalaci).	ANO	Odinstalace agenta může vyžadovat zadání odinstalačního hesla nastaveného v systému.
Systém musí podporovat koncové body s operačními systémy (64bit): - Windows Server 2016, 2019 a novější - Windows 10, 64 bit a novější - Windows 11, 64 bit OS a novější - CentOS 7 a novější - Red Hat Enterprise Linux 7, 8 a novější - Ubuntu 14.04, 16.04,18.04, 20.04, 22.04 a novější - macOS	ANO	Všechny uvedené OS jsou podporovány.
LICENCE		
Licence musí pokrýt minimálně 400 endpointů (PC, servery, virtuální stroje) s možností rozšíření na 450 bez nové soutěže.	ANO	Pokryto odpovídající licencí.

NDR (Network Detection and Response)		
DETEKČNÍ FUNKCE/SCHOPNOSTI		
Systém je cíleně navržen jako nástroj pro bezpečnotní specialisty a SOC týmy pro podporu jejich práce a poskytuje detailní síťovou vizibilitu na síťový provoz a implementuje detekční metody relevatní známým i novým bezpečnostním hrozbám.	ANO	Fidelis Network a Deception platforma byla navržena pro podporu práce SOC a CIRT týmů a je orientována na síťovou vizibilitu a detekci hrozeb na síti.
Detekce probíhají pomocí rozpoznání známých hrozeb DPI pravidly	ANO	DPI funkcionalita je pokryta a vlastní pravidla ve formátu Suricata lze přímo do sytému v případě potřeby i importovat.
Detekce probíhají rozpoznáním známých hrozeb na základě reputace souborů (dle hash), reputace IP adres a dalších reputačních seznamů odvolávající se na atributy obsahu.	ANO	Známé hrozby jsou rozpoznávány pomocí reputačních feedů a to dle řady atributů, včetně všech zmíněných.
Detekce probíhají pomocí heuristiky a emulace postoupením přenášeného spustitelného kódu antivirovému enginu.	ANO	Součástí senzorů je i AV engine, který analyzuje všechen spustitelný kód procházející viditelný pro senzor.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Detekce probíhají pomocí pravidel odvolávající se na obsah spojení: - klíčová slova - regex výrazy pro obsah - YARA výraz	ANO	Uvedené detekce jsou možné, neboť systém má odpovídající indikátory pro tyto metody rozpoznání obsahu.
Detekce probíhají pomocí pravidel odvolávající se na parametry protokolu, kterým spojení probíhá: - odkaz na atribut spojení a relační podmínka - kombinace podmínek v podobě logického výrazu	ANO	Uvedené detekce jsou možné, neboť systém má odpovídající indikátory pro tyto metody rozpoznání obsahu.
Detekce probíhají detonací spustitelného kódu přenášeného po síti na sandboxu.	ANO	Sandboxing je podporovaná detekční metoda, a to s využitím sandboxu jako služby výrobce, nebo volitelně jako nasazeného on-premise v podobě HW appliance.
Detekce probíhají behaviorální analýzou shopnou rozpoznat pomalé útoky korelací síťových aktivit přes dlouhé časové okno.	ANO	Je pokryto kolektorovou analytikou, která je schopna rozpoznat shluky událostí, posloupnosti událostí nebo opakující se děje, a to historickou analýzou pomocí dodaných i vlastních pravidel.
Detekční metody pracují i nad obsahem, který je v přenášených archivech (zip, rar, gzip, tar) nebo vložených dokumentech (například Excel tabulka ve Word dokumentu) a to i v případě opakovaného vložení nebo archivace bez omezení počtu vnoření.	ANO	Pokryto mechanizmem DSI (Deep Session Inspection), které rekonstruuje obsahy TCP spojení a provádí rekurzivně dekompozici obsahu.
Detekce anomálií pomocí modelů strojového učení a případné generování alarmů pro významné anomálie.	ANO	Systém vyhodnocuje 25 ML (Machine Learning) modelů a rozpoznává anomálie v provozu.
Identifikace spojení využívajících neočekávané nebo neznámé protokoly (např. nesoulad portů a protokolů).	ANO	Prováděno pomocí DSI, které je schopno rozpoznat skutečný protokol.
Systém musí klasifikovat události podle MITRE ATT&CK frameworku uvedením odpovídající techniky a/nebo taktiky útočníka. Vlastní pravidla lze definovat tak, aby také používala kategorie MITRE ATT&CK frameworku.	ANO	Systém mapuje detekce na taktiky a techniky dle MITRE ATT@CK. Toto je možné využít i pro vlastní pravidla.
Možnost importu detekčních pravidel s podporou formátů YARA.	ANO	Formát YARA je podporován jako jeden v desítek typů indikátorů.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Možnost definovat pravidla pro vyhledávání shluku událostí nebo posloupnosti událostí v síťovém provozu a generovat výstrahy průběžnou analýzou okamžitých událostí a analýzou již uložených historických záznamů o provozu zpětně.	ANO	Pokryto kolektorovou analytikou.
Analýza síťového provozu v rámci systému se provádí pro veškerý síťový provoz bez ohledu na použité komunikační protokoly, a proto jsou sledována a analyzována všechna probíhající spojení na všech síťových portech.	ANO	Číslo portu není pro systém směrodatné z hlediska analýzy obsahu spojení. Protokol je vždy určen dekodérem, nikoliv odvozen z čísla portu. Systém analyzuje spojení na všech portech.
Systém musí poskytovat kontinuální a neselektivní záznamy o aktivitách na síti formou metadat. Tyto záznamy jsou ukládány bez ohledu na přítomnost detekce, aby sloužily zadavateli při vyšetřování hrozeb a hunting.	ANO	Metadata jsou ukládána bez ohledu na to, zda jsou k nim vázány nějaké detekce.
Systém musí neselektivně popisovat síťovou komunikace minimálně v následujícím rozsahu pro uvedené vybrané protokoly: HTTP Protokol - záznamy musí obsahovat minimálně - URL - Jméno přenášeného souboru (pokud se jedná o přenos souboru) - HTTP Command - Status kód serveru - User Agent - Referer - Informace o ukončení připojení (pro perzistentní HTTP spojení) - Analýza přenášeného obsahu (soubory/HTML)	ANO	Uvedené atributy popisující provoz jsou součástí záznamu v metadatech
TLS Protokol - záznamy musí obsahovat minimálně: - Typ šifry - Délka klíče - Hashovací metoda - Verze TLS/SSL - SNI - JA3 a JA3S	ANO	Uvedené atributy popisující provoz jsou součástí záznamu v metadatech

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ

- Atributy certifikátu:
  - Subjekt
  - Vydavatel
  - Platnost
  - Typ certifikátu		

FTP Protokol - záznamy musí obsahovat minimálně: - Příkaz - Jméno souboru - Režim (pasivní/aktivní) - Uživatelské jméno - Analýza přenášeného obsahu (soubory)	ANO	Uvedené atributy popisující provoz jsou součástí záznamu v metadatech
POP3 Protokol - záznamy musí obsahovat minimálně: - Uživatel - Popis obsahu (obvykle MIME obálky): - Subjekt - From - To - Received hlavičky - Originální IP adresa odesilatele - Jména příloh - Analýza přenášeného obsahu (soubory)	ANO	Uvedené atributy popisující provoz jsou součástí záznamu v metadatech
SMTP Protokol - záznamy musí obsahovat minimálně: - From - To - Uživatelské jméno - Kód odpovědi serveru - Analýza přenášeného obsahu (soubory)	ANO	Uvedené atributy popisující provoz jsou součástí záznamu v metadatech
SSH Protokol - záznamy musí obsahovat minimálně: - Použitá šifra - HASSH klienta - HASSH serveru	ANO	Uvedené atributy popisující provoz jsou součástí záznamu v metadatech
Rozpoznání typu obsahu - bez ohledu na protokol musí systém rozpoznávat typ obsahu pro následující běžně používané souborové formáty a zaznamenávat o nich metadata: - HTML - JavaScript - Archivační a komprimační formáty: zip,	ANO	Uvedené souborové formáty a typy obsahu jsou systémem podporovány a systém pro ně má specializovaný dekodér a generuje pro ně odpovídající metadata.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
rar, gzip, tar, dmg, a další - PDF (včetně vložených aktivních komponent) - Obrazové formáty: jpg, png, ico - Dokumenty: doc, docx, ppt, pptx, xls, xlsx, xlsm (včetně vložených aktivních komponent) - Spustitelné soubory: exe Obsah musí být popsán atributy relevantními pro daný formát. U složených dokumentů (archiv vložené dokumenty do jiných dokumentů) musí být obsah popsán opakovaně a bez omezení hloubky vnoření		
Detekce malwaru přenášeného přes jakýkoli nešifrovaný protokol.	ANO	"Několik detekčních metod cílí na rozpoznání přenosu malware:
Detekce malwaru zabaleného i hluboko v obsahu (v archivech a dalších složených dokumentech).	ANO	- AV engine na senzoru
Možnost definovat pravidla (komunikační matice) pro vyhodnocení oprávněnosti odchozí komunikace vůči definovaným kritickým informačním systémům pomocí kombinací parametrů: - IP adresa/seznam IP adres/rozsah adres - Skutečný typ detekovaného protokolu (nezávisle na definovaném čísle portu TCP/UDP) - Čísla portů (TCP/UDP).	ANO	- signatury v podobě feedů
Možnost importu úplného záznamu síťové komunikace ve formátu PCAP pro kontrolu, popis a hloubkovou analýzu.	ANO	- DPI pravidla
Detekce projevů nástrojů pro vzdálený přístup (RAT).	ANO	- DSI pravidla"
Definice výjimek pro vyloučení určité komunikace z inspekce daným pravidlem.	ANO	Pokryto schopností DSI rozbalovat kompozitní obsah a rekurzivně vybalovat vložené objekty (soubory) bez omezení počtu opakovávání tohoto rekurzivního procesu.
Funkce obsahové analýzy detekuje informace přenášené i hluboko v obsahu, bez ohledu na hloubku vložení a bez ohledu na formát souboru.	ANO	Pokryto schopnostmi DSI pravidel.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Import popisu hrozeb od třetích stran a vlastních, které mohou být dodány ve formátech STIX, TAXII, CSV (podpora ThreatConnect).	ANO	Senzor je schopen "přehrát" provoz zaznamenaný v PCAP a generovat metadata a alerty tak, jako kdyby probíhal v reálném čase.
Obsahová analýza pro detekci exfiltrace informací s možností nasazení v prostředí se značkami (klasifikátory) i bez nich (např. pomocí regulárních výrazů obsahových pravidel, vzorových šablon, atp.).	ANO	"Nástroje pro vzdálený přístup jsou rozpoznávány:
Retrospektivní analýza všech zaznamenaných údajů o chování sítě (podle definované doby retence, požadována je retnce 30 dní s možností rozšíření až na 90 dní), která odhalí sled událostí vedoucích k projevům kybernetického incidentu.	ANO	- analýzou protokolu a obsahu spojení
Možnost definovat vlastní pravidla detekce nad libovolným typem přenášeného obsahu, charakteristikami chování nebo posloupností událostí v síti.	ANO	Pokryto kolektorovou analytikou.
Detekce zpětných volání malwaru Command & Control.	ANO	"Spojení typu C&C jsou rozpoznávány:
Systém bude schopen aplikovat aktualizované signatury na historický síťový provoz uložený v popisných metadatech po dobu požadované retence, aby našel nyní známý malware, který nebyl v minulosti detekován.	ANO	- analýzou protokolu a obsahu spojení
Pravidla analýzy provozu umožňují definovat podmínky vztahující se k přenášenému obsahu a parametrům aplikační vrstvy, například detekovat přenášené soubory, u nichž koncovky soborů neodpovídají obsahu, nebo typická čísla portů neodpovídající typu detekovaného komunikačního protokolu.	ANO	- vzorcem chování kolektorovou analytikou"
Detekce pokusů o zneužití zranitelností na dálku prostřednictvím sítě.	ANO	Nazváno jako "retrospektivní detekce" a realizováno jako aplikace nových signatur na historická metadata.
Podpora spolupráce s řešeními SSL Visibility pro kontrolu provozu přenášeného přes šifrované připojení.	ANO	Pokryto schopnosti DSI, kdy je rozpoznán skutečný protokol a je možné jej porovnat s číslem portu.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Schopnost systému identifikovat specifické komunikační protokoly vyskytující se v provozu organizace zadavatele. Schopnost zahrnout takto identifikovaný protokol do definice detekčních pravidel.	ANO	Systém vyhodnocuje DSI pravidla orientovaná na pokusy zneužít zranitelnosti po síti.
Podpora detekce síťového provozu ve spolupráci s PROXY systémy, které podporují protokol ICAP (Internet Content Adaptation Protocol).	ANO	Podporována je spolupráce s množstvím různých typů zařízení pro dešifrování provozu.
VYŠETŘOVACÍ FUNKCE/SCHOPNOSTI		
Průběžné zaznamenávání informací o síťové komunikaci ve formě, která umožňuje pozdější analýzu (metadata).	ANO	Tvorba metadat popisující hloubkovou analýzu provozu je jednou ze základních funkcionalit systému Fidelis Network.
Export úplného záznamu, předem popsaných síťových komunikací, ve formátu PCAP pro další zkoumání.	ANO	Pravidlo může mimo alertování také uložit komunikaci, která jej spustila, do PCAP souboru.
Extrakce obsahu souborů zachycených při jejich pohybu po síti pro forenzní účely pomocí systémové konzoly.	ANO	Součástí alertu jsou "Forenzní data" a tyto lze z alertu exportovat do souboru.
Systém podporuje efektivitu vyšetřování tím, že dokáže automatizovaně spojovat jednotlivé bezpečnostní události, které mají společnou příčinu, do jedné události (incidentu).	ANO	Systém vytváří tzv. Active Threats, což jsou seskupené alerty, namapované na MITRE ATT@CK taktiky a techniky a prezentované jako incident.
Možnost průběžně zaznamenávat a zpětně analyzovat informace o všech síťových aktivitách (všechny níže uvedené): - IP adresy a jejich zeměpisná poloha - identity uživatelů (např. e-mailové adresy pro rozhraní SMTP/POP3/IMAP a web-mail nebo uživatelská jména pro jiné protokoly). - čísla portů - skutečný typ zjištěného protokolu - parametry rozpoznaných komunikačních protokolů (například hlavičky SMTP, HTTP, ...) - typ přenášených souborů (minimálně excel, word, powerpoint, pdf, exe, msi, obrazové formáty, archivní a kompresní formáty, včetně vnořených) - HASH přenášených souborů	ANO	Všechny uvedené charakteristiky provozu jsou systémem generovány a ukládány do záznamů metadat.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
- velikost přenášených souborů - název a přípona přenesených souborů - informace o tom, že soubor je zašifrovaný, a obecně informace o entropii obsahu souborů - čas a délku spojení - objem přenesených dat.		
Pro následnou analýzu jsou k dispozici historické informace o provozu se stanovenou dobou uchování.	ANO	Retence je dána diskovým prostorem kolektoru metadat a licencí. Vhodná volba licence a velikost diskového prostoru pak zajišťuje požadovanou retenční dobu.
Zaznamenané informace o provozu umožňují vyhledávat spojení podle libovolného atributu popisujícího spojení nebo pomocí logického výrazu s relačními operátory odkazujícími na atributy spojení.	ANO	V metadatech lze vyhledávat dle podmínky vztahující se k libovolnému atributu s využitím relačních operátorů a podmínky pak spojit do logického výrazu pomocí AND a OR.
V oblasti detekce a vyšetřování Advanced persistent threats (APT) musí systém splňovat požadavek na viditelnost stop daného útoku a dostupnost forenzních dat ze všech zachytitelných fází útoku APT (podle fází cyber-kill-chain).	ANO	Metadata odpovídají přivedenému monitorovanému provozu a vhodnou volbou tohoto provozu lze zajistit viditelnost na všechny fáze útoků.
Geolokace komunikujících stran.	ANO	Systém provádí geolokaci dle IP adres a také mapuje IP adresy na ASN.
Možnost vlastní definice geolokačních tabulek IP adres (pro geolokaci privátní IP segmentů).	ANO	Je podporováno importem CSV soboru s dokumentovaným formátem.
Vestavěná podpora pro řízení životního cyklu tiketů pro distribuci úkolů mezi uživatele systému/vyšetřovatele.	ANO	Alerty mají charakter tiketů a lze je přiřadit uživateli nebo skupině a obsahují atributy popisující jejich stav (new, open, closed, …)
Analýza obsahu komunikace u nešifrovaných protokolů u systému jako jsou např.: FileServer, Sharepoint, OneDrive	ANO	Podporováno je několik desítek protokolů a hlubokou analýzou přenášeného obsahu, včetně rozpoznání typu soboru a analýzy

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Exchange, Web Browsers - MS Edge, Google Chrome, Opera, SQL, Oracle atd.		jeho obsahu, a to bez ohledu na síťový protokol.
Rekurzivní analýza složeného obsahu (archivy, složené dokumenty atd.) a popis veškerého i vloženého obsahu v metadatech bez omezení počtu vnoření.	ANO	Podporováno DSI, které bez omezení hloubky analýzy "rozbaluje" přenášený obsah a rekurzivně jej analyzuje.
Systém přiřazuje informace o uživatelském účtu k zaznamenanému síťovému spojení.	ANO	Systém je schopen z protokolu rozpoznat uživatele a připojit tuto informaci ke spojení.
Systém sbírá informace o událostech (alespoň login operace) z Active Directory serveru	ANO	Napojení na AD je podporováno s cílem sbírat informace o dění na AD a současně provádí kontrolu nastavení AD.
REAKČNÍ FUNKCE/SCHOPNOSTI		
Schopnost ukončit spojení na základě detekce.	ANO	Senzor je schopen ukončovat spojení pomocí TCP reset paketů, mail senzor pak umístěním emailu do karantény nebo jeho zahozením a webová senzor signalizací webové proxy, že má spojení ukončit.
Schopnost automatizace pracovních postupů při nápravě kybernetických incidentů: - plně automatická reakce definovaná bezpečnostní politikou pro síťový provoz - podporované metody: DROP při in-line zapojení, nebo TCP Reset pro out-of-band připojení	ANO	Spuštěním akcí na dotčených koncových bodech pomocí playbooku.
Schopnost umísit škodlivý email do karantény.	ANO	
Systém musí být schopen spouštět vyšetřovací nebo nápravné úlohy na koncových bodech prostřednictvím integrace s řešením EDR.	ANO	Ukončením spojení TCP reset na Direct nebo Internet senzoru, nebo umístěním do karantény na Mail Senzoru.
Systém poskytuje webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní.	ANO	Podporováno na Mail senzoru
Předpřipravené integrační vazby na aplikace typu SIEM.	ANO	Podpora automatického spouštění úloh pomocí systému Fidelis Endpoint.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Zdokumentované aplikační rozhraní pro integraci s dalšími bezpečnostními komponentami. Upřednostňujte rozhraní API http a XML nebo JSON.	ANO	Všechny detekce a relevantní údaje (metadata a další datové entity) jsou zobrazovány v jednotném uživatelském rozhraní systému, které tvoří provázaná rozhraní Fidelis Network & Deception a Fidelis Endpoint.
Dashboard a možnosti jeho úprav pro grafické zobrazení informací a podpory rozhodovacího procesu (alert triage).	ANO	Připraveny jsou vazby na ArcSight, Qradar, Splunk a další systémy.
Možnost detailního řízení přístupových práv pro více úrovní pracovníků SOC (analytici, operátoři, IT podpora, forenzní analytici, vyšetřovatelé).	ANO	Systém implementuje velmi granulární RBAC mechanizmus a umožňuje přiřazení rolí uživatelům a přiřazení komponent systému uživatelům.
Možnost napojení na ActiveDirectory/LDAP pro autentizaci uživatelů systému.	ANO	LDAP, RADIUS a TACACS+ jsou podporované autentizační metody.
Jednotné uživatelské rozhraní pro veškerou analytiku, vyšetřování a reakci.	ANO	Systém poskytuje jednotné webově založené uživatelské rozhraní.
Systém je platforma pro forenzní analytiku, detekci, vyšetřování a řízení reakcí na zaznamenané kybernetické události.	ANO	Systém je přímo navržen a vyvíjen jako kybernetická bezpečností platforma pro detekce, vizibilitu a analýzu zaznamenaných jevů.
FUNKCE/SCHOPNOST SANDBOXING		
Systém bude poskytovat službu sandboxingu, která bude využita pro další práci s potencionálně škodlivým obsahem.	ANO	Sandboxing je podporovaná detekční metoda, a to s využitím sandboxu jako služby výrobce, nebo volitelně jako nasazeného on-premise v podobě HW appliance.
Takový obsah bude detonován na Widows OS, který bude provozován v rámci sandboxu.	ANO	Detonace na OS Windows je sandboxu, prováděna
Takový obsah bude detonován na Linux OS, který bude provozován v rámci sandboxu	ANO	Detonace na OS Linu je sandboxem, prováděna
Sandbox rozpozná pokusy o jeho detekci ze strany detonovaného kódu	ANO	Sandbox je schopen rozpoznat snahy kódu o jeho detekci (například pokus o detekci běhu pod debuggerem)
Výstup sandboxingu bude součástí informací v alertech zobrazovaných v konzoli systému	ANO	Výstup sandboxu je přímo součástí alertů.
Sandbox bude možné nastavit do režimu, kdy bude mít detonovaný kód přístup k	ANO	Jsou podporovány oba režimy - sandbox v izolovaném režimu bez

