Název dokumentu	Vysvětlení zadávací dokumentace č. 4
Zadavatel	***ČEPRO, a.s.*** *Praha 7, Dělnická 213/12, Holešovice, PSČ 170 00* *IČ: 60193531* *zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2341* *Zastoupena:* *Mgr. Jan Duspěva, předseda představenstva* *Ing. František Todt, člen představenstva*
Název veřejné zakázky	Privileged Identity Management/ Privileged Access Management (PIM/PAM)
Ev. č. veřejné zakázky	
Druh zadávacího řízení	ZPŘ
Ev. č. zadavatele	178/20/OCN

V rámci výběrového řízení na nadepsanou zakázku na dodávky, která je zadávána postupem analogickým postupu podle zákona č. 134/2016 Sb., o veřejných zakázkách (dále jen „zákon“), Vám zasíláme Vysvětlení zadávací dokumentace č. 4 k nadepsané veřejné zakázce.

Objednatel obdržel dne 15.10.2020 a 22.10.2020 prostřednictvím profilu zadavatele žádost dodavatelů o vysvětlení zadávací dokumentace zakázky, na základě čehož se zadavatel rozhodl poskytnout odpovědi na předložené dotazy k nadepsané zakázce formou zveřejnění tohoto vysvětlení zadávací dokumentace.

Dotaz č. 2	Zadavatel v Zadávací dokumentaci, konkrétně dokumentu „178-20_ZD – PIM PAM – 201002“ v článku č. 1.5.3. Geografické umístění a dohledy uvádí, že: Dostupnost PIM/PAM řešení bude monitorována na úrovni Security Operations Centra v režimu 24x7. Chápe Uchazeč správně, že pro zajištění dostupnosti systému musí mít uchazeč vlastní Security Operations Centrum?
Odpověď č. 2	Zadavatel nepožaduje, aby dodavatel disponoval vlastním Security Operations Centrem (SOC).

Dotaz č. 3	Detekce a blokování podezřelých aktivit Systém umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření – alerting, změna přihlašovacích údajů, terminace/pozastavení relací. Je požadováno za splnění tohoto požadavku, pokud předložené řešení umožní automatickou detekci podezřelého chování, ale nebude přímo automaticky vynucovat nápravná opatření? V praxi je řešení požadované Zadavatelem velmi nekomfortní pro administrátory, jelikož jim může být často přerušováno spojení. Takovouto metodou řešení detekci a blokaci podezřelých aktivit pouze jeden výrobce působící na českém trhu. Neuvolnění by znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 3	Cílem požadavku Zadavatele je efektivně vynutit bezpečnostní politiku v prostředí kritické infrastruktury a včasně ošetřit identifikované incidenty. V případě, zjištění kompromitace hesla musí, dle soudu zadavatele, dojít k okamžité změně hesla a ukončení všech session, které kompromitované heslo používají. Pokud se toto nestane, vystavuje se Zadavatel riziku dokončení kybernetického útoku, které může mít za následek ztráty na životech, majetku a/ nebo způsobit závažnou ekologickou havárii. Požadovaná terminace/ pozastavení relace je vždy předmětem konfigurace a ochranné

	tohoto typu bude vždy realizováno v souladu s mírou daného rizika. Zadavatel připomíná, že očekává, že nasazená pravidla bude možné časově ohraničit např. na dobu mimo pracovní dobu, kde doba reakce na přijatý alert v kombinaci s manuálním zásahem může znamenat významné zvýšení rizika úspěšného dokončení útoku. Zadavatel připomíná, že ochrana zdraví zaměstnanců a občanů, majetku, životního prostředí a zajištění kritické infrastruktury státu jsou hlavní zásady Zadavatele a veškeré požadavky ve zadávacím řízení vždy směřují k zajištění těchto fundamentálních zásad. Zadavatel nijak neomezuje možná řešení požadavku ani způsoby, jakými je dodavatel zajistí, avšak dodané řešení musí umožnit automatické pozastavení, nebo terminaci potenciálně nebezpečných relací, jak je stanoveno v původním požadavku. V této fázi hrubého nástinu dodavatele však není možné určit, zda dodavatelem zamýšlené řešení bude dostatečně plnit veškeré požadavky tohoto bodu, jakož i ostatních požadavků zadávací dokumentace. K tomuto účelu nemůže ani vysvětlení zadávací dokumentace sloužit. V principu a v obecné rovině však Zadavatel nevidí důvod dodavatelem popsané řešení odmítat.