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
vnější konektivitě do internetu nebo bude detonován bez toho přístupu.		přístupu do internetu nebo využití obvykle dedikované konektivity pro tento účel.
Sandbox bude využívat pokročilé technologie pro vyprovokování kódu k činnosti.	ANO	Sandbox simuluje aktivity uživatele a zrychluje čas, aby vyprovokoval případný škodlivý kód k činnosti.
Sandbox musí umožnit detekci podezřelého kódu a vyhodnocení jeho chování v izolovaném prostředí pro Windows a Linux. Výsledky sandboxingu musí být viditelné v centrální konzoli.	ANO	Sandbox vytváří automaticky feed, který lze využít pro další detekce již bez nutnosti detonace kódu na sandboxu.
Popis činnost detonovaného kódu bude součástí výstupu sandboxingu a to alespoň v kategoriích: - spouštěné procesy - zapisované soubory - registrové zápisy a změny - síťová spojení - DNS překlady - popis podezřelých činností, které sandbox rozpoznal	ANO	Tyto činnosti jsou součástí výstupu sandboxingu.
OSTATNÍ FUNKČNÍ POŽADAVKY		
Systém je kompletně nasaditelný do prostředí zákazníka	ANO	Systém lze kompletně a bez omezení funkčnosti nasadit do prostředí zákazníka, dokonce i v režimu air-gap - tedy bez nutnosti online spojení do internetu.
Systém je schopen být plně funkční i bez konektivity do internetu	ANO	Systém lze kompletně a bez omezení funkčnosti nasadit do prostředí zákazníka, dokonce i v režimu air-gap - tedy bez nutnosti online spojení do internetu.
Systém musí podporovat standardní správu oprávnění a přístupů bez požadavku na hierarchický režim pro podřízené organizace.	ANO	Systém podporuje nasazení v hierarchickém režimu, kdy jinak samostatné a celistvé systémy lze spravovat (uživatelé, pravidla) a detekce a metadata vyhodnocovat na tzv. Master CommandPost - tedy nadřízené konzoli, která také může být součástí jinak samostatného systému.
Generování reportů dle předpřipravených šablon.	ANO	Je k dispozici editor reportů a možností ručního nebo automatického generování reportů ve formátu PDF, případně jsou k

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		dispozici i další formáty reportů (CSV, JSON, …). Obvyklé reporty jsou předpřipraveny a lze je využít, nebo upravit nebo vytvořit kopii a na ní založit vlastní report.
Tvorba a generování zákaznicky definovaných reportů.	ANO	Je k dispozici editor reportů a možností ručního nebo automatického generování reportů ve formátu PDF, případně jsou k dispozici i další formáty reportů (CSV, JSON, …). Obvyklé reporty jsou předpřipraveny a lze je využít, nebo upravit nebo vytvořit kopii a na ní založit vlastní report.
Systém monitoruje svůj vnitřní chod a drží historické informace o událostech týkající se vlastního chodu a problémů.	ANO	Interní diagnostika vyhodnocuje vnitřní chod systému a zaznamenává odchylky a problémy, které ukládá a lze v nich vyhledávat.
Možnost nastavení automatického generování a odesílání reportů na emailové adresy.	ANO	Reporty je možné automaticky generovat v určený čas, a to i periodicky a odesílat na určené adresy.
Podpora instalace jednotlivých komponent řešení do virtuálního prostředí na platformě VMware nebo Proxmox.	ANO	Pro provoz je možné využít virtualizační platformy VMware a Proxmox.
Funkcionalita analýzy a záznamu síťového provozu pracuje nad zrcadleným provozem sítě.	ANO	Senzor lze nasadit v out-of-band režimu, kdy je mu dodáván zrcadlený provoz, nebo i in-line, kdy provoz prochází senzorem.
Podpora monitorování provozu na rozhraních Ethernet s rychlostmi 100Mbps, 1Gbps, 10Gbps, 25Gbps.	ANO	Tyto typy rozhraní je možné monitorovat HW senzory výrobce, pro rychlosti do 5Gbps lze využít virtualizované senzory.
Obsahuje službu průběžné aktualizace signatur/definic chování a aktualizace pravidel sandboxu z komerčního zdroje.	ANO	Součástí služeb maintenance je i dodávání aktualizací všech typů threat-intel do systému (DPI, DSI pravidla, feedy, signatury).
LICENCE		
Celková požadovaná retence všech historických metadat o chování sítě v délce min. 30 dnů.	ANO	Pokryto vhodnou licencí.
Schopnost analyzovat provoz až do celkové přenosové rychlosti min. 1 Gbps.	ANO	Pokryto vhodnou licencí.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
INTELIGENTNÍ PASTI (Honeypots)		
OBECNÉ POŽADAVKY		
Systém je cíleně navržen jako nástroj pro bezpečnostní specialisty a SOC týmy pro podporu jejich práce a poskytuje možnost rychle a operativně vystavovat pasti do síťového prostředí a seznamovat se s detaily detekcí na pastech.	ANO	Systém je koncipován jako nástroj pro SOC týmy a umožňuje jednoduše a rychle spravovat pasti a vyhodnocovat detekce.
Jedním HW nebo VM komponentem systému bude možné realizovat až 1000 pastí v různých částech sítě.	ANO	Počet pastí není omezen licenčně, ale pouze výkonem komponenty Decoy server. Jeden Decoy server s high-end sizingem umožňuje realizovat až 1000 pastí.
Komunikace mezi komponenty systému bude zabezpečena a bude možné ji vydělit do zvláštní sítě nebo segmentu.	ANO	Vnitřní komunikaci systému lze zcela oddělit do vlastního segmentu.
Pasti jsou schopny využívat statické IP adresy nebo DHCP pro přidělení adresy.	ANO	Oba způsoby získání IP adresy jsou pastmi podporovány.
Systém bude podporovat nasazení pastí až v několika stovkách VLANů.	ANO	Jeden Decoy server je schopen vystavit pasti do až 200 VLAN.
Systém bude schopen rozpoznat, že jde o stejný koncový bod i po případné a příležitostné změně jeho IP adresy.	ANO	Systém odlišuje pojem Asset a IP adresa a podporuje několik metod, jak párovat měnící se IP adresy na stejný Asset.
Systém bude schopný připojení trunkem i porty bez VLAN taggingu.	ANO	Obě metody jsou podporovány. Při použití trunku je možné vystavit pasti do libovolné VLAN, kam trunk umožní přístup. V případě připojení do jednoho segmentu je pak možné pasti vystavit právě tam.
Systém bude spravován z centrální konzole.	ANO	Systém využívá stejnou centrální konzoli jako systém Fidelis Network. Jde o integrované řešení.
Systém bude využívat pro svůj provoz HW vlastní appliance nebo dodanou virtualizační platformu.	ANO	Systém je možné provozovat na HW společnosti Fidelis Security, nebo na virtualizační platformě Proxmox nebo VMware.
Systém nalezne automaticky proxy servery v organizaci.	ANO	Systém je schopen rozpoznat webové proxy.
Systém neomezuje nasazení návnad na koncové body licenčně z hlediska počtu.	ANO	Návnady jsou v systému označovány jako Breadcrumbs a jejich počet není omezen licenčně.
Systém umožní využití podvržených MAC adres u pastí.	ANO	Pasti mohou využít skutečnou MAC adresu zařízení, které je realizuje (Decoy server), nebo lze zapnout

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		MAC address spoofing, kdy jsou použity realistické podvržené MAC adresy.
ZÁKLADNÍ FUNKCIONALITY/SCHOPNOSTI		
Autentizační metody na pastech by měly pokrývat uživatelsky definované účty, před-definované účty a úspěšné přihlášení po několika pokusech simulující prolomení hesla.	ANO	Všechny tyto autentizační chování systém podporuje.
Návnady bude možné nasazovat pomocí SCCM nebo nástroji EDR.	ANO	Návnady lze nasadit pomocí EDR Fidelis Endpoint nebo pomocí binárního nástroje, který lze distribuovat a spouštět například pomocí GPO.
Nekonečně vnořená klamná struktura složek na pastech poskytujících souborové služby pro zpomalení útočníka.	ANO	Emulované souborové systému mohou vykazovat toto chování.
Pasti budou součástí domény a budou schopné komunikovat s Active Directory, aby vzbudily zdání skutečných aktivit uživatelů.	ANO	Pasti mohou být členy domény a pak provádějí login/logout operace proti doméně.
Pasti musí aktivně vystupovat na síti. aby útočníci poslouchající síťový provoz a snažící se o MITM typ útoku byli vedeni k pastem. Příkladem mohou být aktivity protokoly LLMNR, ARP nebo NetBIOS.	ANO	Pasti jsou aktivní na síti a generují WPAD, LLMNR, ARP, NetBIOS a další typy provozu, aby zvýšily svou autenticitu.
Pasti poskytující souborové služby umožní vystavení určitých skutečných souborů.	ANO	V emulovaném souborovém systému mohou být umístěny skutečné soubory s daným obsahem.
Pasti poskytující souborové služby umožňují nastavit jinou než originální velikost souborů při stahování útočníkem pro jeho zpomalení.	ANO	Emulované soubory mohou mít i jinou než originální velikost - například i nekonečnou.
Systém automaticky detekuje servery v síti včetně DNS, Proxy, FTP a SSH serverů.	ANO	Servery poskytující tyto služby jsou rozpoznány.
Systém automatizovaně zvolí vhodné návnady pro dané koncové body.	ANO	Nasazení breadcrubs probíhá automatizovaně z hlediska volby typů návnad.
Systém automatizovaně zvolí vhodné pasti pro daný segment sítě na základě profilování a klasifikace zařízení.	ANO	Volbu typů pastí lze nechat na systému, který pak využije profily assetů v daném segmentu pro volbu vhodných pastí.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém bude adaptovat pasti na změny v síti – na nové segmenty sítě. operační systémy a aplikace.	ANO	Pokryto volitelně aktivovatelnou funkcí adaptivnosti systému pastí na změny v síti.
Systém bude aktualizovat pasti tak. aby odpovídali měnícímu se ICT prostředí a to automatizovaně na základě profilování a klasifikace zařízení.	ANO	Volbu typů pastí lze nechat na systému, který pak využije profily assetů v daném segmentu pro volbu vhodných pastí. Profily vznikají automaticky na základě analýzy provozu daného assetu.
Systém bude detekovat příchozí spojení z Internetu včetně rozpoznání protokolu.	ANO	Systém rozpoznává spojení, která přicházení zvenčí organizace a procházejí dNAT na firewallu a sumarizuje je ve zvláštním pohledu.
Systém bude implementovat mechanismy pro zpomalení aktivit útočníka.	ANO	Systém umožňuje nastavení zpomalení vlastních odpovědí na aktivity útočníka a tím jej také zpomalit.
Systém bude lákat útočníka k pastem s využitím síťových aktivit. falešných indicií distribuovaných na skutečné koncové body a integrací s AD.	ANO	Všechny tyto metody jak zvýšit atraktivitu pastí pro útočníka jsou podporovány.
Systém bude měnit pasti tak. aby útočník nebyl schopen naučit se podobu a umístění pastí.	ANO	Pokryto schopností adaptace.
Systém bude podporovat různé úrovně interaktivity pastí – nízkou, střední a vysokou.	ANO	Všechny úrovně jsou pokryty - nízká a střední pomocí emulovaných pastí, vysoká pak s použitím RealOS pastí.
Systém bude umožnovat realizaci postí s různými operačními systémy: Windows. Linux. MacOS. které bude možné provozovat současně.	ANO	Systém pastí je schopen emulovat všechny tyto OS.
Systém detekuje odesílání souborů do Internetu a rozpozná objem a použitý protokol.	ANO	Systém provádí požadované a poskytuje speciální pohled se sumarizací odesílaných dat, zdrojů a protokolů k tomu využitých.
Systém detekuje použití protokolů na jiných než obvyklých portech.	ANO	Pokryto DSI se schopností rozpoznání skutečného protokolu, bez ohledu na číslo portu.
Systém klasifikuje alerty z hlediska technik a taktik dle MITRE ATT&CK frameworku.	ANO	Detekce jsou mapovány na taktiky a techniky dle MITRE ATT@CK.
Systém musí být schopen detekovat IT a IoT zařízení v síti a vytvářet pasti odpovídajícího typu.	ANO	Volbu typů pastí lze nechat na systému, který pak využije profily assetů v daném segmentu pro volbu vhodných pastí. Profily

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		vznikají automaticky na základě analýzy provozu daného assetu.
Systém musí být schopen vytvořit pasti automatizovaně na základě pasivně prováděného profilování sítě a tak. aby odpovídali skutečně používaným OS a službám.	ANO	Volbu typů pastí lze nechat na systému, který pak využije profily assetů v daném segmentu pro volbu vhodných pastí. Profily vznikají automaticky na základě analýzy provozu daného assetu.
Systém musí být schopen vytvořit vhodné pasti na základě importu bezpečnostního skenu sítě.	ANO	Import seznamu pastí ve formátu CSV nebo vlastním formátu je podporován.
Systém musí podporovat bezpečnostní specialisty při huntingu integrací se systémem typu NDR.	ANO	Systém pastí je integrován s EDR Fidelis Endpoint a také NDR Fidelis Network a lze jednoduše najít relevantní aktivity na koncovém bodě odpovídajícím detekci na pasti.
Systém musí podporovat vytvoření pastí ve více podsítích/segmentech sítě.	ANO	Pokryto schopností systému využít pro publikaci pastí trunk nebo připojení do většího množství segmentů.
Systém musí pokrývat tyto případy užití: 1) detekce laterálního pohybu 2) vnitřní útočník 3) ukradené přihlašovací údaje 4) Man-in-the-Middle 5) ransomware 6) útoky na IP tiskárny, úložiště a síťové prvky 7) hunting a reakce na útok	ANO	Všechny tyto situace jsou schopnostmi systému pokryty a systém je pro jejich detekci koncipován.
Systém musí vytvářet profily a klasifikovat zařízení v síti pro poskytnutí přehledu o rolích a aktivitách jednotlivých zařízení.	ANO	Toto je součást procesu nazývaného Terrain Mapping, kdy systém z provozu usuzuje operační systém a roli assetu v síti. Aktivity jsou pak zaznamenávány v podobě metadat.
Systém nasadí specificky vytvořené návnady pro jednotlivé koncové body. které budou vycházet například z uživatele koncového bodu.	ANO	Návnady je možné nasadit buď pomocí EDR Fidelis Endpoint nebo s využitím nástroje (malá utilitka), který návnady vytvoří. Sada návnad je vždy specifická pro určitý koncový bod.
Systém nebude vyžadovat instalaci agentů na koncové body.	ANO	Fidelis Deception není založen na agentech.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém nezanechá žádné stopy ukazující na způsob vytvoření návnad na koncových bodech.	ANO	Návnady jsou vytvořeny nástrojem, který není instalován, ale jen jednorázově/opakovaně spouštěn a není tedy trvale přítomný na koncovém bodě.
Systém ověří. že existuje komunikační cesta mezi návnadou a odkazovanou pastí.	ANO	Při vytváření návnad systém validuje konektivitu na pasti a vytvoří návnady odkazující jen na dostupné pasti.
Systém poskytne detailní informace o dění a činnosti útočníka na pastech.	ANO	Činnosti jsou zaznamenávány a jsou součástí Deception alertů.
Systém poskytne informace o komunikaci mezi koncovými body, a tedy jdoucími i vlastní mimo pasti.	ANO	Systém je integrován s NDR Fidelis Network a dohromady pokrývají požadavek na záznam veškeré komunikace. Nicméně i samotný Fidelis Deception tvoří komunikační mapu, která naplňuje tento požadavek.
Systém poskytne seznam používaných prohlížečů v organizaci.	ANO	Systém mapuje agent hlavičky HTTP požadavků na typy prohlížečů.
Systém předkládá všechny získané informace v přehledné a celistvé podobě.	ANO	Pohled na alert poskytuje komplexní přehled o události a sjednocuje informace o detekované události s informací o pasti i assetu, který s ní komunikoval.
Systém rozpozná http využívající nástroje a aplikace (prohlížeče. aktualizační programy. …)	ANO	Systém mapuje agent hlavičky HTTP požadavků na typ aplikace, která HTTP využívá.
Systém rozpozná používané TLS využívající nástroje a aplikace.	ANO	Mimo automatizovaného nasazení pastí je možné pak nadefinovat kompletně ručně a specifikovat detailně její parametry.
Systém umožní manuální a detailní konfiguraci pastí v případě potřeby.	ANO	Systém umožňuje na past emulující http(s) server nasadit vlastní podobu webu. Provádí se to "nahráním" komunikace s existujícím webovým serverem do souboru HAR a pak importem do systému Fidelis Deception.
Systém umožní nahrát obsah pro pasti přístupné přes http(s).	ANO	Kontejnery vytvořené nástrojem Kubernetes mohou plnit funkci pastí.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém umožní nasadit na kubernetes/docker hostitele kontejnery, které budou pastmi.	ANO	Pasti emulují zranitelnosti a je možné pro danou past zobrazit emulované zranitelnosti.
Systém umožní nasadit pasti se zranitelnostmi a bude určité zranitelnosti i emulovat	ANO	RealOS pasti jsou pasti založené na běhu skutečného operačního systému a tento může být vytvořen z typického pre-load organizace.
Systém umožní nasazení vlastního pre-loadu operačního systému organizace na pasti.	ANO	Uvedené služby je možné pastmi emulovat.
Systém umožní realizaci emulovaných pastí poskytujících alespoň tyto služby: FTP, SSH, VNC, Databáze, HTTP(S), SMTP, SMB.	ANO	Simulace z pohledu obránce a útočníka jsou součástí pohledů na terén.
Systém umožní vytvoření a distribuci návnad v podobě falešných profilů do klientských aplikací, které budou odkazovat na pasti. Tyto návnady budou realizovány jako klíče v registrech, soubory aplikačních profilů. cookies prohlížečů, položky historie prohlížečů pro operační systému koncových bodů Windows, Linux a MacOS.	ANO	Návnady mohou mít podobu všech uvedených forem odkazu na past.
Systém umožní vytvořit past se souborovou strukturou (nikoliv obsahem) odpovídající skutečným koncovým bodům.	ANO	Pro tento účet systém poskytuje malou utilitu, která vytvoří popis struktury existujícího souborového systému a tento popis lze následně využít pro emulované pasti.
Systém umožní vytvořit pasti v podobě emulovaných služeb na různých emulovaných operačních systémech.	ANO	Mimo RealOS pastí založených na skutečném operačním systému a službách je podporováno vytvoření emulovaných pastí s volbou mnoha OS (Windows, Linux, MacOS) a s volbou mnoha služeb.
Systém umožní zobrazit jaká návnada na koncovém bodě odkazuje na jakou past.	ANO	Návnady mají speciální pohled, kde je graficky zobrazeno, které koncové body s návnadami odkazují na kterou past.
Systém umožňuje výběrový záznam komunikace do PCAP.	ANO	Systém je schopen provádět záznam komunikace do PCAP kolem alertu.
Systém umožňuje vytvoření emulovaných pastí i pastí využívajících skutečné operační systémy provozované jako virtuální stroje.	ANO	Oba typy pastí jsou podporovány – emulované a RealOS založené na skutečných OS a službách.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém umožňuje zobrazit mapu sítě na úrovni IP sítí a koncových bodů a komunikační vazby mezi nimi.	ANO	Pokryto pohledem nazvaným Komunikační mapa.
Systém určí rizikové koncové body a IP sítě.	ANO	Systém počítá riziko jako vyhodnocení důležitosti, relevantních alertů a pokrytí bezpečnostními nástroji Fidelis Security, a to pro každý vnitřní asset a následně i segment.
Systém umožňuje nasadit návnady, které budou ukazovat na falešné cíle umístěné na různých podsítích.	ANO	Návnady nejsou omezeny jen na vlastní segment assetu, ale mohou odkazovat na pasti v dalších segmentech.
INTEGRAČNÍ FUNKCIONALITY/SCHOPNOSTI		
Systém musí umožňovat automaticky reagovat na koncovém bodě vykonáním určené aktivity – úlohy nebo playbooku – intgerací se systémem EDR.	ANO	Funkcionalita "Playbooků" je implementována a umožňuje na koncovém bodě spustit jakoukoliv dostupnou úlohu jako reakci na detekci NDR, pastí nebo i EDR.
Systém odesílá notifikace jako emailové zprávy.	ANO	Mimo jiných komunikačních kanálů je podporována i elektronická pošta.
Systém podporuje integraci se systémy typu NTA/NDR pro dohledání detailů o spojeních.	ANO	Systém je podstaven jako integrovaný a tyto detaily jsou dosažitelné z alertu na jedno kliknutí.
Systém poskytuje otevřené a dokumentované API pro napojení na systémy jiných stran.	ANO	Jsou připraveny vazby na Qradar, ArcSight, Splunk a další SIEM/SOAR systémy.
Systém umožňuje jednoduché/předpřipravené napojení na aplikace typu SIEM.	ANO	Jakýkoliv spustitelný kód uložený na past je postoupen sandboxu.
Systém odesílá soubory uložené na emulované pasti útočníky do sandboxu pro zjištění jejich škodlivosti.	ANO	Funkcionalita "Playbook" je implementována a umožňuje na koncovém bodě spustit jakoukoliv dostupnou úlohu jako reakci na detekci NDR, pastí nebo i EDR.
POŽADAVKY NA REPORTING		
Systém obsahuje předpřipravené typické reporty.	ANO	K dispozici jsou předpřipravené reporty pro běžné potřeby zákazníka.
Systém umožní export pohledů na alerty s aplikovanými filtry do souboru PDF nebo CSV.	ANO	Je podporováno jak pro alerty, pak pro mnoho dalších pohledů v konzoli.
Systém umožňuje export informací minimálně ve formátech PDF a CSV.	ANO	PDF a CSV jsou podporovány.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém umožňuje nastavit periodicitu a adresy příjemců pro generování reportů.	ANO	Řešeno pomocí "schedulingu" reportů.
Alerty lze v rozhraní systému vyhledávat dle jakéhokoliv jeho atributu.	ANO	Pro vyhledávání lze použít jakýkoliv atribut, relační operátor (je, není rovno, menší, větší, …) a takové podmínky spojit do logického výrazu pomocí AND a OR.
Dashboard obsahuje předpřipravené komponenty a je možné doplnit a parametrizovat vlastní.	ANO	Je připraveno několik typických dashboardů a lze tvořit vlastí nebo existující modifikovat.
Systém sdruží alerty relevantní k jedné události/incidentu.	ANO	Alerty jsou sdružovány do "Active Threats" pohledů, které odpovídají hrozbám.
Uživatelské rozhraní je schopné zobrazit v reálném čase alerty a jejich detaily a výsledky profilování.	ANO	Alerty jsou uloženy na serveru konzole systému a jsou k dispozici téměř okamžitě a jsou také do této databáze ukládány s minimálním zpožděním.
POŽADAVKY NA SPRÁVU SYSTÉMU		
Systém je schopen provést aktualizaci všech komponent z centrální konzole.	ANO	Naplněno částí "Version Control" konzole a odpovídajících funkcionalit pro stáhnutí, distribuci a nasazení aktualizací na všechny komponenty systému NDR a pastí.
Systém umožňuje definovat výjimky na základě zdrojové a cílové IP adresy a protokolu.	ANO	Naplněno mechanizmem whitelistování jak u NDR, tak u pastí.
Systém umožňuje whitelistovat situace, kdy by nemělo dojít ke vzniku alertu (například při přístupu bezpečnostního scanneru na past).	ANO	Naplněno mechanizmem whitelistování jak u NDR, tak u pastí.
V případě výpadku komponenty je k dispozici automatická záloha její konfigurace, kterou lze využít pro nakonfigurování komponenty nové.	ANO	V případě nové registrace Decoy serveru se stejnou IP adresou provede systém obnovení konfigurace tohoto komponentu. V případě napojení nového sensoru je systém schopen automaticky nasadit všechna aktivní pravidla.
Systém je kompletně nasaditelný do prostředí zákazníka (on-site).	ANO	Systém je plně nasaditelný do prostředí zákazníka.
Systém je shopen být plně funkční i bez konektivity do internetu.	ANO	Systém nevyžaduje žádnou konektivitu do internetu pro svou činnost.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
LICENCE		
Systém bude chránit pastmi min. 400 zařízení s IP adresou v síti Zadavatele.	ANO	Pokryto vhodnou licencí.
Systém bude umožňovat vystavit pasti min. do 50 VLAN v síti Zadavatele.	ANO	Pokryto vhodnou licencí.
Systém nebude omezovat počet realizovatelných pastí nebo návnad licencí.	ANO	Není licenčním parametrem a není tedy omezeno licencí.
SLUŽBY IMPLEMENTACE A ŠKOLENÍ		
Implementační práce v prostředí Zadavatele (instalace všech HW a SW součástí řešení, nastavení pravidel komunikace a monitoringu IT zařízení v LAN, nastavení response pravidel, napojení na další systémy KB Zadavatele a Dashboard kybernetické bezpečnosti, testovací provoz minimálně 14 dní).	ANO	Pokryto nabídkou služeb.
Tvorba a realizace testovacích scénářů před uvedením systému do produkce.	ANO	Pokryto nabídkou služeb.
Zaškolení administrátorů.	ANO	Pokryto nabídkou služeb.

ID 02 MFA (Vícefaktorové ověřování)

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
LICENCE		
Min. 400 uživatelů	ANO	
FUNKCIONALITY PRO UŽIVATELE		
Umožňuje uživateli samostatný reset hesla k doméně ve WIN AD lokálně, z úrovně vlastního počítače nebo dálkově, za použití internetového prohlížeče. Vše bez pomoci interního IT oddělení.	ANO	Systém pro kompletní správu účtu AD přímo uživatelem - https://www.manageengine.com/products/self-service-password/help/admin-guide/Configuration/Self-Service/directory-selfservice.html
Umožňuje uživateli domény samostatné odblokování účtu v doméně (v případě jeho zablokování) lokálně, z úrovně vlastního počítače nebo prostřednictvím internetového prohlížeče. Vše bez pomoci interního IT oddělení.	ANO	Systém pro kompletní správu účtu AD přímo uživatelem. Jedná se webovou aplikaci.
Umožňuje uživateli domény aktualizovat své osobní údaje v prostředí Active Directory.	ANO	Systém pro kompletní správu účtu AD přímo uživatelem.
Umožňuje uživateli domény resetovat si heslo ze zamknutého účtu přímo z přihlašovací obrazovky Windows, macOS a Linuxu.	ANO	Součástí řešení je agent Gina, která zajistí komunikaci se serverem přímo z uzamčené obrazovky https://www.manageengine.com/products/self-service-password/help/admin-guide/Configuration/Admin-Tools/GINA/GINA-Mac-Linux-installation.html
Umožňuje uživatelům používat SSO pro přístup do OS, ke svým aplikacím a zařízením.	ANO	Systém umožní připojit další aplikace, které provedou automatické ověření uživatele - https://www.manageengine.com/products/self-service-password/kb/integrate-custom-saml-application-for-single-sign-on.html
FUNKCIONALITY PRO ADMINISTRÁTORY/SPRÁVCE		
Kompletní auditní výkazy, které se týkají uživatelů a úkonů, které samostatně provedli v oblasti hesel.	ANO	Systém nabízí předefinované reporty a auditů nebo lze vytvořit I vlastní https://www.manageengine.com/products/self-service-password/help/admin-guide/Reports/Reports.html
Kontrolu používaných uživatelských hesel proti slovníkovému filtru, kontrole vzorových kombinací a podobných způsobů kontroly.	ANO	Systém umožňuje propracovanou volbu politiky hesel https://www.manageengine.com/products/self-service-password/help/admin-guide/Configuration/Self-

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		Service/Password-Policy-Enforcer.html
Zapnutí MFA pro přístupy do Window, macOS a Linux, případně pro VPN přístupy pro všechny či jen vybrané uživatele.	ANO	Aplikace politiky přítupů se aplikují na skupiny v AD
MFA musí umožňovat použití těchto faktorů: Fingerprint/Face ID authentication, YubiKey Authenticator, RSA SecurID, SMS codes, Email codes, Phone call, App-based codes, Push notifikace, Microsoft Authenticator, RADIUS, OATH hardware token např. Yubico, DeepNet Security, atd. ,Google Authenticator, Time-based one-time password, QR code-based authentication, SAML authentication, Smart Card Authentication, Security questions and answers, AD-based security questions.	ANO	Systém umožňuje konfigurace různých způsobů ověření, které lze mezi sebou kombinovat a získat X-faktorové ověření. https://www.manageengine.com/products/self-service-password/help/admin-guide/Configuration/Self-Service/Identity-Verification-Steps.html Systém také umožňuje přidat vlastní TOTP - https://www.manageengine.com/products/self-service-password/help/admin-guide/Configuration/Self-Service/custom-totp-authenticator.html
Mobilní aplikaci pro iOS a Android s funkcionalitami uvedenými v části A2.	ANO	Mobilní aplikace je plnohodnotným doplňkem pro uživatelskou správu účtu
Nastavení podmíněného přístupu pro uživatele na základě IP adresy, času přihlášení, geolokaci, zařízení, ze kterého se přihlašuje, počtu nepodařených přihlášení, atd.	ANO	Ano, systém umožňuje omezení přístupů na základě pravidel https://www.manageengine.com/products/self-service-password/help/admin-guide/Configuration/Self-Service/conditional-access.html
SLUŽBY IMPLEMENTACE A ŠKOLENÍ		
Analýza potřeb – definice systémů napojených na SSO, stanovení pravidel a politiky hesel, analýza potřeb v oblasti reportingu a statistických výkazů.	ANO	Součástí přípravy nastavení je i správné pochopení očekávaného použití a návrh vhodné kombinace nastavení.
Příprava HW a SW prostředí - prostupností v infrastruktuře, otevření požadovaných portů, otevření DMZ, stanovení postupu deploymentu agentů na koncová zařízení	ANO	ANO
Instalace systému do infrastruktury zadavatele.	ANO	ANO
Konfigurace systémů dle výstupů procesní a systémové analýzy a současně napojení servisního účtu, nastavení politik bezpečnosti, nastavení MFA, příprava pro enrollment uživatelů.	ANO	Viz. bod Analýza potřeb
Tvorba a realizace testovacích scénářů před uvedením systému do produkce.	ANO	ANO

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Uvedení do produkčního prostředí.	ANO	ANO
Zaškolení administrátorů.	ANO	ANO

ID 03 Kompletní správa životního cyklu logů

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
OBECNÉ TECHNICKÉ POŽADAVKY		
Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.	ANO	Ano, systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Katalogový list je zde: https://logmanager.com/cs/podpora#documents-for-download
Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.	ANO	Ano, systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	ANO	Ano, veškerá konfigurace systému se provádí v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nekonfiguruje za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.
Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou	ANO	Ano, Logmanager umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému – Uživatelsky definované parsery. Dokumentace obsahuje přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nemá vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
dokumentaci k vytváření parserů a testování jejich funkčnosti.		opravuje uživatele a upozorňuje ho na chyby Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/parsers/
Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.	ANO	Ano, Logmanager umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/classifiers/
Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici nabízeného systému a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.	ANO	Ano, Logmanager přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém umožnuje příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále Logmanager nabízí podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Komunikace Logmanageru zde: https://doc.logmanager.com/latest/cz/additional-informations/communication-of-logmanager/
Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.	ANO	Ano, přijaté logy systém Logmanager standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení,

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		konfigurační změna, značka/tag. Tyto meta informace je možné přidávat i v uživatelsky definovaných parserech.
Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	ANO	Ano, hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.	ANO	Ano, Logmanager zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ANO	Ano, všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem
Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.	ANO	Ano, Logmanager podporuje sběr událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	ANO	Ano, Logmanager nikdy neumožnuje mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou – administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log má dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.	ANO	Ano, Logmanager umožnuje konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace není použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém provádí konsolidaci logů na interním storage logovacího systému.	ANO	Odkaz na klasifikaci zde: https://doc.logmanager.com/latest/cz/web-interface/parser/classifiers/
Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.	ANO	Ano, Logmanager umožnuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu
Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.	ANO	Dokumentace zde: https://doc.logmanager.com/latest/web-interface/logs/reports/
Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	ANO	Ano, Logmanager provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace je dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace, manuální aktualizace a umožňuje používat tuto funkci jen pro vybrané IP adresné prostory. Doložte odkazem na dokumentaci, jakým způsobem se požadované funkce v grafickém rozhraní systému nastavují.	ANO	Ano, Logmanager umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele. Všechny operace uživatelů včetně prohledávání dashboardů jsou logované a lze je auditovat přímo v systému
Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí	ANO	Ano, Logmanager podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365.		prostředí a bez nutnosti instalovat dodatečné externí komponenty
V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.	ANO	Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/sources/ (záložka 0ffice 365)
Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.).	ANO	Ano, Logmanager zajistí v případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám že nedojde ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události jsou ukládány do vyrovnávací paměti.
Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.	ANO	Ano, Logmanager umožnuje unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).
Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.	ANO	Ano, Logmanager má možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nelze administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.
Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO	Ano, Logmanager obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data nelze používat SQL jazyk
Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.	ANO	Ano, Logmanager zajišťuje, že na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.	ANO	Ano, konfigurační a systémové rozhraní a dokumentace k těmto rozhraním je identické v anglickém i v českém jazyce. Není zahrnuta omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran
Systém umožňuje kapacitní i výkonovou škálovatelnost.	ANO	Dokumentace zde: https://doc.logmanager.com/latest/cz/
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB dat.	ANO	Ano, Logmanager nabízí kapacitní i výkonovou škálovatelnost.
Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	ANO	ANO, čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému je 40TB dat pro nabízený Logmanager ve variantě L.
Pokročilá telemetrie a monitoring stavu systému. Systém musí umět zobrazovat kromě běžných telemetrických dat o svojí činnosti i data ohledně rychlosti indexování, délce fronty dat čekající na zpracování a rychlosti odezvy DNS serverů vyřizujících DNS PTR odpovědi. Dále musí umožňovat alertování při překročení prahových hodnot nebo chybě systému, s odesláním upozornění pomocí SMTP nebo Syslogu.	ANO	ANO, díky konfiguraci RAID je možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků neovlivňuje požadovanou kapacitu úložiště.
Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.	ANO	Ano, Logmanager obsahuje jednotnou centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Logmanager nemá více rozdílných konzolí od různých výrobců s rozdílným ovládáním. Konfigurace se neprovádí mimo jednotné webové rozhraní. Dokumentace zde: https://doc.logmanager.com/latest/cz A webové rozhraní konzole: https://doc.logmanager.com/latest/cz/web-interface/

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.	ANO	Ano, Logmanager umožnuje jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Systémové skupiny: https://doc.logmanager.com/latest/web-interface/users/system-groups/ Databázové skupiny: https://doc.logmanager.com/latest/web-interface/users/database-groups/
Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.	ANO	Ano, Logmanager obsahuje ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Monitorování systémů Windows probíhá pomocí agentů.
Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	ANO	Ano, Logmanager podporuje ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému podporuje ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
MINIMÁLNÍ HW KONFIGURACE		
Jedna hardwarová appliance o velikosti max. 2U, včetně lyžin umožňujících vysunutí zapnutého systému z racku pro servisní účely.	ANO	Ano, Logmanager je jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.
HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	ANO	Ano, HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech
2 procesory, min. 16 jader každý, s podporou HyperThreadingu nebo Multi-Threadingu.	ANO	Ano, Logmanager L obsahuje 2 procesory, 16 jader každý, s podporou HyperThreadingu
Min. 128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).	ANO	Ano, Logmanager L obsahuje 128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).
Minimálně 40 TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 8GB. Řadič diskového	ANO	Ano, Logmanager L obsahuje 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.		cache 8GB. Řadič diskového pole obsahuje zálohování
Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.	ANO	Ano, Logmanager obsahuje 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.
Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.	ANO	Ano, Logmanager ve variantě L obsahuje 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému
Ventilátory redundantní a vyměnitelné za provozu.	ANO	
Napájecí zdroje redundantní a vyměnitelné za chodu (hotplug).	ANO	Ano, větráky v systému jsou vyměnitelné za provozu a redundantní.
Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	ANO	Ano, Logmanager obsahuje 2x napájecí zdroje s redundancí napájení za chodu (hotplug)
Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	ANO	Ano, virtuální KVM v Logmanageru umožnuje převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače
VÝKONNOVÉ POŽADAVKY		
Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	ANO	Ano, Logmanager funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).
Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	ANO	Ano, aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace jsou prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému Poznámky jsou na odkazu: Poznámky k vydání | Logmanager dokumentace
Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není	ANO	Ano, Logmanager podporuje downgrade v jednom kroku, pro případ problémů s novou verzí

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade, nebo přiložte odkaz na dokumentaci s detailním popisem.		systému po upgrade. Downgrade je možný bez součinnosti výrobce. Dokumentace zde: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-software-downgrade/
Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	ANO	Ano, Logmanager zajišťuje průměrný trvalý příjem 5000 událostí/s. Výkon je dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém kompletně zpracuje přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťuje normalizaci, zamezuje ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.
Špičkový příjem minimálně 10000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.	ANO	Ano, Logmanager zajišťuje příjem 10000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém zpracuje přijaté události, zamezuje ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu je možné zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nedovolí ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40TB a nad to musí podporovat kompresi ukládaných dat.	ANO	Ano, Logmanager má neomezený počet zařízení pro příjem zasílaných událostí včetně neomezeného množství událostí v GB. Integrovaná databáze má čistou velikost 40TB a podporuje kompresi ukládaných dat

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	ANO	Ano, uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk umožnuje uživateli psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/parsing-rules/
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	ANO	Ano, konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy
Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.	ANO	Ano, Logmanager podporuje on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů lze mít možnost vložení minimálně 20 testovacích zpráv současně Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/parser/parsing-rules/
V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd.	ANO	Ano, Logmanager podporuje v centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		Windows, zpráva byla vygenerována firewallem atd.
Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	ANO	Ano, všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem
Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.	ANO	Ano, v rámci budoucího nasazení ve vysoké dostupnosti a výkonnostní rozšíření je podpora sestavení ve vysoké dostupnosti – Logmanager zajišťuje podporu minimálně 4 nodů v clusteru. Nastavení clusteru se kompletně realizuje v grafickém rozhraní správcovské konzole v jednom kroku, nelze konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti přehledně informuje o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti je kompletní a popisuje všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/system/cluster/
Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.	ANO	Ano, Logmanager využívá pro bezpečné sestavení clusteru i komunikaci s Logmanager Forwardery pevně dané kryptografické algoritmy: pro dohodu na klíči používá Diffieho–Hellmanův protokol s využitím eliptických křivek s křivkou Curve25519, samotné šifrování má podobu autentizovaného šifrování šifrou ChaCha20 a autentizační funkcí Poly1305 s hašovací funkcí BLAKE2. Pro klíče hašovacích tabulek používá SipHash. Použitý je UDP port 51820 pro Cluster a UDP port 51821 pro komunikaci Logmanager <-> Logmanager Forwarder.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	ANO	Ano, v případě rozšíření systému na cluster Logmanager zajistí bez-výpadkovost sběru logů.
Řešení musí umožňovat rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 6TB.	ANO	Ano, Logmanager umožňuje rozšíření mezi-paměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 6TB.
Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	ANO	Ano, Logmanager umožňuje export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.	ANO	Ano, Logmanager podporuje zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore
Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.	ANO	Ano, Logmanager podporuje důvěryhodné zálohování dat na externí systém. Zajišťuje plánované i ad-hoc zálohování. Zálohy dat jsou vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore/
SPRÁVA ALERTŮ		
Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO	Ano, Logmanager je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.
Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	ANO	Ano, text emailu vygenerovaného alertem je uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.
Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	ANO	Ano, Logmanager obsahuje výrobcem předpřipravené sety/vzory alertů a korelací