Dotaz č. 4	Zadání: Export auditních dat Systém musí umožňovat export auditních záznamů pro nástroje typu Crystal reports atp. Dotaz: Pokud by Zadavatel požadoval export auditních dat pro nástroje tupu Crystal reports atp. jednalo by se o bezpečnostní riziko. Standardní řešení PIM/PAM si lze představit jako „trezor“ kde jsou veškerá data bezpečně uložena a nejsou k nim známa hesla. Z tohoto důvodu veškeré citlivé informace uchovává PIM/PAM v sobě. Požadavek směřuje na jednoho výrobce. Neuvolnění by znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 4	Zadavateli není ze žádosti dodavatele zcela zřejmé jaký je dotaz, na který by bylo z jeho strany možné odpovědět. Přesto se pokusí alespoň v obecné rovině vyjádřit, tak jak je uvedeno níže. Cílem požadavku je umožnit práci s auditním záznamem mimo prostředí PIM/ PAM a to zejména v případech nutné externí forenzní analýzy/ šetření, vyšetřování incidentů a nestandardních činností v rámci společnosti, včetně možnosti využití pokročilých analytických metod softwarů třetích stran, které již Zadavatel vlastní. Zadavatel je toho názoru, že v případě auditních záznamů je kritická zejména jejich integrita a nepopiratelnost, která se exportem jejich kopie nijak nesnižuje. Dodavatel ve svém dotazu naznačuje, že řešení PIM/ PAM je jediným správným nástrojem pro správu auditních záznamů, což dle názoru Zadavatele naopak limituje ostatní řešení, které by pro správu auditních záznamů mohli použít jiné systémy. Dále, Zadavatel je toho názoru, že v oblasti IT je běžná analýza logů mimo řešení PIM/ PAM, jako jsou řešení typu SIEM nebo BI řešení, která umožňují využití tzv. machine-learning algoritmů nebo artificial inteligence, a významným způsobem tak zjednodušují jejich analýzu a korelaci. Zadavatel dále považuje za běžnou praxi, že společnost pracuje s citlivými údaji (údaji kde je kritická důvěrnost dat) ve formě elektronických a tištěných dokumentů, tedy mimo nástroj PIM/ PAM a při dodržení odpovídajících požadavků na zabezpečení, nepovažuje export auditních záznamů z nástroje PIM/ PAM za nijak problematický. Aby Zadavatel předešel nedorozumění pramenící z nesprávně interpretovaného požadavku dodavatele, uvádí následující – není podmínkou, aby nástroj PIM/ PAM umožňoval export auditních záznamů výhradně ve formátu crystal reports a zcela určitě připouští možnost exportu i do jiných druhů strukturovaných typů dokumentů, které je možné otevřít na trhu běžně dostupnými kancelářskými nástroji, jako je např. formát CSV, Microsoft EXCEL, Microsoft Access, apod.

Dotaz č. 5	Zadání: Zálohování systému Řešení musí umožňovat bezpečné zálohování dat systému -

	zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů. Dotaz: Zabezpečení Disaster Recovery Key je pojem používaný primárně jedním výrobce PIM/PAM. Co jsi pod tímto pojmem obecně představit? Je možné využít např. přístup pomoc zabezpečených hesel?
Odpověď č. 5	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Pojmy „disaster recovery“ (překládaný jako „obnova po havárii“), „key“ (překládaný jako „klíč“ nebo též „heslo“), nebo jejich spojení, jsou dle názoru a znalosti Zadavatele zcela běžné pojmy používané v oblasti IT a IT bezpečnosti, ke kterým neexistuje, separátně ani ve spojení, žádná ochranná známka. Pokud je tento pojem mimo znalost Zadavatele ve skutečnosti registrován specifickým dodavatelem nebo výrobcem, žádá zadavatel o prokázání této skutečnosti a pojem v zadávací dokumentaci bude neprodleně změněn. Pro vyloučení jakýchkoliv pochybností zadavatel dodává, že uvedl-li v zadávací dokumentaci pojem „disaster recovery key“ a tento pojem by představoval označení konkrétního výrobku či služby, tak obdobně podle ustanovení § 89 odst. 6 zákona připouští rovnocenné řešení. Cílem tohoto požadavku je zabezpečení záloh pomocí obecného mechanismu, který je dostatečně robustní a bezpečný pro zajištění obnovy zálohovaných dat v případě řešení havarijního stavu.