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací.	ANO	Ano, Logmanager provádí konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů umožnuje okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Dokumentace zde: https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/special-blocks/special-elements/send-alert/
Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.	ANO	Ano, jako výstupní pravidlo Alertu Logmanager umí odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu je možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran Dokumentace zde: https://doc.logmanager.com/latest/web-interface/logs/syslog-output
V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.	ANO	Ano, v alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Dokumentace zde: https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/data-structures-blocks/message-add-tag/
Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.	ANO	Ano, systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a obsahuje možnost vložení testovací zprávy a

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		zobrazení výsledku testu o provedené akci
SBĚR UDÁLOSTI - OS WINDOWS		
Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.	ANO	Ano, události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent současně podporuje jak monitoring interních Windows logů, tak monitoring textových souborových logů. Agent se neinstaluje instalovat individuálně, ale prostřednictvím MS AD Group Policy a nevyžaduje žádnou konfiguraci na cílovém systému. Dokumentace zde: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/logmanager-orchestrator/
Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů Systém, Security, Sysmon atd. a zahoď logy s EventId 9999.	ANO	Ano, agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například zašli pouze logy z adresářů Systém, Security, Sysmon atd. a zahoď logy s EventId 9999.
Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.	ANO	Ano, Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Dokumentace zde: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-agents/
Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace	ANO	Ano, Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Windows agenta se neprovádí z Group Policy.		konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.
Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.	ANO	Ano, komunikace Windows agenta a centrálního systému je zabezpečena TLS 1.2 a podporuje ověřování certifikátem
Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířit Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.	ANO	Ano, Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířit Sysmonem. Dále Windows agent podporuje centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Dokumentace zde: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-agents/
OBSLUŽNOST POBOČEK		
Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček.	ANO	Ano, Logmanager obsahuje centrálně spravované řešení (Logmanager forwarder), které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.
Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.	ANO	Dokumentace zde: https://doc.logmanager.com/latest/cz/web-interface/sources/forwarder/
Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	ANO	Ano, Logmanager Forwarder podporuje centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.
Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven prostup přes firewally a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak	ANO	Ano, Logmanager Forwarder je schopen automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
vypadá komunikační matice pro připojení rešení pro sběr událostí na pobočkách.		centrálou spojení automaticky obnoví.
Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO	Ano, Logmanager forwarder má kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.	ANO	Ano, Logmanager Forwarder má výkon více než 5 tisíc událostí/s, a to i v trvalé zátěži.
Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.	ANO	Ano, Logmanager Forwarder poskytuje podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.
Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO	Ano, Logmanager Forwarder je k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.
Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO	Ano, Logmanager Forwarder je schopen komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
SERVISNÍ PODPORA NA HW A SW		
HW - Požadovaná minimálně 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	ANO	Ano, bude dodána k Logmanageru 5-letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.
Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	ANO	Ano, Logmanager podporuje vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.
SW - Podpora výrobce na aktualizaci systému a parserů min na 5 let. Podpora musí obsahovat pravidelnou aktualizaci SW minimálně 2x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.	ANO	Ano, bude dodána 5-letá podpora výrobce na aktualizaci systému a parserů. Podpora obsahuje pravidelnou aktualizaci SW minimálně 2x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem
SLUŽBY IMPLEMENTACE A ŠKOLENÍ		
Implementační a konfigurační práce v prostředí Zadavatele podle jeho požadavků tj. zejména napojení logovaných zdrojů, provozní reporting, integrace na další systémy kybernetické bezpečnosti a Dashboard kybernetické bezpečnosti.	ANO	Ano, součástí je tvorba a realizace testovacích scénářů před uvedením systému do produkce.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Tvorba a realizace testovacích scénářů před uvedením systému do produkce.	ANO	Ano, součástí je zaškolení administrátorů
Zaškolení administrátorů.	ANO	Ano, součástí je tvorba a realizace testovacích scénářů před uvedením systému do produkce.

ID 04 Bezpečnostní Dashboard

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
FUNKČNÍ POŽADAVKY NA DASHBOARD		
Systém disponuje prostředky pro zobrazení aktuálních provozních informací o infrastruktuře a prostředky pro zobrazení reportů pro podporu řízení.	ANO	Pro zobrazení aktuálních provozních informací je využita kombinace nástrojů PostgreSQL/Grafana. Pro tvorbu a reportování statistických informací pro podporu řízení je využit nástroj PowerBI.
Systém musí zobrazovat stav monitorovaných celků se zpožděním maximálně v řádu jednotek vteřin.	ANO	Nástroj je závislý na zdroji informací, tedy systémech, které provádí samotné měření. Od získání těchto dat, jsou přehledy dostupné v řádu vteřin. Data jsou načítána přehledovými grafy v okamžik jejich zobrazení.
Systém disponuje integrací na zdroje dat Zabbix API, Zabbix DB, MS AD LDAP, MS SQL Server a obecným API pro další systémy.	ANO	Systém disponuje rest API, které umožňuje integraci, Systém disponuje datovými konektory na vyjmenované zdroje.
Systém umožňuje definovat pravidla, která vyhodnocují skupiny provozních atributů ze systému Zabbix a definují úrovně, které jsou provozně optimální, provozně neoptimální, avšak akceptovatelné a provozně neakceptovatelné. Tato pravidla umožňuje seskupovat do skupin, které pokrývají určitý prvek nebo oblast IT infrastruktury, přičemž není omezen počet možných nadskupin, do kterých lze pravidla seskupovat. Stav takto definovaných skupin (např. Virtuální OS) je možné graficky zobrazit i s historií za uživatelsky definovanou periodu.	ANO	Systém disponuje datovou pumpou, jejíž konfigurace umožňuje vyhodnocovat úrovně sledovaných parametrů pro určitý prvek. Tyto prvky lze skládat do větších celků. V grafickém rozhraní je možné zobrazit prvky nejvyšší úrovně a postupně zobrazovat nižší vrstvy. Každý prvek/celek má možnost nastavit úroveň detekce na OK, ERROR, WARNING
Systém umožňuje vizuálně znázornit stav IT bezpečnosti provozu minimálně v těchto oblastech: Infrastruktura, Aplikace, Bezpečnost.	ANO	Systém umožňuje libovolné seskupování prvků infrastruktury, tedy i celky jako je: Infrastruktura, Aplikace, Bezpečnost.
Vyhodnocené údaje jsou ukládány do datového skladu a slouží jako podklad pro statistické vyhodnocení provozu.	ANO	Naměřené hodnoty jsou jednou denně přeneseny do datového skladu. Ten slouží jako podklad pro PowerBI reporty.F195:G199

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Provozní grafické přehledy i reporty pro management umožňuje systém vytvářet a upravovat v dostupném uživatelském nástroji, bez nutnosti zásahu programátora a úpravy samotného systému.	ANO	Systém umožňuje definovat provozní přehledu i statistické PowerBI reporty v nástrojích na designování těchto reportů.
V operativních přehledech i manažerských reportech je možné si zvolit časový rozsah za který je vizualizace vytvořena.	ANO	Ano, je možné konfiguračně nastavit datumové a časové rozmezí.
Systém umožnuje spouštět zpracování dat ze zdrojových systémů a jejich transformaci do interního datového skladu v konfigurovatelných časových intervalech, ale umožňuje také manuální spuštění tohoto procesu.	ANO	Ano, časová úloha pro přenos dat je konfigurovatelná a umožňuje také manuální spuštění.
Uživatelské rozhraní aplikace je realizováno formou webové aplikace a umožnuje definovat vlastní strom složek, do kterého budou organizovány provozní přehledy a manažerské reporty	ANO	Systém disponuje editovatelným stromem pro organizaci tohoto typu obsahu.
Datový sklad systému je svou strukturou rozšiřitelný o nové datové struktury v případě napojení systému na nový zdroj dat, který není v současné době známý. Datové transformace ze zdroje do datového skladu je možné definovat bez nutnosti zásahu programátora.	ANO	Datový sklad je realizován formou MS SQL Serveru a služeb Integration services a Analytics services. Veškerá konfigurace probíhá za využití nástroje MS SQL Server Studio.
Architektura systému umožňuje vyvinout a integrovat datový konektor na nové datové zdroje.	ANO	Systém disponuje mechanismem datových konektorů, na kterých je zbytek systému nezávislý. Tyto konektory transformují specifická data od jednotlivých systémů do interního formátu systému.
Systém umožňuje načítat a synchronizovat uživatelské účty a uživatelské skupiny z MS Active Directory a autentizovat tyto uživatele proti MS AD.	ANO	Systém disponuje plnou integrací na MS Active Directory
Systém umožňuje přiřazovat uživatelům a skupinám aplikační role, které definují přístup k aplikačním funkcím systému.	ANO	Systém disponuje mechanismem aplikačních rolí, do kterých lze přiřazovat uživatele nebo skupiny a tím jim přiřadit oprávnění k aplikačním funkcím.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém umožňuje definovat oprávnění pro aplikační roli, skupinu uživatelských účtů a konkrétní uživatelské účty.	ANO	Systém umožňuje přiřadit oprávnění aplikačním rolím, skupinám uživatelů a uživatelů.
Systém umožňuje nastavit oprávnění na čtení a zápis na složky, do kterých jsou organizovány provozní přehledy a manažerské reporty.	ANO	Systém umožňuje vybraným uživatelům z uživatelského rozhraní zobrazit dialog pro přiřazení oprávnění do složek.
Systém umožňuje definovat synchronizaci uživatelů a skupin s MS AD v konfigurovatelných časových intervalech, ale umožňuje také manuální spuštění tohoto procesu.	ANO	Je možné definovat interval naplánované úlohy, která provádí synchronizaci s MS AD.
Systém umožňuje zobrazit historii běhu naplánovaných úloh.	ANO	V nastavení systému je obrazovka pro zobrazení historie běhu naplánovaných úloh.
Systém umožňuje nahrávat do složek soubory ze souborového systému.	ANO	Systém umožňuje do složek vložit vybraný obsah ze souborového systému.
Systém disponuje detailním auditním logem.	ANO	Auditní/Transakční log je součástí administračního rozhraní.
Systém lze konfigurovat z uživatelského webového rozhraní bez nutnosti zásahů na straně serveru.	ANO	Ano, systém lze konfigurovat z uživatelského rozhraní v modulu "Nastavení systému"
OSTATNÍ POŽADAVKY		
Součástí dodávky je Instalační, administrační a uživatelské dokumentace. Uživatelské rozhraní disponuje kontextovou uživatelskou nápovědou.	ANO	Zmíněné dokumenty dodávány jako PDF dokumenty. Uživatelská příručka je součástí aplikačního helpu.
Systém lze provozovat na operačních systémech Windows a Linux.	ANO	Ano, je systémem plně podporováno.
Součástí dodávky je instalace a konfigurace systému na produkční a testovací prostředí.	ANO	V případě, že je připraveno produkční a testovací prostření, probíhá instalace i konfigurace na oboje.
Systém disponuje dokumentovaným API rozhraním.	ANO	API rozhraní je dokumentováno formou OpenAPI 3.0
Uživatelské webové rozhraní je možné provozovat v posledních verzích prohlížečů Edge, Chrome, Safari a Firefox.	ANO	Ano, systém je testován na vyjmenovaných prohlížečích.
KONFIGURAČNÍ SLUŽBY SYSTÉMU ZABBIX		
Nastavení konfigurace notifikace pomocí SMS a e-mailových služeb.	ANO	součástí řešení je notifikace pomocí SMS a e-mailových služeb.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Konfigurace propojení alertů do Service Deskového systému.	ANO	Systém bude propojen v rámci tiketovacího systému nebo helpdesku
Konfigurace pro:	ANO	Systém bude konfigurování na objevování file systému, CPU a CPU core, SNMP OID, ODBC SQL dotazů a služeb operačních systémů
- objevování file systémů,	ANO	Systém bude konfigurování na objevování file systému, CPU a CPU core, SNMP OID, ODBC SQL dotazů a služeb operačních systémů
- objevování CPU a CPU core,	ANO	Systém bude konfigurování na objevování file systému, CPU a CPU core, SNMP OID, ODBC SQL dotazů a služeb operačních systémů
- objevování SNMP OID,	ANO	Systém bude konfigurování na objevování file systému, CPU a CPU core, SNMP OID, ODBC SQL dotazů a služeb operačních systémů
- objevování ODBC SQL dotazů,	ANO	Systém bude konfigurování na objevování file systému, CPU a CPU core, SNMP OID, ODBC SQL dotazů a služeb operačních systémů
- objevování služeb operačních systémů.	ANO	Systém bude konfigurování na objevování file systému, CPU a CPU core, SNMP OID, ODBC SQL dotazů a služeb operačních systémů
Parametrizace alert skriptů.	ANO	Systém bude konfigurován skripty dle dohodnutých parametrů
Konfigurace pro monitorování fyzických serverů, kde bude nastaveno sledování pro následující parametrů:	ANO	V systému budou monitorovány fyzické servery dle parametrů teplota, LAN interface, stavy úložišť serveru a stavy ventilátorů.
- teplota,	ANO	V systému budou monitorovány fyzické servery dle parametrů teplota, LAN interface, stavy úložišť serveru a stavy ventilátorů.
- LAN interface,	ANO	V systému budou monitorovány fyzické servery dle parametrů teplota, LAN interface, stavy úložišť serveru a stavy ventilátorů.
- stavy úložišť serveru,	ANO	V systému budou monitorovány fyzické servery dle parametrů teplota, LAN interface, stavy úložišť serveru a stavy ventilátorů.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
- stavy ventilátorů.	ANO	V systému budou monitorovány fyzické servery dle parametrů teplota, LAN interface, stavy úložišť serveru a stavy ventilátorů.
Konfigurace výkonnostních parametrů na vybraných zařízeních:	ANO	Systém bude konfigurován dle výkonnostních parametrů na vybraných zařízení – Utilizace CPU, RAM i využití diskové kapacity
- utilizace CPU,	ANO	Systém bude konfigurován dle výkonnostních parametrů na vybraných zařízení – Utilizace CPU, RAM i využití diskové kapacity
- utilizace RAM,	ANO	Systém bude konfigurován dle výkonnostních parametrů na vybraných zařízení – Utilizace CPU, RAM i využití diskové kapacity
- využití diskové kapacity.	ANO	Systém bude konfigurován dle výkonnostních parametrů na vybraných zařízení – Utilizace CPU, RAM i využití diskové kapacity
Konfigurace monitoringu operačních systémů a stavy běžících služeb na monitorovaném operačním systému.	ANO	Bude konfigurován monitoring operačních systémů a stavy běžících služeb na monitorovaném operačním systému. V rámci operačního systému bude také sledováno využití utilizace CPU, utilizace RAM a její celkové množství, využití poskytnutého diskového prostoru, míra využití diskových operací
V rámci operačního systému bude také sledováno využití:	ANO	Bude konfigurován monitoring operačních systémů a stavy běžících služeb na monitorovaném operačním systému. V rámci operačního systému bude také sledováno využití utilizace CPU, utilizace RAM a její celkové množství, využití poskytnutého diskového prostoru, míra využití diskových operací
- utilizace CPU,	ANO	Bude konfigurován monitoring operačních systémů a stavy běžících služeb na monitorovaném operačním systému. V rámci operačního systému bude také

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		sledováno využití utilizace CPU, utilizace RAM a její celkové množství, využití poskytnutého diskového prostoru, míra využití diskových operací
- utilizace RAM a její celkové množství,	ANO	Bude konfigurován monitoring operačních systémů a stavy běžících služeb na monitorovaném operačním systému. V rámci operačního systému bude také sledováno využití utilizace CPU, utilizace RAM a její celkové množství, využití poskytnutého diskového prostoru, míra využití diskových operací
- využití poskytnutého diskového prostoru,	ANO	Bude konfigurován monitoring operačních systémů a stavy běžících služeb na monitorovaném operačním systému. V rámci operačního systému bude také sledováno využití utilizace CPU, utilizace RAM a její celkové množství, využití poskytnutého diskového prostoru, míra využití diskových operací
- míra využití diskových operací.	ANO	Bude konfigurován monitoring operačních systémů a stavy běžících služeb na monitorovaném operačním systému. V rámci operačního systému bude také sledováno využití utilizace CPU, utilizace RAM a její celkové množství, využití poskytnutého diskového prostoru, míra využití diskových operací
Konfigurace monitoringu databázových prostředí:	ANO	V systému bude nastavena konfigurace monitoringu databázových prostředí a to stavy jednotlivých databází, transakční logy, přihlášení uživatelé k databází, velikost souborů transakční logy, přihlášení uživatelé k databázi, detekce starých full backup záloh, sledování verzí databází, velikost souborů transakčních logů,

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		sledování počtu transakcí za definovanou jednotku času, počet aktuálně blokovaných procesorů, počet zámků za určenou časovou jednotku.
- stavy jednotlivých databází,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- transakční logy,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- přihlášení uživatelé k databázi,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- detekce starých full backup záloh,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- sledování verzí databází,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- velikost souborů transakčních logů,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- sledování počtu transakcí za definovanou jednotku času,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- počet aktuálně blokovaných procesů,	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
- počet zámků za určenou časovou jednotku.	ANO	Dle popisu “ Konfigurace monitoringu databázových prostředí:”
Konfigurace monitoringu síťové konektivity:	ANO	V systému bude provedena konfigurace monitoringu síťové konektivity a to stavy vytížení jednotlivých portů, samostatné stavy portů, vytíženost monitorovaných linek.
- stavy vytížení jednotlivých portů,	ANO	V systému bude provedena konfigurace monitoringu síťové konektivity a to stavy vytížení jednotlivých portů, samostatné stavy portů, vytíženost monitorovaných linek.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
- samotné stavy portů,	ANO	V systému bude provedena konfigurace monitoringu síťové konektivity a to stavy vytížení jednotlivých portů, samostatné stavy portů, vytíženost monitorovaných linek.
- vytíženost monitorovaných linek.	ANO	V systému bude provedena konfigurace monitoringu síťové konektivity a to stavy vytížení jednotlivých portů, samostatné stavy portů, vytíženost monitorovaných linek.
Konfigurace monitoringu síťových prvků:	ANO	V systému bude provedena konfigurace monitoringu síťových prvků a to teplota zařízení, verze firmware, stavy jednotlivých komponent síťových prvků, monitoring stavů jednotlivých datových portů
- teplota zařízení,	ANO	Popis dle výše uvedeného “ Konfigurace monitoringu síťových prvků:”
- verze firmware,	ANO	Popis dle výše uvedeného “ Konfigurace monitoringu síťových prvků:”
- monitoring stavu stohovacích portů,	ANO	Popis dle výše uvedeného “ Konfigurace monitoringu síťových prvků:”
- monitoring stavů jednotlivých datových portů.	ANO	Popis dle výše uvedeného “ Konfigurace monitoringu síťových prvků:”
Konfigurace monitoringu diskových úložišť:	ANO	V systému bude provedena konfigurace monitoringu diskových úložišť a to stavy jednotlivých diskových úložišť, sledování teploty diskových úložišť, sledování stavů LAN/SAN portů a sledování zaplněnosti diskového kapacity
- provozní stavy jednotlivých diskových úložišť,	ANO	Popis dle výše uvedeného bodu “ Konfigurace monitoringu diskových úložišť:”
- sledování teploty diskových úložišť,	ANO	Popis dle výše uvedeného bodu “ Konfigurace monitoringu diskových úložišť:”

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
- sledování stavů LAN/SAN portů,	ANO	Popis dle výše uvedeného bodu “ Konfigurace monitoringu diskových úložišť:”
- sledování zaplněnosti diskové kapacity.	ANO	Popis dle výše uvedeného bodu “ Konfigurace monitoringu diskových úložišť:”
Konfigurace parametrů SLA pro sledovaná zařízení:	ANO	V systému bude provedena konfigurace monitoringu diskových úložišť a to stavy jednotlivých diskových úložišť, sledování teploty diskových úložišť, sledování stavů LAN/SAN portů a sledování zaplněnosti diskového kapacity
- procentuální splnění SLA a jeho grafické znázornění pro sledovaná zařízení.	ANO	V systému bude provedena konfigurace monitoringu diskových úložišť a to stavy jednotlivých diskových úložišť, sledování teploty diskových úložišť, sledování stavů LAN/SAN portů a sledování zaplněnosti diskového kapacity
SLUŽBY IMPLEMENTACE A ŠKOLENÍ		
Součástí dodávky je procesní a systémová analýza – definice zdrojových a ukládaných dat a jejich transformace, definice oprávněních příslušných uživatelů a uživatelských skupin. Definice grafických výstupů.	ANO	Výchozí analýza mapující všechny vztahy a jejich mapování na grafické výstupy je součástí dodávky.
Příprava provozních prostředí a zapojení do infrastruktury Zadavatele.	ANO	Součástí dodávky je příprava potřebných provozních prostředí, které se skládá z instalace databází, přípravou virtualizovaných kontejnerů, nastavení síťových záležitostí, nastavení oprávnění, přesměrování logů, zmapování prostupů, definice DNS, a dalších kroků vedoucích k plnému zprovoznění systému.
Konfigurace systémů na základě analýzy.	ANO	Systém bude konfigurován na základě výstupů z úvodní analýzy.
Tvorba a realizace testovacích scénářů před uvedením systému do produkce.	ANO	Systém je dodáván s testovacími scénáři, které jsou přepraveny na míru konkrétní instalace.
Zaškolení administrátorů a klíčových uživatelů.	ANO	Součástí dodávky je školení klíčových uživatelů a administrátorů

ID 05 DLP (data loss prevention)

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
AUDITOVÁNÍ AKCÍ NAD SOUBORY		
Monitoring a reporting všech aktivit spojených se soubory: create, delete, rename, modify, overwrite, move, read, vše v reálném čase.	ANO	Systém nabízí velké množství předefinovaných report a lze sestavit I vlastní. Včetně nastavení upozornění.
Sledování a záznam aktivit se soubory kopírovanými přes tzv. "clipboard" Ctr+C a přes right-click myší.	ANO	Na stanicích lze monitorovat všechny operace se soubory a zajistit i jejich omezení https://www.manageengine.com/data-security/help/es/configuring-copy-prevention-policy-using-datasecurity-plus.html
Audituje a analyzuje všechny úspěšné i neúspěšné uživatelské přístupy k souborům pro případ důkazní potřeby.	ANO	Systém nabízí velké množství předefinovaných report a lze sestavit I vlastní. Včetně nastavení upozornění.
Tvorba detailních záznamů o všech souborových aktivitách, "Kdo, kdy a odkud přistoupil k jakým souborům, kde byly soubory uloženy.	ANO	Systém nabízí velké množství předefinovaných report a lze sestavit I vlastní. Včetně nastavení upozornění.
Analýza auditních dat s cílem identifikace např. nejaktivnější uživatel pracující se soubory, soubor s nejvíce přístupy, proces použitý nejčastěji pro přístup k souborům, atp.	ANO	Systém nabízí velké množství předefinovaných report a lze sestavit I vlastní. Včetně nastavení upozornění.
MONITORING SOUBOROVÉ INTEGRITY		
Správce systému je okamžitě upozorněn v případě např. nárůstu neúspěšných pokusů o úpravu souborů nebo odstranění důležitých firemních dat.	ANO	Systém nabízí velké množství předefinovaných report a lze sestavit I vlastní. Včetně nastavení upozornění.
Systém sleduje indikátory souborové kompromitace, např. aktivita se soubory mimo pracovní dobu a další neobvyklé aktivity.	ANO	Systém nabízí velké množství předefinovaných report a lze sestavit I vlastní. Včetně nastavení upozornění.
Systém sleduje zneužívání oprávnění sledováním častých změn oprávnění, změn SACL, změn vlastníků atd.	ANO	Systém vyhodnocuje chování uživatelů a vytváří jejich skóre https://www.manageengine.com/data-security/help/ra/ownership-analysis.html
Systém umí selektivně monitorovat souborové aktivity u nedůvěryhodných uživatelů a skupin.	ANO	Systém umožní definovat sledování aktivit podle různých kritérií a na základě těchto událostí vytvořit I alert.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
DETEKCE RANSOMWARE ATTACK		
Identifikace ransomware útoků pomocí neobvyklých změn v souborových aktivitách, např. změny oprávnění, počty přístupů, atp. s možností okamžité notifikace správcům systému či pověřeným pracovníkům.	ANO	Součástí monitoring a alertování je i možnost sestavit vlastní notifikaci a akci pro eliminaci hrozby - https://www.manageengine.com/data-security/help/fa/configuring-new-incidents.html
Automatický systém odezvy na incidenty umožňuje vypnutí infikovaného zařízení, zakázání nebo odpojení relace problémového uživatele, atd.	ANO	Viz. předchozí bod a automatické spuštění reakce
Systém umožňuje provedení root-cause analýzy s cílem nalézt "uživatele 0" a popsat způsob šíření infekce.	ANO	
Systém umožňuje vyhledat všechny soubory "pozměněné" v rámci útoku pomocí zabudované knihovny, která obsahuje známé ransomware typy.	ANO	Systém umožní report vybrat soubory, které byly zašifrované jako dopad útoku. https://www.manageengine.com/data-security/help/fa/storage-reports.html
DLP FUNKCE		
Systém umí vynutit použití pouze schválených vyměnitelných úložných zařízení.	ANO	Systém umožní nastavení pravidel používání externích zařízení https://www.manageengine.com/data-security/help/es/configure-external-device-control-policy-using-datasecurity-plus.html
Systém umožní blokovat kopírování souborů na USB úložná zařízení, na místní či síťová sdílení.	ANO	Systém umožní nastavení politik práce se soubory https://www.manageengine.com/data-security/help/es/configure-process-restriction-using-datasecurity-plus.html
Systém umožňuje plnou kontrolu v rámci aktivit se soubory nad zařízeními typu Bluetooth, Wifi, CD/DVD, atp.	ANO	Systém nabízí omezení i pro tyto technologie, viz. https://www.manageengine.com/data-security/help/es/configure-external-device-control-policy-using-datasecurity-plus.html
Systém umí zabránit posílání citlivých souborů formou emailových příloh.	ANO	
Systém umí zabránit tzv. "ex-filtraci" souborů přes externí úložná media.	ANO	Nastavením politik lze zabránit kopírování souborů na externí zařízení.
Systém umí odstranit soubory nebo je umístit do karantény, zastavit přenosy dat přes USB a spustit další aktivní	ANO	

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
preventivní opatření, aby nedošlo k úniku dat.		
Systém umožňuje spuštění tzv. vynucené selektivní kontroly nad externím úložištěm ve formě např. umožnění přístupu pouze pro čtení k podezřelým zařízením, zastavení spuštění spustitelných souborů na USB a další.	ANO	Systém politik umožní omezení přístupu na externí zařízení nebo kontrolu na spuštění souborů na základě jména nebo hash.
Systém umožňuje uzamčení periferních portů koncové stanice v reakci na škodlivé chování uživatelů a tím zabránit potenciálním únikům dat.	ANO	
Systém umožňuje reporting, kdo kdy a odkud připojil jaké zařízení ke koncovým bodům počítačové sítě (např. USB, fotoaparát, microSD a další).	ANO	Systém nabízí USB Security Response
Sledování a analýza, kdy je jakýkoli důležitý soubor zkopírován do nebo z vyměnitelných úložných zařízení.	ANO	Systém nabízí sadu report pro přehled práce se soubory.
Systém umožňuje okamžité uzamčení portů USB, když přes ně uživatelé přesunou omezený obsah. Po vyřešení potenciálního problému je možno porty hned odblokovat.	ANO	Systém nabízí nastavení Response - Enable block USB v Alert Profile
Systém umožní zobrazit vyskakovací zprávy na obrazovce, které uživatele informují a varují před kritickými porušeními firemních pravidel.	ANO	
Systém musí umožnit klasifikaci souborů na základě jejich citlivosti do kategorií, např. Veřejné, Soukromé, Důvěrné nebo Omezené.	ANO	Systém umožňuje nastavení pravidel pro identifikaci souborů s citlivými údaji a na ně aplikovat politiky.
Systém musí umožňovat na koncových stanicích audit všech přístupů k souborům a jejich úprav – včetně vytváření, mazání, přejmenování, změny oprávnění a dalších, vše v reálném čase.	ANO	Systém nabízí sadu report pro přehled práce se soubory s možností alertů pro konkrétní případy.
Systém musí umožnit sledovat emailové aktivity typu kdo e-mail poslal, komu, s jakou přílohou a předmětem, kdy a odkud.	ANO	Systém zahrnuje Email Auditing Report
Systém musí zaznamenávat podrobnosti o všech činnostech se soubory prostřednictvím prohlížečů, jako jsou	ANO	Systém zahrnuje Web Auditing Report

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
např. aktivity zaměstnanců při nahrávání a stahování.		
Systém audituje využití místního tiskového serveru a sleduje, kdo a kdy vytiskl jaké soubory.	ANO	Systém zahrnuje Printer Auditing Report
Systém umožní sledovat vzorce sdílení dat prostřednictvím webových aplikací, jako jsou SharePoint, Exchange, OneDrive, DropBox, a další, s podrobnostmi o tom, kdo, kdy a odkud požadavek podal.	ANO	Systém nabízí kompletní monitoring v rámci Cloud Protection https://www.manageengine.com/data-security/help/cp/
Systém kontroluje neúspěšné pokusy o přístup ke schváleným i neschváleným cloudovým aplikacím, analyzuje požadavky zaslané do nešifrovaných, zakázaných nebo cloudových aplikací s nízkou spolehlivostí, zda nevykazují známky zneužití a kompromitace.	ANO	Systém nabízí řadu reportů s možností upřesnění Control policies
Systém umožní regulovat používání nechtěných webových služeb a zakázat cloudové aplikace, které snižují produktivitu, jako jsou sociální média, streamování videa, online hry a další.	ANO	Systém nabízí řadu reportů s možností upřesnění Control olicies
Systém umožňuje monitorovat prostředí podnikových úložišť a poskytuje zprávy o objemu, typu a trendech v ukládání citlivých dat. Vyhledává např. čísla pasů, e-mailové adresy, čísla kreditních karet a více než padesát dalších typů osobních údajů pomocí předem nakonfigurovaných a přizpůsobitelných patternů/vzorů.	ANO	Systém nabízí kompletní přehledy o úložištích a detekci souborů s citlivými údaji na základě předefinovaných pravidel.
Systém umožňuje automatizovanou klasifikaci souborů obsahujících citlivá, osobní, či jinak kritická data.	ANO	Viz. předchozí bod.
Systém obsahuje předpřipravené reporty a umožňuje být souladu min. s PCI DSS, HIPAA.	ANO	Systém nabízí předpřipravené sady reportů.
Systém umožňuje identifikovat zaměstnance, kteří mají přístup k souborům obsahujícím osobní údaje, a ověřit, zda jsou pro jejich roli vyžadována přístupová práva.	ANO	Systém umožňuje přehled nad přístupy uživatelů napříč úložištěm a identifikaci jejich stupně oprávnění.
Systém umožňuje vyhledat redundantní, zastaralá a tzv. (ROT) data a odebrat je ze souborových serverů pro, pro	ANO	Systém nabízí detailní přehled o struktuře souborů a uložených dat.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
předcházení problémům s výkonem primárního úložiště. Systém umí generovat upozornění na porušení zásad ukládání dat, například zaměstnanci hromadí velké dokumenty, osobní soubory, média nebo jiné nepodstatné soubory.		
Systém generuje reporty o typu, počtu, umístění, vlastnictví duplicitních souborů a umožňuje jejich odstranění.	ANO	Systém nabízí detailní přehled o struktuře souborů a uložených dat.
Systém generuje podrobné reporty o využití diskového prostoru.	ANO	Systém nabízí detailní přehled o struktuře souborů a uložených dat.
Systém generuje podrobné reporty o přístupových právech každého uživatele ke konkrétním souborů, složkám, diskům s cílem odstranit přístupová oprávnění, která nejsou nutná pro výkon práce uživatele.	ANO	Systém nabízí detailní přehledy nad oprávněními pro jednotlivé soubory nebo uživatele.
NOTIFIKAČNÍ FUNKCE		
Systém umožňuje vytvořit vlastní notifikace specifické pro danou organizaci na např. vznik souborů definované velikosti, příliš mnoho souborových změn, atd.	ANO	Systém notifikací je postaven na velké variabilitě podmínek pro splnění podmínky, včetně nastavení trasholdu.
Audit a reporting v souladu s regulačními nařízeními jako např. GDPR. Ukládání auditních dat musí být v databázi MySQL, MS SQL, nebo Oracle.	ANO	Systém umožní provoz i na MS SQL.
SLUŽBY IMPLEMENTACE A ŠKOLENÍ		
Procesní a systémová analýza – definice ukládaných dat, definice oprávněních příslušných uživatelů.	ANO	Součást implementační postupu.
Příprava HW a SW prostředí.	ANO	
Instalace systému do infrastruktury zadavatele.	ANO	Součást implementační postupu.
Konfigurace systémů dle výstupů procesní a systémové analýzy a současně stanovení přístupů a rolí.	ANO	Součást implementační postupu.
Tvorba a realizace testovacích scénářů před uvedením systému do produkce.	ANO	Součást implementační postupu.
Uvedení do produkčního prostředí.	ANO	Součást implementační postupu.
Zaškolení administrátorů.	ANO	Součást implementační postupu.

ID 06 Zavedení systému ISMS a dodání platformy pro řízení kybernetické bezpečnosti

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
FUNKČNÍ POŽADAVKY NA APLIKACI		
Systém podporuje zpracování analýzy rizik.	ANO	Systém podporuje zpracování analýzy rizik.
Systém podporuje nastavení vlastních úrovní hodnot aktiva, pravděpodobnosti hrozeb, výše zranitelnosti, výše rizika hodnocení dodavatelů, účinnosti opatření, a to včetně nastavení barev pro tyto úrovně.	ANO	Systém podporuje nastavení vlastních úrovní hodnot aktiva, pravděpodobnosti hrozeb, výše zranitelnosti, výše rizika hodnocení dodavatelů, účinnosti opatření, a to včetně nastavení barev pro tyto úrovně.
Systém umožňuje provádět analýzu rizik dle norem ISO 27001, Zákona o kybernetické bezpečnosti (včetně implementace EU nařízení NIS2)	ANO	Systém umožňuje provádět analýzu rizik dle norem ISO 27001, Zákona o kybernetické bezpečnosti (včetně implementace EU nařízení NIS2)
Systém disponuje vzorovými katalogy hrozeb a zranitelností. Systém umožňuje přidávat vlastní hrozby a zranitelnosti.	ANO	Systém disponuje vzorovými katalogy hrozeb a zranitelností. Systém umožňuje přidávat vlastní hrozby a zranitelnosti.
Systém nedovolí měnit výchozí položky číselníků a vzorových katalogů. Výchozí položky viditelně označí.	ANO	Systém nedovolí měnit výchozí položky číselníků a vzorových katalogů. Výchozí položky viditelně označí.
Systém umožňuje zavést si vlastní normu s vlastním výčtem hrozeb a zranitelností.	ANO	Systém umožňuje zavést si vlastní normu s vlastním výčtem hrozeb a zranitelností.
Systém umožňuje definovat výchozí pravděpodobnosti hrozeb a výchozí výše zranitelností, které se aplikují při použití těchto položek v identifikovaném riziku.	ANO	Systém umožňuje definovat výchozí pravděpodobnosti hrozeb a výchozí výše zranitelností, které se aplikují při použití těchto položek v identifikovaném riziku.
Systém umožňuje provádět analýzu rizik dle více norem současně.	ANO	Systém umožňuje provádět analýzu rizik dle více norem současně.
Systém disponuje výchozím katalogem rizikových situací, který obsahuje pravděpodobné a smysluplné kombinace hrozeb a zranitelnosti pro různé typy aktiv.	ANO	Systém disponuje výchozím katalogem rizikových situací, který obsahuje pravděpodobné a smysluplné kombinace hrozeb a zranitelnosti pro různé typy aktiv.
Systém při vytváření rizik nabídne dle typu aktiva jen ty kombinace hrozeb a zranitelností, které jsou uvedeny ve vzorovém katalogu rizikových situací.	ANO	Systém při vytváření rizik nabídne dle typu aktiva jen ty kombinace hrozeb a zranitelností, které jsou