Dotaz č. 6	Zadání: Automatická instalace Veškeré komponenty řešení musí umožňovat automatickou instalaci v cloud i on-premise prostředí. Řešení minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci pre-requisite, instalaci komponent, hardening a základní konfiguraci. Automatickou instalaci je možné řešit například pomocí Ansible roles. Dotaz: Co je myšleno „automatickou instalací“? Chápeme správně, že se to týká přidání nových „assetů“ nebo účtů v cloudu nebo on-premise prostředí? Dále prosíme, co je myšleno kopírováním instalačních souborů? Můžete specifikovat nějaký konkrétní případ, čeho konkrétně se má týkat kopírování instalačního souboru, resp. čím se toho má dosáhnout?
Odpověď č. 6	Hlavním cílem tohoto požadavku je zajištění snadného, rychlého a efektivního procesu instalace a nápravy chybových stavů. Zadavatel cílí na maximální automatizaci instalačního procesu, která je nezbytná pro přípravu, testování a případné využití tzv. DRP plánů neboli plánů obnovy po havárii . Automatickou instalací je myšleno zejména možné využití instalačních skriptů. Součástí těchto skriptů by měla být jak instalace nástroje PIM/ PAM, tak přidání existujících assetů tak, aby nástroj PIM/ PAM mohl být v případě havárie rychle obnoven, nastaven a použit. Součástí instalačního procesu jsou automatické před a post implementační kontroly včetně automatického hardeningu prostředí. Možnost automatizovaného přidávání nových assetů je vítanou možností zjednodušení provozu a správy prostředí. Zadavatel má zkušenost, že při realizaci DRP je výhodné provést kopii instalačních souborů na místo instalace, aby instalace probíhala lokálně (v případě vážných aktivace DPR plánu může docházet k výpadkům např. komunikačních linek a tím k přerušení instalace, prodlužování doby obnovy a nedodržení stanovených RPO). Lokální kopie má za cíl předejít těmto stavům. Zadavatel dále nerozumí části dotazu „…resp. čím se toho má dosáhnout“ – pokud předchozí informace není dostatečná, žádá Zadavatel dodavatele o bližší upřesnění jeho dotazu.

Dotaz č. 7	Zadání: Konzultační služby Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení zadavatele. Dotaz:

	Splní Uchazeč požadavek, pokud je výrobce schopen poskytovat konzultační služby požadované ve výše uvedeném požadavku, ale nejsou součástí dodávky? Veškeré výše uvedené konzultační služby standardně zvládají partneři jednotlivých výrobců. V případě zájmu Zadavatele je možné využít konzultačních hodin v rámci maintenance řešení, případně si separátně objednat. Pokud si Zadavatel trvá na přesném výše uvedeném znění, směřuje tento požadavek na jednoho výrobce PIM/PAM. Neuvolnění by znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 7	Ano, pokud dodavatel doloží, že výrobce řešení je schopen konzultační služby dle požadavku poskytnout, Zadavatel bude považovat požadavek za splněný. Zadavatel nedisponuje dostatečnou znalostí daného produktů PIM/ PAM a není schopen interně ověřit kvalitu dodaného díla. Cílem požadavku je získat ujištění, že v případě potřeby Zadavatele bude možné provést ověření kvality implementace ze strany výrobce nebo jím certifikovaného partnera, který je oprávněn provádět audit kvality, a to buď jako celku nebo její části, a to z pohledu úplnosti, dodržení výrobcem stanovených postupů a best-practice, optimálnosti prodaných licencí, bezpečnosti, sizingu a/ nebo integrace na okolní systémy. Vlastní konzultace není předmětem veřejné zakázky.