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
		uvedeny ve vzorovém katalogu rizikových situací.
Systém disponuje katalogem vzorových opatření pro každou normu. Výchozí opatření nelze měnit, ale je možné vytvářet vzory vlastní.	ANO	Systém disponuje katalogem vzorových opatření pro každou normu. Výchozí opatření nelze měnit, ale je možné vytvářet vzory vlastní.
U každého vzorového opatření je možné určit na jaké zranitelnosti je účinné a jak velká tato účinnost je.	ANO	U každého vzorového opatření je možné určit na jaké zranitelnosti je účinné a jak velká tato účinnost je.
Systém umožňuje evidovat identifikovaná aktiva, kterým lze přiřadit odpovědné garanty, gestory a evidovat u nich dodavatele, finanční hodnotu a způsoby likvidace.	ANO	Systém umožňuje evidovat identifikovaná aktiva, kterým lze přiřadit odpovědné garanty, gestory a evidovat u nich dodavatele, finanční hodnotu a způsoby likvidace.
Systém umožňuje ohodnotit aktiva způsobem komponent CIA (Confidentality, Integrity, Accessibility).	ANO	Systém umožňuje ohodnotit aktiva způsobem komponent CIA (Confidentality, Integrity, Accessibility).
Systém umožňuje konfiguračně nastavit algoritmus hodnocení aktiva. Na výběr musí být minimálně tyto algoritmy: součet CIA, průměr CIA, nejvyšší z CIA.	ANO	Systém umožňuje konfiguračně nastavit algoritmus hodnocení aktiva. Na výběr musí být minimálně tyto algoritmy: součet CIA, průměr CIA, nejvyšší z CIA.
Systém umožňuje vytvářet mezi nadřízenými a podřízenými aktivy vazby a těmto vazbám přiřadit sílu vazby. Úrovně vazby je možné konfiguračně nastavit. Aktivum může mít jedno nebo více aktiv na kterých je závislé. Aktivum může mít jedu nebo více vazeb na aktiva, která jsou závislá na něm.	ANO	Systém umožňuje vytvářet mezi nadřízenými a podřízenými aktivy vazby a těmto vazbám přiřadit sílu vazby. Úrovně vazby je možné konfiguračně nastavit. Aktivum může mít jedno nebo více aktiv na kterých je závislé. Aktivum může mít jedu nebo více vazeb na aktiva, která jsou závislá na něm.
Systém umožňuje definovat šablony aktiv, na základě, kterých lze zakládat opakující se podobná aktiva.	ANO	Systém umožňuje definovat šablony aktiv, na základě, kterých lze zakládat opakující se podobná aktiva.
Systém umožňuje urychlit identifikaci aktiv tím, že umožňuje kopírovat existující aktiva a ukládat je jako nová aktiva.	ANO	Systém umožňuje urychlit identifikaci aktiv tím, že umožňuje kopírovat existující aktiva a ukládat je jako nová aktiva.
Systém umožňuje definovat vlastní atributy, které lze přiřadit šabloně aktiv nebo přímo konkrétnímu aktivu. Lze volit	ANO	Systém umožňuje definovat vlastní atributy, které lze přiřadit šabloně aktiv nebo přímo konkrétnímu aktivu.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
typ vlastního atributu v rozsahu číslo, text, datum, výčet, ano/ne. Lze zvolit výchozí hodnotu atributu.		Lze volit typ vlastního atributu v rozsahu číslo, text, datum, výčet, ano/ne. Lze zvolit výchozí hodnotu atributu.
Systém umožňuje evidovat identifikovat rizika na aktivech tím, že jim umožní přiřazovat hrozby a zranitelnosti.	ANO	Systém umožňuje evidovat identifikovat rizika na aktivech tím, že jim umožní přiřazovat hrozby a zranitelnosti.
Systém umožňuje hromadně zakládat rizika k aktivu dle vzorového katalogu rizikových situací.	ANO	Systém umožňuje hromadně zakládat rizika k aktivu dle vzorového katalogu rizikových situací.
Systém podporuje hodnocení rizik volbou pravděpodobnosti hrozby, výše zranitelnosti a dopadem na aktivum.	ANO	Systém podporuje hodnocení rizik volbou pravděpodobnosti hrozby, výše zranitelnosti a dopadem na aktivum.
Systém umožňuje u nově zakládaného aktiva vytvářet nová rizika.	ANO	Systém umožňuje u nově zakládaného aktiva vytvářet nová rizika.
Systém podporuje evidenci zvládání rizika pro snižování úrovně rizika.	ANO	Systém podporuje evidenci zvládání rizika pro snižování úrovně rizika.
Systém umožňuje přiřazovat jedno zvládání více rizikům a také přiřazovat více zvládání jednomu riziku.	ANO	Systém umožňuje přiřazovat jedno zvládání více rizikům a také přiřazovat více zvládání jednomu riziku.
Systém umožňuje evidovat náklady spojené se zvládáním rizika, a to na úrovni celého zvládání, tak na úrovni dílčích zvládání pro jednotlivá rizika.	ANO	Systém umožňuje evidovat náklady spojené se zvládáním rizika, a to na úrovni celého zvládání, tak na úrovni dílčích zvládání pro jednotlivá rizika.
Systém umožňuje evidovat finanční náklady i pracnosti spojené se zaváděním zvládání rizika.	ANO	Systém umožňuje evidovat finanční náklady i pracnosti spojené se zaváděním zvládání rizika.
Systém umožňuje ke každému zvládání přiřazovat dokumenty, které dokladují toto zvládání rizika.	ANO	Systém umožňuje ke každému zvládání přiřazovat dokumenty, které dokladují toto zvládání rizika.
Systém podporuje evidenci dodavatelů a jejich hodnocení.	ANO	Systém podporuje evidenci dodavatelů a jejich hodnocení.
Systém umožňuje ke každému dodavateli přiřazovat dokumenty.	ANO	Systém umožňuje ke každému dodavateli přiřazovat dokumenty.
Systém umožňuje označit významného dodavatele.	ANO	Systém umožňuje označit významného dodavatele.
Systém umožňuje evidovat dodavatele jako aktivum.	ANO	Systém umožňuje evidovat dodavatele jako aktivum.
Systém umožňuje k dodavateli evidovat vlastní atributy.	ANO	Systém umožňuje k dodavateli evidovat vlastní atributy.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém disponuje správou organizační struktury na úrovni organizačních jednotek a osob. Osoba nemusí být uživatel. Tato struktura bude využitelná pro definici odpovědných osob na úrovni aktiv, rizik, zvládání rizika a dodavatelů.	ANO	Systém disponuje správou organizační struktury na úrovni organizačních jednotek a osob. Osoba nemusí být uživatel. Tato struktura bude využitelná pro definici odpovědných osob na
Systém podporuje generování auditních dokumentů v rozsahu: Zpráva z hodnocení rizik, Prohlášení o aplikovatelnosti a Plán zvládání rizik.	ANO	úrovni aktiv, rizik, zvládání rizika a dodavatelů.
Systém umožňuje vygenerované dokumenty stáhnout do zařízení uživatele a nahrát ze zařízení uživatele jako novou verzi stejného dokumentu.	ANO	Systém podporuje generování auditních dokumentů v rozsahu: Zpráva z hodnocení rizik, Prohlášení o aplikovatelnosti a Plán zvládání rizik.
Systém podporuje fulltextové vyhledávání na úrovni metadat evidovaných objektů i v nahraných dokumentech.	ANO	Systém umožňuje vygenerované dokumenty stáhnout do zařízení uživatele a nahrát ze zařízení uživatele jako novou verzi stejného dokumentu.
Systém disponuje funkcemi pro správu jednotlivých tenantů/organizací, které umožní tenanty zakládat, aktivovat a deaktivovat.	ANO	Systém podporuje fulltextové vyhledávání na úrovni metadat evidovaných objektů i v nahraných dokumentech.
POŽADAVKY NA TECHNICKOU A BEZPEČNOSTNÍ ARCHITEKTURU APLIKACE, PROVOZNÍ POŽADAVKY		
Uživatelská i serverová část aplikace je spustitelná minimálně na operačních systémech Windows a Linux.	ANO	Uživatelská i serverová část aplikace je spustitelná minimálně na operačních systémech Windows a Linux.
Systém disponuje uživatelským webovým rozhraním, které lze spustit v běžně používaných webových prohlížečích Chrome, Firefox a MS Edge v aktuálních verzích.	ANO	Systém disponuje uživatelským webovým rozhraním, které lze spustit v běžně používaných webových prohlížečích Chrome, Firefox a MS Edge v aktuálních verzích.
Jednotlivé komponenty systému lze spouštět ve více instancích a na více serverech a lze se tak přizpůsobovat požadavkům na výkon. Zátěž mezi těmito instancemi je rovnoměrně rozdělována samotným systémem.	ANO	Jednotlivé komponenty systému lze spouštět ve více instancích a na více serverech a lze se tak přizpůsobovat požadavkům na výkon. Zátěž mezi těmito instancemi je rovnoměrně rozdělována samotným systémem.
Systém je možné provozovat v plně virtualizovaném prostření.	ANO	Systém je možné provozovat v plně virtualizovaném prostření.

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Systém je distribuován a provozován formě Docker kontejnerů.	ANO	Systém je distribuován a provozován formě Docker kontejnerů.
Systém dokáže monitorovat sám sebe a tyto informace je schopen prezentovat na svém aplikačním rozhraní. Systém je schopen poskytnout tyto informace monitorovacím systémům třetích stran.	ANO	Systém dokáže monitorovat sám sebe a tyto informace je schopen prezentovat na svém aplikačním rozhraní. Systém je schopen poskytnout tyto informace monitorovacím systémům třetích stran.
Systém dokáže zobrazit statistické informace o svém běhu.	ANO	Systém dokáže zobrazit statistické informace o svém běhu.
Systémové záznamy o běhu aplikace jsou dostupné administrátorovi z uživatelského rozhraní.	ANO	Systémové záznamy o běhu aplikace jsou dostupné administrátorovi z uživatelského rozhraní.
Systém je v principu stavěn na principu tří vrstvé architektury, kdy je od sebe odděleno uživatelské rozhraní, funkce systému a ukládání dat.	ANO	Systém je v principu stavěn na principu tří vrstvé architektury, kdy je od sebe odděleno uživatelské rozhraní, funkce systému a ukládání dat.
Systém disponuje komponentou pro centrální konfigurací.	ANO	Systém disponuje komponentou pro centrální konfigurací.
Funkce systému jsou dostupné přes REST nebo SOAP aplikační rozhraní.	ANO	Funkce systému jsou dostupné přes REST nebo SOAP aplikační rozhraní.
Systém disponuje centrálním transakčním logem, který zaznamenává události o tom kdo, kdy a jakou změnu provedl.	ANO	Systém disponuje centrálním transakčním logem, který zaznamenává události o tom kdo, kdy a jakou změnu provedl.
Komponenty systému zaznamenávají své systémové záznamy o svém běhu do centrálního úložiště. Pokud je jedna funkční událost provedena na více komponentách a generuje více systémových záznamů, musí log obsahovat i korelační ID, které umožní vybrat záznamy z více komponent v kontextu této události.	ANO	Komponenty systému zaznamenávají své systémové záznamy o svém běhu do centrálního úložiště. Pokud je jedna funkční událost provedena na více komponentách a generuje více systémových záznamů, musí log obsahovat i korelační ID, které umožní vybrat záznamy z více komponent v kontextu této události.
Systém podporuje multi-tenantní provoz, kdy je možné na jedné instalaci systému provozovat více samostatných organizací, které jsou datově nezávislé tak, že jsou jejich data uložena v samostatných nezávislých datových	ANO	Systém podporuje multi-tenantní provoz, kdy je možné na jedné instalaci systému provozovat více samostatných organizací, které jsou datově nezávislé tak, že jsou jejich data uložena v samostatných

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
strukturách minimálně na úrovni databáze nebo databázových schématu.		nezávislých datových strukturách minimálně na úrovni databáze nebo databázových schématu.
Systém poskytuje své služby přes jeden vstupní síťový proxy bod, a neumožňuje přímé volání komponent systému.	ANO	Systém poskytuje své služby přes jeden vstupní síťový proxy bod, a neumožňuje přímé volání komponent systému.
Systém disponuje mechanismem naplánovaných úloh pro spouštění operací synchronizace uživatelů.	ANO	Systém disponuje mechanismem naplánovaných úloh pro spouštění operací synchronizace uživatelů.
Systém je možné integrovat na MS Active Directory nebo Azure Entra ID a synchronizovat uživatele a skupiny uživatelů. Je možné konfiguračně určit jaké skupiny uživatelů synchronizovat a na jaké aplikační role tyto skupiny mapovat.	ANO	Systém je možné integrovat na MS Active Directory nebo Azure Entra ID a synchronizovat uživatele a skupiny uživatelů. Je možné konfiguračně určit jaké skupiny uživatelů synchronizovat a na jaké aplikační role tyto skupiny mapovat.
Systém disponuje systémem aplikačních rolí, skupin uživatelů a samotných uživatelů, kterým lze přiřazovat oprávnění.	ANO	Systém disponuje systémem aplikačních rolí, skupin uživatelů a samotných uživatelů, kterým lze přiřazovat oprávnění.
Oprávnění je možné aplikovat na aplikační funkci, typ objektu nebo na konkrétní objekt.	ANO	Oprávnění je možné aplikovat na aplikační funkci, typ objektu nebo na konkrétní objekt.
Systém podporuje autentizaci v souladu se standardem OAuth2, a to buď svými vlastními prostředky nebo integrací na externí zdroj autentizace, který tento standard podporuje, jako je například MS AD nebo Azure Entra ID.	ANO	Systém podporuje autentizaci v souladu se standardem OAuth2, a to buď svými vlastními prostředky nebo integrací na externí zdroj autentizace, který tento standard podporuje, jako je například MS AD nebo Azure Entra ID.
Systém uchovává data v šifrované podobě.	ANO	Systém uchovává data v šifrované podobě.
Systém disponuje transakčním protokolem, který uchovává informace o tom kdo, kdy a co v systému zakládal, mazal nebo měnil.	ANO	Systém disponuje transakčním protokolem, který uchovává informace o tom kdo, kdy a co v systému zakládal, mazal nebo měnil.
Systém umožňuje definovat samostatné nezávislé administrační účty pro každého tenanta zvlášť. Účty je možné aktivovat a deaktivovat dle potřeby.	ANO	Systém umožňuje definovat samostatné nezávislé administrační účty pro každý tenant zvlášť. Účty je možné aktivovat a deaktivovat dle potřeby.
UŽIVATELSKÉ ROZHRANÍ		

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Uživatelské rozhraní systému je plně ovladatelné klávesnicí.	ANO	Uživatelské rozhraní systému je plně ovladatelné klávesnicí.
Uživatelské rozhraní systému je plně ovladatelné myší.	ANO	Uživatelské rozhraní systému je plně ovladatelné myší.
Uživatelské rozhraní systému je přístupné zrakově postiženým.	ANO	Uživatelské rozhraní systému je přístupné zrakově postiženým.
Uživatelské rozhraní umožňuje náhled PDF dokumentů v prostředí aplikace, bez nutnosti stahování PDF souboru do zařízení uživatele.	ANO	Uživatelské rozhraní umožňuje náhled PDF dokumentů v prostředí aplikace, bez nutnosti stahování PDF souboru do zařízení uživatele.
Uživatelské rozhraní systému umožňuje změnu měřítka/velikosti a automatické přizpůsobení ovládacích prvků tomuto měřítku.	ANO	Uživatelské rozhraní systému umožňuje změnu měřítka/velikosti a automatické přizpůsobení ovládacích prvků tomuto měřítku.
POŽADAVEK NA SLUŽBY SOUVISEJÍCÍ SE ZAJIŠTĚNÍM PLNĚNÍ POVINNOSTÍ PLYNOUCÍCH ZE ZoKB (NIS 2)		
Výkon bezpečnostní role osoby odpovědné za kybernetickou bezpečnost	ANO	Výkon bezpečnostní role osoby odpovědné za kybernetickou bezpečnost
Pasivní komunikace s NÚKIB a případně dalšími orgány	ANO	Pasivní komunikace s NÚKIB a případně dalšími orgány
Aktivní komunikace vůči orgánům veřejné správy	ANO	Aktivní komunikace vůči orgánům veřejné správy
Aktivní komunikace vůči NÚKIB - hlášení změn, incidentů apod.	ANO	Aktivní komunikace vůči NÚKIB - hlášení změn, incidentů apod.
Alerting v oblasti hrozeb, změn legislativy a metodik	ANO	Alerting v oblasti hrozeb, změn legislativy a metodik
Zajišťuje procesní část hodnocení a hlášení incidentu včetně dokumentace a archivace	ANO	Zajišťuje procesní část hodnocení a hlášení incidentu včetně dokumentace a archivace
Individuální komunikace administrátora s klientem	ANO	Individuální komunikace administrátora s klientem
Kontaktní místo pro zaměstnance klienta	ANO	Kontaktní místo pro zaměstnance klienta
Informační kanál vůči zaměstnancům klientů	ANO	Informační kanál vůči zaměstnancům klientů
Kontaktní bod pro informace o nestandardním chování	ANO	Kontaktní bod pro informace o nestandardním chování
Kontrola podezřelých e-mailů a příloh	ANO	Kontrola podezřelých e-mailů a příloh
Obsahuje a řídí dokumentaci odpovídající povinnostem ze ZoKB	ANO	Obsahuje a řídí dokumentaci odpovídající povinnostem ze ZoKB
Veškeré změny a úkony mají prokazatelnou auditní stopu, dokumentace je verzována	ANO	Veškeré změny a úkony mají prokazatelnou auditní stopu, dokumentace je verzována

PARAMETRY	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
Odpovědnost za soulad dokumentace se zákonem a metodikami NÚKIB	ANO	Odpovědnost za soulad dokumentace se zákonem a metodikami NÚKIB
Zajišťuje každoroční přezkum aktuálnosti dokumentace	ANO	Zajišťuje každoroční přezkum aktuálnosti dokumentace
Zajišťuje záznam o seznámení klienta s dokumentací	ANO	Zajišťuje záznam o seznámení klienta s dokumentací
Zajišťuje revize bezpečnostních opatření vedením klienta	ANO	Zajišťuje revize bezpečnostních opatření vedením klienta
Zajišťuje vedení a revize evidence aktiv	ANO	Zajišťuje vedení a revize evidence aktiv
Zajišťuje vzorové smluvní doložky pro povinná smluvní ujednání a dle doporučení NÚKIB	ANO	Zajišťuje vzorové smluvní doložky pro povinná smluvní ujednání a dle doporučení NÚKIB
Vede přehledy o školeních kybernetické bezpečnosti	ANO	Vede přehledy o školeních kybernetické bezpečnosti
Zajišťuje vstupní školení v oblasti kybernetické bezpečnost formou e-learningu	ANO	Zajišťuje vstupní školení v oblasti kybernetické bezpečnost formou e-learningu
Provádí pravidelná školení v oblasti kybernetické bezpečnosti formou e-learningu	ANO	Provádí pravidelná školení v oblasti kybernetické bezpečnosti formou e-learningu
Doporučuje potřebná odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost v souladu s jejich pracovní náplní	ANO	Doporučuje potřebná odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost v souladu s jejich pracovní náplní
Jednou ročně provede a dokumentuje vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně aktualizace přehledu bezpečnostních opatření	ANO	Jednou ročně provede a dokumentuje vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně aktualizace přehledu bezpečnostních opatření
Provede pravidelné přezkoumání nastavení veškerých přístupových oprávnění	ANO	Provede pravidelné přezkoumání nastavení veškerých přístupových oprávnění
Zajišťuje plánování a dokumentování auditů, penetračních testů a scanů zranitelnosti	ANO	Zajišťuje plánování a dokumentování auditů, penetračních testů a scanů zranitelnosti

ID 07 Zabezpečené datové úložiště pro provozní zálohy a bezpečnostní logy včetně aplikačních dat ISMS

Dodávka ID 07 Zabezpečené datové úložiště je definována ve 3 následujících specifikacích:
1/ Technická specifikace **POLE 1** a **POLE 2**
2/ Technická specifikace - SOUBOROVÝ A OBJEKTOVÝ SYSTÉM
3/ Technická specifikace ŘÍDÍCÍ SERVER - požadované množství 4 ks

1/ TECHNICKÁ SPECIFIKACE POLE 1 A POLE 2

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
ROZSAH DODÁVKY	Je požadována dodávka 2 (slovy dvou) totožných diskových polí (pokud není dále specifikováno jinak, viz. definice parametrů pro POLE1 a POLE 2). Hodnota všech uvedených parametrů je minimální požadovaná.	ANO	Dodání dle popisu
ARCHITEKTURA A ROZŠIŘITELNOST, PODPOROVANÉ DISKY	Modulární, minimálně dvou řadičové hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce.	ANO	Modulární, dvou řadičové hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce.
	Škálování výkonnosti je možné přidáváním dalších řadičů minimálně do osmi řadičové konfigurace a škálování kapacit pomocí expanzních jednotek.	ANO	Škálování výkonnosti je možné přidáváním dalších řadičů až do 32 řadičové konfigurace a samozřejmě škálování kapacit pomocí expanzních jednotek.
	Celková velikost cache/RAM v jednom řadiči je minimálně 128GB s možností rozšíření na min. dvojnásobek.	ANO	Celková velikost cache/RAM v jednom řadiči je 128GB s možností rozšíření na dvojnásobek.
	Celková rozšiřitelnost je minimálně 420 disků, v případě nasazení více řadičů až čtyřikrát tolik disků.	ANO	Celková rozšiřitelnost jednoho pole je minimálně 420 disků, v případě nasazení více řadičů až 32x tolik

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	Podpora 2,5” nebo 3,5” disků výhradně technologie SSD/flash a to současně: - podpora SCM (Storage Class Memory) - enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD minimálně 1 a vyšší - SSD s hodnotou DWPD minimálně 1 - všechny požadované typy SSD musí být NVMe standardu a musí být možno je současně osadit (mixovat) v rámci jedné diskové police - řešení musí umožňovat nasazení redukce dat tak v reálném čase tak, aby nedošlo k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je požadována separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat	ANO	Podpora 2,5” nebo 3,5” disků výhradně technologie SSD/flash a to současně: - podpora SCM (Storage Class Memory) - enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů FCM s hodnotou DWPD minimálně 1 a vyšší - SSD s hodnotou DWPD minimálně 1 - všechny požadované typy SSD jsou NVMe standardu a je možno je současně osadit (mixovat) v rámci jedné diskové police - řešení umožňuje nasazení redukce dat v reálném čase tak, aby nedošlo k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je přítomna separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat
	Podpora minimálně následujících režimů RAID - 1, 5, 6, 10 nebo minimálně DRAID 1, 6	ANO	Podpora DRAID 1, 6
MINIMÁLNÍ HRUBÁ KAPACITA A OCHRANA DAT	**POLE 1**, Tier 0: minimálně 115 TB na SSD / Flash ve variantě enterprise (DWPD 1 a vyšší). Maximální velikost SSD / Flash modulu je 10TB **POLE 2**, Tier 0: minimálně 14 TB na SSD / Flash ve	ANO	POLE 1, Tier 0: 115,2 TB na FCM modulech ve variantě enterprise DWPD 1, velikost modulu Flash modulu je 9,6TB POLE 2, Tier 0: 14,4 TB na FCM modulech ve variantě enterprise DWPD 1. Velikost Flash modulu je 4,8TB

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	variantě enterprise (DWPD 1 a vyšší). Maximální velikost SSD / Flash modulu je 5TB **POLE 2**, Tier 1: minimálně 288 TB na SSD / SAS 10k nebo NL-SAS 7,2k discích ve variantě enterprise. Maximální velikost disku je 25TB Pro všechny tiery je požadována ochrana dat minimálně proti výpadku 2 disků/modulů současně.		POLE 2, Tier 1: 288 TB na NL-SAS 7,2k discích ve variantě enterprise. Maximální velikost disku je 24TB Pro všechny tiery je k dispozici ochrana dat minimálně proti výpadku 2 disků/modulů současně.
KONEKTIVITA (FRONT-END)	Diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 64/32Gbit FC a 25/10Gbit iSCSI.	ANO	Diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 64/32Gbit FC a 25/10Gbit iSCSI.
	Jsou požadovány min. 2 porty 10Gb iSCSI na řadič, a 4x 32Gbit FC porty na jeden řadič. Tzn. minimálně 8x 32Gbit FC portů a 4x 10Gbit iSCSI portů na jedno dvouřadičové diskové pole.	ANO	Jsou k dispozici 2 porty 10Gb iSCSI na řadič, a 4x 32Gbit FC porty na jeden řadič. Tzn. 8x 32Gbit FC portů a 4x 10Gbit iSCSI portů na jedno dvouřadičové diskové pole.
	POLE 1 je požadována možnost rozšíření FC portů na min. 16 portů 32Gb FC na diskové pole celkem bez nutnosti dokupovat řadiče nebo jiný HW, kromě přídavných FC karet.	ANO	Je možnost rozšíření na 16x 32Gb FC portů na diskové pole celkem bez nutnosti dokupovat řadiče nebo jiný HW, kromě přídavných FC karet.
FUNKCIONALITY PRO EFEKTIVNÍ UKLÁDÁNÍ A SPRÁVU DAT, POKUD JE LICENCOVÁNO, LICENCE MUSÍ BÝT SOUČÁSTÍ DODÁVKY	Vytváření virtuálních logických disků.	ANO	Pole podporuje vytváření virtuálních logických disků.
	Thin provisioning (včetně detekce a reklamace prázdného prostoru).	ANO	Pole podporuje Thin provisioning (včetně detekce a reklamace prázdného prostoru).
	Komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně	ANO	Komprese dat v reálném čase je bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně patřičného HW

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	patřičného HW akcelerátoru nebo na jednotlivých modulech.		akcelerátoru na jednotlivých FCM modulech.
	Deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence.	ANO	Deduplikace dat v reálném čase je bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence.
	Šifrování dat minimálně pro flash/SSD nabízenou kapacitu ve standardu minimálně FIPS 140-3 Level 1 včetně případné licence s podporou quantum safe šifrování.	ANO	Šifrování dat je pro nabízenou flash kapacitu ve standardu FIPS 140-3 Level 1 a to včetně případné licence s podporou quantum safe šifrování Krystals Cyber.
	Inteligentní správa výkonnostních charakteristik (pro minimálně 3 tiery a to včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM).	ANO	Inteligentní správa výkonnostních charakteristik (pro 3 tiery a to včetně případných SCM) virtualizovaných diskových prostorů (tzn, je k dispozici automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM).
	Podpora externí storage virtualizace pro stávající diskové pole včetně potřebné licence a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný.	ANO	Podporuje externí storage virtualizace pro stávající diskové pole včetně potřebné licence a možnost dalšího připojení externích diskových polí od různých výrobců pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný ZDE .
	Podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně	ANO	Podporuje a obsahuje nástroje pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií vice než 1 rok.

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	1 rok (možnost řešit i externím SW nástrojem v rámci dodávky).		
	Podpora Microsoft VSS.	ANO	Podpora Microsoft VSS.
	Podpora VMware VAAI, VASA a VVOL.	ANO	Podpora VMware VAAI, VASA a VVOL.
PODPORA OPERAČNÍCH SYSTÉMŮ A HYPERVIZORŮ	IBM AIX 7.3 a novější.	ANO	IBM AIX 7.3 a novější.
	IBM i 7.2 a novější.	ANO	IBM i 7.2 a novější.
	IBM VIOS 3.1 a novější.	ANO	IBM VIOS 3.1 a novější.
	Oracle Enterprise Linux 7.9 a novější.	ANO	Oracle Enterprise Linux 7.9 a novější.
	Oracle Solaris 11 a novější.	ANO	Oracle Solaris 11 a novější.
	RHEL 7.9 a novější.	ANO	RHEL 7.9 a novější.
	SUSE Linux ES 15 a movější.	ANO	SUSE Linux ES 15 a movější.
	VMware 8.x a vyšší včetně VAAI a VASA integrací	ANO	VMware 8.x a vyšší včetně VAAI a VASA integrací
	Windows server 2016 a novější.	ANO	Windows server 2016 a novější.
TYP PŘÍSTUPU K DATŮM	Blokový, standard FCP a iSCSI.	ANO	Blokový, standard FCP a iSCSI.
KOPÍROVACÍ FUNKCE – LICENCE MUSÍ BÝT SOUČÁSTÍ NABÍDKY A MUSÍ BÝT NA NEOMEZENOU KAPACITU, POČET DISKŮ, EXPANZÍCH JEDNOTEK ATD.	Zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole).	ANO	Je podporováno zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole).
	Možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: - snapshot se po určité době může automaticky stát klonem - inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu - lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) - reverzní snapshoty - lze provést zpětné přesunutí	ANO	Podporuje možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: - snapshot se po určité době může automaticky stát klonem - inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu - lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) - reverzní snapshoty - lze provést zpětné přesunutí dat z

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	dat z klonu do původního originálního Volume		klonu do původního originálního Volume
	Interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle.	ANO	Podporuje Interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle.
ZAJIŠTĚNÍ KONTINUÁLNÍ DOSTUPNOSTI DAT (DR A HA ŘEŠENÍ) - LICENCE MUSÍ BÝT SOUČÁSTÍ NABÍDKY A MUSÍ BÝT NA NEOMEZENOU KAPACITU, POČET DISKŮ, EXPANZÍCH JEDNOTEK ATD.	Upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum.	ANO	Upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum.
	Jednotlivá disková je možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod.	ANO	Jednotlivá disková je možné spojit do clusteru (IBM Flash Grid), který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod.
	Vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na OS nebo virtualizační platformě včetně příslušných licencí	ANO	Je dostupné vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na OS nebo virtualizační platformě včetně příslušných licencí
	Nabízená disková pole musí být možné spravovat, monitorovat z jednoho místa včetně možnosti bez odstávkového přesunu workloadů na jakékoliv diskové pole, které je součástí clusteru tzn. zajištění loadbalancingu na úrovni polí v clusteru, tedy nejenom na úrovni řadičů jednotlivých polí.	ANO	Pomocí integrované funkcionality IBM Flash Grid
	Podpora replikace do třetí lokality.	ANO	Podpora replikace do třetí lokality.
	SW pro redundantní datové cesty v ceně řešení.	ANO	SW pro redundantní datové cesty v ceně řešení.
	Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být	ANO	Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	dohledatelné v matici kompatibility na stránkách Vmware.		v matici kompatibility na stránkách Vmware.
MIGRACE DAT	Transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možností rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit.	ANO	Pomocí externí zabudované storage virtualizace
POČET HOSTITELSKÝCH SERVERŮ PŘIPOJOVANÝCH K DISKOVÉMU POLI	Řešení obsahuje licence na neomezený počet připojení hostitelských serverů.	ANO	Řešení obsahuje licence na neomezený počet připojení hostitelských serverů.
SPRÁVA DISKOVÉHO POLE A DALŠÍ DOSTUPNÉ FUNKCIONALITY	SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru).	ANO	SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru).
	Remote Service (call home) v ceně řešení.	ANO	Remote Service (call home) v ceně řešení.
	Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd.	ANO	Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd.
	Je požadováno potvrzení od lokálního zastoupení výrobce, že nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce.	ANO	Přiloženo v nabídce
BEZPEČNOST	Je požadována ochrana proti ransomware útokům	ANO	Podporuje pomocí dostupných funkcionalit Inline Data

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavením do read-only modu není dostatečná pro splnění tohoto požadavku.		Corruption Detection, Safeguarded Copy a Ransomware detekci na FCM modulech
	Řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni před uložením na SSD / flash moduly.	ANO	Pomocí Inline Data Corruption Detection funkcionality
	Nabízené řešení musí umožňovat kontrolu dat a detekci anomálií a ransomware přímo na úrovni jednotlivých SSD / flash modulech včetně vyhodnocení a dostupnost alertů z jednoho dashboardu.	ANO	Nabízené řešení umožňuje kontrolu dat a detekci anomálií a ransomware přímo na úrovni jednotlivých FCM modulech včetně vyhodnocení a dostupnost alertů z jednoho dashboardu
	Řešení musí umožňovat identifikovat a odhalovat potenciální škodlivý přístup a pro účely auditu shody s příslušnými předpisy musí být tyto protokoly o přístupu plně integrovány se stávajícím SIEM řešením u zadavatele. Zadavatel požaduje doložení oficiální dokumentace, kde bude výše zmíněná integrace detailně popsána.	ANO	Integrace popsána zde
	Integrace se stávajícím SIEM řešením musí být na takové úrovni, aby SIEM dokázal vyvolat vytvoření imutabilní kopie na diskovém poli v případě	ANO	Integrace se stávajícím SIEM řešením je na úrovni, kdy SIEM dokáže vyvolat vytvoření imutabilní kopie na diskovém poli v případě detekce podezřelého chování nezávisle

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	detekce podezřelého chování nezávisle na nastaveném schedulingu diskového pole.		na nastaveném schedulingu diskového pole.
	Software pro správu snapshotů musí podporovat integraci s bezpečnostním řešením, které provádí automatické skenování variability dat mezi snapshoty, aby bylo možné detekovat možné změny a hrozby ransomwaru. Tato kombinace musí být součástí nabídky.	ANO	Software pro správu snapshotů plně podporuje integraci s bezpečnostním řešením, které provádí automatické skenování variability dat mezi snapshoty tak, aby bylo možné detekovat možné změny a hrozby ransomwaru. Tato kombinace je součástí nabídky.
	Je požadována automatizace bezpečnostních skenů HW snapshotů podle typu kritické aplikace (vytvoření více SLA politik) a v případě nalezení hrozby musí existovat možnost obnovit data z čisté verze HW snapshotu.	ANO	Je k dispozic automatizace bezpečnostních skenů HW snapshotů podle typu kritické aplikace (vytvoření více SLA politik) a v případě nalezení hrozby je dostupná možnost obnovit data z čisté verze HW snapshotu.
	Hlášení o pozitivní detekci ransomwarového útoku musí být okamžitě nahlášeno v nabízeném bezpečnostním řešení (pro účely bezpečnostního týmu) a také v softwarovém řešení pro správu snapshotů (pro účely Infrastrukturního týmu).	ANO	Hlášení o pozitivní detekci ransomwarového útoku je okamžitě nahlášeno v nabízeném bezpečnostním řešení (pro účely bezpečnostního týmu) a také v softwarovém řešení pro správu snapshotů (pro účely Infrastrukturního týmu).
	Je požadována tvorba a automatizace aplikačně konzistentních imutabilních kopií pro rychlou obnovu do produkce, pro testování a pro validaci.	ANO	V rámci SW nástroje IBM Storage Sentinel
	Pokud jsou požadovány licence pro výše uvedené, pak je třeba pokrýt kapacitu	ANO	Jsou požadovány licence pro výše uvedené, v nabídce je pokryta kapacita 15TB, platí pouze pro POLE 1.

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	minimálně celkem 15TB, platí pouze pro **POLE 1**.		
	Nabízené řešení musí umožňovat správu bezpečnostních klíčů, jejich periodickou obměnu a možnost exportu na externí zařízení. Lze řešit i externím serverem pro správu těchto klíčů, který však musí být plně certifikován s nabízeným diskovým polem.	ANO	Nabízené řešení umožňuje správu bezpečnostních klíčů, jejich periodickou obměnu a možnost exportu na externí zařízení.
PŘÍSLUŠENSTVÍ	Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.	ANO	Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.
SERVISNÍ PODPORA	Minimálně 5 let; online režim 24x7 s odezvou tentýž den včetně SW podpory, která umožňuje přístup k novým verzím FW, opravným patchům atd.	ANO	Obsahuje servisní podporu na 5 let; online režim 24x7 s odezvou tentýž den včetně SW podpory, která umožňuje přístup k novým verzím FW, opravným patchům atd.
2/ TECHNICKÁ SPECIFIKACE - SOUBOROVÝ A OBJEKTOVÝ SYSTÉM			
PODPORA STANDARDNÍCH PROTOKOLŮ PRO PŘÍSTUP K SOUBORŮM	POSIX-kompatibilní přístup (např. přes NFSv3/4, SMB/CIFS, FTP).	ANO	Podpora všech protokolů včetně CSI/CNSA pro K8s/OpenShift a především nativního GPFS pro extrémní datové přenosy
	Přímý přístup přes GPFS klienty (nativní připojení k file systému).	ANO	Viz předchozí bod
SDÍLENÝ PŘÍSTUP K DATŮM Z VÍCE UZLŮ (PARALLEL FILE SYSTEM)	Možnost paralelního přístupu více klientů k jednomu souborovému systému.	ANO	Vysoká úroveň paralelizace a konkurentní přístup prostřednictvím protokolů je zajištěn
	Podpora synchronního i asynchronního přístupu.	ANO	Je možné vybrat obě možnosti podle parametrů linky nebo preference uživatele
	Horizontální škálování napříč uzly.	ANO	Rozšiřování přístupovými uzly a storage kontrolery.

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
MOŽNOST ŠKÁLOVÁNÍ KAPACITY A VÝKONU	Možnost přidávání disků a uzlů bez výpadku.	ANO	Dynamická rekonfigurace a přidání capacity ke stávajícímu řešení je možné
SPRÁVA SOUBOROVÝCH SYSTÉMŮ A KVÓT	Vytváření vícero file systémů s možností nastavení kvót pro uživatele/skupiny.	ANO	Na globálním file systému jsou vytvářeny manší oddělené FileSety, které je možné přidělovat uživatelům a také nastavovat mnoho vlastností. Například QoS nebo kvoty.
	Automatická migrace dat mezi úrovněmi úložiště (tiering – např. SSD/HDD/TAPE oběma směry).	ANO	Je možné využít funcionalitu Live Cycle Managmentu a policy engine, který zajistí vhodné umístění dat
PODPORA DATOVÉ REDUNDANCE A VYSOKÉ DOSTUPNOSTI	Replikace nebo erasure coding.	ANO	Je možné využít replikace bloků nebo EC dle potřeby uživatele
	Podpora pro diskovou i uzlovou redundanci.	ANO	Záleří na návrhu řešení, kdy navrhujeme N+1 design nebo lepší
SNAPSHOTY A KLONOVÁNÍ	Možnost vytvářet konzistentní snapshoty souborového systému.	ANO	Je možné na úrovni Filesetu. Je udržovan ve skrytém root adresáři FileSetu pro obnovu dat.
	Rychlé klonování dat pro test/dev účely.	ANO	Viz předchozí bod. Je možné použít pro mnoho případů užití jako je backup nebo kopie dat.
INTEGRACE S AUTENTIZAČNÍMI SYSTÉMY	Podpora LDAP, Kerberos, Active Directory.	ANO	Standardní funkcionalita pro o uživatelskou autentifikace
AUDITING A LOGOVÁNÍ	Záznamy o přístupu, změnách souborů, bezpečnostních událostech.	ANO	Logování je zajištěno na úrovni přístupu dle nastavení zákazníka na mnoha úrovních přístupu, modifikace dat atd. Reporting směrem na SIEM systémy.
QOS A I/O POLITIKA	Možnost definovat I/O limity, priority pro různé workloady.	ANO	Profily je možné nastavit individuálně na úrovni FileSet
KOMPATIBILITA SE STANDARDNÍM S3 API	Podpora základních i pokročilých operací (PUT, GET, DELETE, LIST, versioning).	ANO	S3 Integrace prostřednictvím S3 protokolu na CES protokolých uzlech.
	Podpora bucketů, ACL, tagů.	ANO	S3 přístup je na Buckety, které jsou následně prezentované

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
			na jako jednotlivé Filesety. ACL listy, tagy jsou porporoavané
AUTENTIZACE A AUTORIZACE PŘÍSTUPU	IAM-like řízení přístupových práv k bucketům a objektům.	ANO	Scale S3 používá vlastní IAM nebo může vyuřívat přes OAuth externí systémy
	Podpora autentizace přes LDAP nebo externí systémy.	ANO	Na úrovni Specrum Scale Fileset
VERZOVÁNÍ OBJEKTŮ	Schopnost udržovat více verzí jednoho objektu.	ANO	Je možné zapnout na úrovni backetu.
OBJEKTOVÉ TIERING A POLITIKA ŽIVOTNÍHO CYKLU	Možnost automatické migrace objektů na jiné úložné vrstvy.	ANO	Toto je trasparantní na úrovni S3 protokolu a přístupu a děje se na pozadí FileSetu a nastavené politiky
	Podpora politik pro expirační dobu objektů.	ANO	Na úrovni backetu je možné nastavit LifeCycle politiky například 60 dnů atd…
ŠKÁLOVATELNOST A VYSOKÁ DOSTUPNOST	Horizontální škálovatelnost objektové vrstvy.	ANO	Automaticky škáluje s CES nody.
	Podpora více CES (Cluster Export Services) gateway uzlů.	ANO	Cca do 32 uzlů
INTEGRACE S FILE BACKENDEM	Možnost přímého přístupu ke stejným datům jako file i jako object (např. přes unified namespace).	ANO	Je možné přistupovat k objektum který byl například uložen do NSF share prostřednictvím S3 protokolu
PODPORA PRO MULTIPART UPLOADY A VELKÉ OBJEKTY	Možnost ukládat objekty větší než 5 GB pomocí multipart uploadu.	ANO	Ano je to možně a podporované pro S3 API
MONITORING A AUDITOVÁNÍ PŘÍSTUPU	Export metrik do Promethea / Grafany.	ANO	Exporty je dle požadavků možné připravit flexibilně
	Přehled o využití bucketů a datech.	ANO	Resource monitoring je součástí.
PODPORA ŠIFROVÁNÍ	Šifrování dat při přenosu (HTTPS/TLS).	ANO	Pro všechny edice je to standard
	Šifrování dat v klidovém stavu (at rest).	ANO	Pro edice ECE a DME
DATA INTEGRITY A CONSISTENCY	Mechanismy pro kontrolu a opravu poškozených objektů.	ANO	Storage agenti procházejí filesystem a kontrolují pravidlně data
	Podpora pro eventual i strong consistency (konfigurovatelné).	ANO	Redundance je zajištěna na obou úrovních

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
NÍZKÁ LATENCE A VYSOKÁ PROPUSTNOST (THROUGHPUT)	Úložiště musí zajistit nízkou latenci a dostatečnou propustnost pro provoz SIEM, EDR/NDR a log managementu, s optimalizací pro paralelní přístup k logům a databázím.	ANO	Dle návrhu. Zcela univerzální a flexibilní dle potřeby klienta
	Možnost jemného ladění I/O profilu dle typu zátěže.	ANO	Perf tuning rozhrani a parametry prostřednictvím CLI
PREDIKOVATELNOST VÝKONU	I při vysokém zatížení musí systém zajišťovat konzistentní odezvu.	ANO	Dle sizing a navržené architektury. Nicméně lze měnit v případě změny load profilu
VYSOKÁ DOSTUPNOST SLUŽEB	Minimalizace výpadků (≥ 99,99 %).	ANO	Ano dle doporučení pro HA architekturu
	Možnost bezvýpadkové údržby (rolling upgrade, failover).	ANO	Jednotlivé nody, filesystem
HORIZONTÁLNÍ ŠKÁLOVATELNOST	Možnost přidávat další uzly bez přerušení provozu.	ANO	Dynamicky CLI příkaz
	Možnost škálovat storage i výpočetní zdroje nezávisle.	ANO	Bez limitu
OCHRANA PROTI SELHÁNÍ UZLU, DISKU ČI CELÉ LOKALITY	Podpora pro RAID, erasure coding, nebo replikaci dat.	ANO	Na pozadí filesystemu
	Možnost geo-distribuované replikace.	ANO	Sync a Asnyc replikace nebo Streched cluster
AUTOMATICKÉ ZOTAVENÍ (SELF-HEALING)	Automatická oprava poškozených bloků dat nebo metadata.	ANO	Automaticke během pravidelné kontroly konzistence a integrity dat/metadat
ŠIFROVÁNÍ	Data at-rest i in-transit.	ANO	Aktualně dle všech crypto standard, pracuje se na úrovni PQS
	Možnost integrace s HSM/KMS systémy.	ANO	Například IBm GKLM nebo HashiCorp
AUDITOVÁNÍ A ZÁZNAM ČINNOSTÍ	Logování přístupů k objektům a souborům, podpora pro SIEM IBM Qradar.	ANO	Integrace je již součástí. Snadné nastavení
ROLE-BASED ACCESS CONTROL (RBAC)	Možnost oddělení práv na úrovni správy, provozu a přístupu k datům.	ANO	Různé nastavení úrovně přístupu dle požadavku
CENTRALIZOVANÁ SPRÁVA A GUI	Možnost správy přes webové rozhraní.	ANO	CLI i GUI je součástí

PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
INTEGRACE S MONITOROVACÍMI NÁSTROJI	SNMP, REST API pro integraci s externími nástroji (např. Zabbix, Nagios).	ANO	Všechny uvedené včetně Xormon
AUTOMATIZACE PROVOZU	Podpora pro Ansible playbooky, REST API, CLI nástroje.	ANO	Všechny uvedené
PODPORA VÍCE OS A ARCHITEKTUR	Linux (RHEL, SLES, Ubuntu), AIX, případně Windows jako SMB.	ANO	Podporuje všechny uvedené
KOMPATIBILITA S BĚŽNÝMI APLIKAČNÍMI SCÉNÁŘI	Úložiště musí být plně kompatibilní se zálohovacím softwarem Veeam, využívaným ve stávající infrastruktuře.	ANO	Standardní přístup prostřednictvím protokolů. Backup server pokud by byl na Linux patformě může být I součástí clusteru.
INSTALACE	Musí být automatizovatelná (Ansible nebo Deployment Toolkit).	ANO	Existující scripty nebo Ansible PB
	Možnost rolling upgrade bez výpadku služeb.	ANO	Je používáno pro údržbu systému
INTEGRACE	s enterprise backup systémem Veeam.	ANO	Prostřednictvím protokolů
	Snapshoty a export dat do S3 / tape.	ANO	Možno přímo jako Tiering do Tape i S3
PODPORA HYBRIDNÍHO A MULTICLOUD PROSTŘEDÍ	Object storage nebo archivní páskové systémy.	ANO	Oba případy použití
	Podpora pro cloud bursting (např. do AZURE, AWS, Google Cloud, IBM Cloud).	ANO	Je používáno jako cache pro externí datové capacity jako je Cloud, NAS a nebo jiné S3 systémy

3/ TECHNICKÁ SPECIFIKACE ŘÍDÍCÍ SERVER			
TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
POŽADOVANÉ MNOŽSTVÍ	4 kusy	ANO	4x Dell PowerEdge R6615
PROVEDENÍ	1U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Požadujeme LCD display pro základní diagnostiku serveru a uzamykatelný přední panel. Zásuvné ližiny včetně ramene pro vedení kabeláže.	ANO	R6615 with LCD Bezel & ReadyRails Sliding Rails CMA
CPU	Systém založený na AMD EPYC nebo jiném ekvivalentním procesoru kompatibilním se stávající infrastrukturou. Osazení minimálně 32 fyzických jader celkem (1× CPU), frekvence min. 3,0 GHz na jádro. Požadovaná cache CPU min. 256 MB, maximální TDP 280 W.	ANO	AMD EPYC 9354P 3.25GHz, 32C/64T, 256M Cache (280W) DDR5-4800 | https://www.spec.org/ cpu2017/results/rint2017
RAM	Požadovaná kapacita minimálně 512GB. DDR5 min. 4800MT/s, osazeno minimálně 8 moduly s možností dalšího rozšíření.	ANO	8x 64GB RDIMM, 5600MT/s, Dual Rank
DISKY	Server musí podporovat osazení min. 10 x 2,5 palcových disků kategorie SATA/SAS/SSD/NVMe, požadujeme server osazený hot-plug disky: - 2x 480GB SSD SATA s DWPD1 - disky pro OS na odděleném řadiči typu M.2 a kapacitě min. 400GB v RAID1	ANO	2.5" Chassis with up to 10 SAS4/SATA Drives including 4 Universal Slots, Front PERC 11 | 2x 480GB SSD SATA Read Intensive 6Gbps 512e 2.5in Hot-plug AG Drive, 1 DWPD | BOSS-N1 controller card + with 2 M.2 480GB (RAID 1)
DISKOVÝ ŘADIČ	Typu HBA pro přímé připojení disků do systému.	ANO	Dell HBA355i Controller Front

TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
SÍŤOVÉ ROZHRANÍ	- 2 x 1 Gb port Ethernet - 2 x 10/25 Gb port Ethernet typu SFP+/SFP28 - 2 x 32Gb Fibre Channel HBA včetně 2ks 32Gb FC modulů	ANO	Broadcom 57504 Quad Port 10/25GbE, SFP28, OCP 3.0 NIC | Dual Port 32GB Fibre Channel HBA, PCIe Low Profile
NAPÁJENÍ	redundantní síťové napájecí zdroje zajišťující maximální výkon serveru i při výpadku jednoho zdroje a s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting)	ANO	Dual, Hot-Plug, Power Supply Redundant (1+1), 1100W MM Titanium
INTERFACE A ROZŠIŘOVACÍ POZICE	- 3 x USB (1 vpředu, 2 vzadu) - 1 x VGA - min. 2 xPCIe Gen5, z toho min. 1 x 16x	ANO	3 x USB (1 vpředu, 2 vzadu) | 1 x VGA | 2xPCIe Gen5 16x
OS KOMPATIBILITA	- VMware vSphere™ 8.0 a novější - Microsoft® Windows Server® 2019/2022, x64 - Ubuntu Server LTS - Red Hat® Enterprise Linux	ANO	kompatibilita s požadovanými OS
MANAGEMENT A SPRÁVA	Samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru.	ANO	iDrac port
	S podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6.	ANO	iDRAC9, Enterprise 16G
	Monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu	ANO	iDRAC9, Enterprise 16G

TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách.		
	Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP.	ANO	iDRAC9, Enterprise 16G
	Management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů.	ANO	iDRAC9, Enterprise 16G
	Automatická instalace a obnova SSL certifikátu vestavěného serveru.	ANO	iDRAC9, Enterprise 16G
	Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE.	ANO	iDRAC9, Enterprise 16G
	Podpora multifaktorové autentizace, podpora MS AD a generického LDAP.	ANO	iDRAC9, Enterprise 16G
	Možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack.	ANO	iDRAC9, Enterprise 16G
	Data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace.	ANO	iDRAC9, Enterprise 16G
	Podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS	ANO	iDRAC9, Enterprise 16G

TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	serveru a firmware BMC, firmware rollback.		
	Podpora dynamických změn nastavení externích USB portů systému.	ANO	iDRAC9, Enterprise 16G
	Podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment).	ANO	iDRAC9, Enterprise 16G
	Management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora.	ANO	iDRAC9, Enterprise 16G
	Management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace Biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.	ANO	iDRAC9, Enterprise 16G
	OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy	ANO	iDRAC9, Enterprise 16G

TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině.		
	OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home).	ANO	iDRAC9, Enterprise 16G
	Možnost přístupu přes dedikovaný USB port s emulací síťového připojení.	ANO	iDRAC9, Enterprise 16G
	Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle).	ANO	iDRAC9, Enterprise 16G
	Management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru.	ANO	iDRAC9, Enterprise 16G
	Licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit.	ANO	iDRAC9, Enterprise 16G
	Možnost přístupu přes wifi a BT rozhraní přes aplikaci podporující Android a iOS.	ANO	iDRAC9, Enterprise 16G + Quick Sync 2

TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	Management umožňuje monitoring spotřeby el. energie na úrovni serveru.	ANO	iDRAC9, Enterprise 16G
	Konfigurace základních LAN parametrů managementu pomocí LCD na šasi serveru.	ANO	iDRAC9, Enterprise 16G + LCD Bezel
	Identifikace připojeného vzdáleného uživatele.	ANO	iDRAC9, Enterprise 16G
	Vzdálená identifikace serveru.	ANO	iDRAC9, Enterprise 16G
BEZPEČNOSTNÍ FUNKCE	Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli.	ANO	iDRAC9, Enterprise 16G + Secured Component Verification
LICENCE	RHEL, 1-2SKT, Physical Node, 5YR Premium Sub, 1 Virtual Guest, Digitally Fulfilled	ANO	RHEL, 1-2SKT, Physical Node, 5YR Premium Sub, 1 Virtual Guest
ZÁRUKA, SERVISNÍ PODMŃKY	Jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory. Součástí nabídky musí být certifikovaná instalace a zprovoznění zejména veškerého dodaného HW, včetně konfigurace HW, SW a politik pro práci s daty v plném rozsahu dodávky, provedení akceptačních testů, předání uživatelské a další	ANO	ProSupport Next Business Day Onsite Service 60 měsíců

TECHNICKÉ PARAMETRY	SPECIFIKACE PARAMETRU	SPLŇUJE ANO/NE	POPIS ŘEŠENÍ
	dokumentace a přístupových hesel HW.		

IBM Česká republika, spol. s r.o.

The Park
V Parku 2294/4
148 00 Praha 4 –
Chodov
[redacted]

V Praze dne 12. září 2025

Věc: **Potvrzení výhradního zastoupení výrobce IBM**

Pro: Open Apps Development, a.s., Kurta Konráda 2517/1, Libeň, 190 00 Praha 9, IČO: 116 49 275

Název VZ: Zvýšení kybernetické bezpečnosti Městské části Praha 2
evidenční číslo ve VVZ: Z2025-045459

Zadavatel: Městská část Praha 2, náměstí Míru 600/20, 120 00 Praha 2
IČO: 00063461

Společnost IBM Česká republika, spol. s r.o., se sídlem V Parku 2294/4, 148 00 Praha 4 - Chodov, tímto potvrzuje že nabízené řešení (disková pole) je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce.

Toto potvrzení je vydáno na žádost partnera.

....
[redacted]
IBM Česká republika, spol. s r.o.

Příloha č. 4: Harmonogram prací

Milník	**Termín**	**Popis**
D0	Den účinnosti smlouvy	Zahájení plnění
D1	D0 + 45 dní	Dokončení etapy 1
D2	D0 + 120 dní	Dokončení etapy 2
D3	D2 + 60 měsíců	Ukončení poskytování technické podpory výrobce

Příloha č. 5: Realizační tým

SPECIFIKACE ROLÍ A SEZNAM ČLENŮ REALIZAČNÍHO TÝMU VČETNĚ POŽADOVANÉ KVALIFIKACE

1/ Specifikace rolí včetně požadované kvalifikace

SEZNAM ROLÍ V REALIZAČNÍM TÝMU	
Požadavky	**Projektový manažer**
Požadovaná minimální certifikace	Platná certifikace v oblasti projektového řízení nebo technická certifikace v oblasti informačních technologii. Certifikace na úrovni: - Prince 2 – Practitioner certificate in Project management a vyšší. (Zadavatel umožňuje předložit i obdobné certifikace např. IMPA D nebo PMI CAPM). - certifikát ITIL v3 Foundation nebo ekvivalent
Požadovaná zkušenost	Osobní účast na pozici projektového manažera (nebo jeho zástupce) nebo specialisty implementace kyberbezpečnostních systémů (XDR, SIEM apod.) na realizaci alespoň 1 projektu, splňujících definici významné zakázky podle odst. 1) – 4) čl. 5.1.2, dokumentu Požadavky zadavatele na kvalifikaci.
Požadavky	**Specialista architekt řešení**
Požadovaná minimální certifikace	Platná certifikace v oblasti návrhu a architektury informačních technologií. Certifikace v úrovni: TOGAF 9 Foundation a vyšší. Zadavatel umožňuje předložit i obdobné certifikace např. Archimate Foundation, IASA Associate či CITA-P (Certified Information Technology Architect Professional Certification)
Požadovaná zkušenost	Osobní účast na pozici architekta řešení či specialisty implementace kyberbezpečnostních systémů (XDR, SIEM apod.) na realizaci alespoň 1 projektu, splňujících definici významné zakázky podle odst. 1) – 4), čl. 5.1.2, dokumentu Požadavky zadavatele na kvalifikaci.
Požadavky	**Specialista řízení IT služeb**
Požadovaná minimální certifikace	Platná certifikace v oblasti řízení a správy IT služeb. Certifikace v úrovni: ITIL – Foundation a vyšší. Zadavatel umožňuje předložit i obdobné certifikace např. Lead auditor pro IT služby
Požadovaná zkušenost	Osobní účast na pozici specialisty řízení IT služeb či specialisty implementace kyberbezpečnostních systémů (XDR, SIEM apod.) na realizaci alespoň 1 projektu, splňujících definici významné zakázky podle odst. 1) – 4), čl. 5.1.2, dokumentu Požadavky zadavatele na kvalifikaci.
Požadavky	**Specialista systémů řízení bezpečnosti informací (SŘBI)**
Požadovaná minimální certifikace	Platná certifikace v oblasti řízení bezpečnosti informací: Information Security Management System Lead Auditor (ISO/IEC 27001) nebo CISA (Certified Information Systems Auditor) nebo CISSP (Certified Information Systems Security Professional) nebo obdobná.
Požadovaná zkušenost	Osobní účast na pozici specialisty systémů řízení bezpečnosti nebo specialisty implementace kyberbezpečnostních systémů (XDR, SIEM apod.) na realizaci alespoň 1 projektu, splňujících definici významné

	zakázky podle odst. 1) – 4), čl. 5.1.2, dokumentu Požadavky zadavatele na kvalifikaci.
Požadavky	**IT specialista #1**
Požadovaná minimální certifikace	Dvě platné technické certifikace specialisty od výrobce nabízeného řešení kyberbezpečnostních systémů (XDR, SIEM apod.)
Požadovaná zkušenost	Osobní účast na pozici IT specialisty SIEM nebo specialisty implementace kyberbezpečnostních systémů (XDR, SIEM apod.) na realizaci alespoň 1 projektu, splňujících definici významné zakázky podle odst. 1) – 2), čl. 5.1.2, dokumentu Požadavky zadavatele na kvalifikaci.
Požadavky	**IT specialista #2**
Požadovaná minimální certifikace	Dvě platné technické certifikace specialisty od výrobce nabízeného řešení kyberbezpečnostních systémů (XDR, SIEM apod.)
Požadovaná zkušenost	Osobní účast na pozici IT specialisty SIEM nebo specialisty implementace SIEM na realizaci alespoň 1 projektu, splňujících definici významné zakázky podle odst. 1) – 2), čl. 5.1.2, dokumentu Požadavky zadavatele na kvalifikaci.
Požadavky	**IT specialista OS Linux**
Požadovaná minimální certifikace	Platná technická certifikace (RHCE) Redhat Enterprise Linux Certified Engineer v.8 a vyšší
Požadavky	**IT specialista OS Windows**
Požadovaná minimální certifikace	Platná technická certifikace MCSA nebo MCSE v oblasti serverů Microsoft.
Požadavky	**IT specialista na desktopové virtualizační datacentrové systémy VMware**
Požadovaná minimální certifikace	Platná certifikace VMware Certified Professional – Data Center Virtualization 2023 a vyšší
Požadavky	**IT specialista na zálohování dat VEEAM**
Požadovaná minimální certifikace	Platná certifikace: Veeam Certified Engineer 2021 (VMCE 2021) a vyšší
Požadavky	**IT specialista na systémy SIEM QRADAR**
Požadovaná minimální certifikace	Dvě platné certifikace IBM Certified Deployment Professional Security QRadar SIEM V7.5 a vyšší, a zároveň IBM Certified Administrator - Security QRadar SIEM V7.5 a vyšší

2/ Jmenný seznam členů týmu

Role v týmu	Jméno, Příjmení	Kontakt (email, telefon)	Status[1]
Projektový manažer	[redacted]	[redacted]	zaměstnanec dodavatele
Specialista architekt řešení	[redacted]	[redacted]	zaměstnanec poddodavatele
Specialista řízení IT služeb	[redacted]	[redacted]	zaměstnanec dodavatele
Specialista systémů řízení bezpečnosti informací (SŘBI)	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista #1	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista #2	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista OS Linux	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista OS Windows	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista na desktopové virtualizační datacentrové systémy VMware	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista na zálohování dat VEEAM	[redacted]	[redacted]	zaměstnanec poddodavatele
IT specialista na systémy SIEM QRADAR	[redacted]	[redacted]	zaměstnanec poddodavatele

[1] **Status vyjadřuje právní vztah příslušné osoby k dodavateli, tj. vyžadujeme informaci, zda se jedná poddodavatele nebo zaměstnance dodavatele či zaměstnance poddodavatele.**

Příloha č. 6: Obsah základní provozní dokumentace.

OBSAH ZÁKLADNÍ PROVOZNÍ DOKUMENTACE

Základní provozní dokumentace je vyžadována pro produkty ID 01, 02,03,04, 05 a 07, pro 06 není relevantní.

Dokumentace musí obsahovat zejména:

- součást dodávky produktu je HW:

  - schematické znázornění zapojení HW komponent v síti LAN
  - použitý IP adresní prostor
  - popis účelu, který HW komponenta plní
  - fyzické umístění (označení a pozice v RACKu)
  - označení SWITCH/PORT připojení NIC (data a management) HW zařízení do LAN
  - účet administrátora (plná správa zařízení)

- . součást dodávky produktu je SW:

  - seznam použitých licencí (S/N nebo označení výrobce nebo P/N výrobce, množství)
  - identifikace zařízení v LAN, na kterém je SW instalován
  - specifikace a umístění aplikační databáze (pokud existuje), účet administrátora databáze
  - konfigurace síťové komunikace (protokol, port)
  - identifikace propojení na další aplikace a systémy
  - specifikace umístění a specifikace schématu provozních záloh pokud bylo řešeno v rámci dodávky
  - účet administrátora (plná konfigurace systému)

Příloha č. 7: Seznam poddodavatelů

Obchodní firma nebo název nebo jméno a příjmení poddodavatele	IČO a sídlo poddodavatele	Část díla, jehož provádění bude poddodavatel plnit či zajišťovat
Next Generation Security Solutions s.r.o.	06291031 U Uranie 954/18, Holešovice, 170 00 Praha 7	Spolupráce při dodávce hardware a software včetně základního nastavení prostředí nástroje pro detekci kybernetických bezpečnostních událostí (EDR/XDR), MFA (vícefaktorového ověřování), nástroje na sběr a vyhodnocování logů, bezpečnostního dashboardu a DLP. Služby IT specialistů: Specialista – architekt řešení Návrh cílového implementačního konceptu a architektonického řešení. Definice integračních vazeb mezi dodávanými systémy (XDR, SIEM, DLP, ISMS, úložiště). Koordinace technického návrhu a metodické vedení realizačního týmu. Specialista – systémů řízení bezpečnosti informací (SŘBI) Zavedení a rozvoj ISMS dle zákona o kybernetické bezpečnosti a NIS2. Vytvoření bezpečnostních politik, metodik a dokumentace. Podpora při nastavení procesů řízení rizik, přístupů a bezpečnosti dodavatelského řetězce. IT specialista 1. osoba Implementace a konfigurace nástrojů EDR/XDR. Nastavení pravidel detekce, reakce a forenzních funkcí. Integrace s dalšími bezpečnostními systémy (SIEM, Dashboard). IT specialista 2. osoba Podpora implementace a konfigurace XDR řešení. Monitoring a testování funkčnosti systému, tvorba reportů. Spolupráce na zátěžových a akceptačních testech. IT specialista OS Linux Instalace, konfigurace a správa bezpečnostních agentů a nástrojů v prostředí Linux. Integrace Linux serverů do log-managementu a SIEM. Řešení provozních incidentů a zajištění bezpečnostních aktualizací. IT specialista OS Windows Nasazení a konfigurace agentů EDR/XDR pro Windows servery a stanice. Integrace Windows logů do SIEM a log-managementu.

		Nastavení politik, oprávnění a MFA ve Windows prostředí. IT specialista na desktopové virtualizační datacentrové systémy VMware Implementace a správa virtualizační platformy VMware v kontextu bezpečnostního řešení. Integrace zálohování a monitoringu ve virtualizovaném prostředí. Podpora vysoké dostupnosti a testování záložních scénářů. IT specialista na zálohování dat Veeam Implementace a konfigurace zálohovacího systému Veeam. Nastavení strategií zálohování a obnovy, testování obnovitelnosti dat. Integrace s úložišti a dalšími KB systémy. IT specialista na systémy SIEM QRadar Instalace, konfigurace a integrace SIEM IBM QRadar. Nastavení parserů, korelačních pravidel a dashboardů. Monitoring bezpečnostních událostí a podpora forenzních analýz.

Doložka

potvrzující, že byly splněny podmínky platnosti právního úkonu, ve smyslu ust. § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů

Zveřejněno: od / do /

~~Schváleno~~ odsouhlaseno usnesením ~~ZMČ~~ RMČ

č. 598 ze dne 6.10.2025

vedoucí odboru:

…….

podpis

Nehodící se škrtněte