Dotaz č. 8	Zadání: Implementační služby Výrobce poskytuje vlastní implementační služby v rámci projektů implementace PAM řešení na lokálním trhu. Dotaz: Splní Uchazeč požadavek, pokud je výrobce schopen poskytovat implementační služby požadované ve výše uvedeném požadavku, ale nejsou součástí dodávky? Veškeré výše uvedené implementační služby standardně zvládají partneři jednotlivých výrobců. V případě zájmu Zadavatele je možné využít implementačních hodin, které by si separátně objednat. Pokud si Zadavatel trvá na přesném výše uvedeném znění, směřuje tento požadavek na jednoho výrobce PIM/PAM. Neuvolnění by znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 8	Ano, pokud dodavatel doloží, že výrobce řešení je schopen konzultační služby dle požadavku poskytnout, Zadavatel bude považovat požadavek za splněný. Zadavatel nedisponuje dostatečnou znalostí daného produktů PIM/ PAM a není schopen interně ověřit kvalitu dodaného díla. Cílem požadavku je získat ujištění, že v případě potřeby Zadavatele bude možné provést ověření kvality implementace ze strany výrobce nebo jím certifikovaným partnerem, který je oprávněn provádět audit kvality, a to buď jako celku nebo její části, a to z pohledu úplnosti, dodržení výrobcem stanovených postupů a best-practice, optimálnosti prodaných licencí, bezpečnosti, sizingu a/ nebo integrace na okolní systémy. Vlastní konzultace není předmětem veřejné zakázky.

Dotaz č. 9	Zadání: PAS Assessment tool Výrobce zákazníkům poskytuje nástroj, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí zadavatele, vzhledem k předem definovaným rizikům. Celý koncept PAS Assessment nástroje umožňuje zákazníkům postupné povyšování bezpečnosti a případné porovnání aktuálního stavu s anonymním údaji tisíců zákazníků po celém světě. Dotaz: Tento princip kopíruje způsob jednoho konkrétního výrobce řešení PIM/PAM. Je možné požadavek zmírnit, upravit či vypustit tak, aby byla možná účast ve veřejné soutěži pro více výrobců řešení PIM/PAM? V případě zadání požadavku do internetového vyhledávače typu google lze vidět jediného výrobce splňujícího tento požadavek. Neuvolnění by znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení

	na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 9	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Cílem požadavku je zajistit soulad s vyhláškou o kybernetické bezpečnosti č. 82/2018 Sb. (dále v tomto vysvětlení jen „VoKB“), která jasně požaduje zajištění procesu řízení zranitelností. Vzhledem ke specifické oblasti PIM/ PAM nedisponuje Zadavatel interním nástrojem pro tuto oblast a dle názoru Zadavatele by bez odpovídajícího nástroje nebyl schopen efektivně plnit požadavky VoKB. Zadavatel proto požaduje, aby součástí dodávky byla též metodika, dle které může Zadavatel na pravidelné bázi ověřit způsob používání nástroje vzhledem k privilegovaným účtům a best-practice výrobce. Cílem druhé části požadavku na porovnání stavu bezpečnosti s jinými společnostmi je snaha odhadnout a optimálně řídit bezpečnostní rizika, získat informace pro rozhodování na taktické a strategické úrovni organizace. Porovnání s dosaženou úrovní bezpečnosti je klíčový vstup pro řízení dalších investice do oblasti PIM/ PAM ve společnosti. Dodavatel v dotazu požaduje úpravu zadávací dokumentace způsobem, která znevýhodňuje Zadavatele vzhledem k plnění zákonných požadavků a upřednostňuje jedno řešení (pravděpodobně takové, které hodlá nabídnout dodavatel), což Zadavatel považuje za nepřípustné.

Dotaz č. 10	Zadání: Druh licence Řešení musí být dimenzované minimálně pro 100 uživatelů při budoucím rozšíření licence. Licence není omezena na počet koncových zařízení nebo řízených účtů. Součástí licence je i řešení redundance všech komponent a taktéž geo-redundance (active-active) s dodatečnou místní redundancí v druhé geolokaci. Dotaz: Zadavatel v ZD uvádí konkrétní požadavky na maximální počty spravovaných systémů. Systémy PIM/PAM mají různé typy licencování. Umožní Zadavatel i licencování na počty systémů, nikoli pouze na počet administrátorů systému? Tento požadavek směřuje na jednoho výrobce PIM/PAM. Neuvolnění by znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 10	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Zadavatel nemá detailní znalost možností licencování jednotlivých výrobců/ dodavatelů. Cílem Zadavatele je v zadávací dokumentaci uvést veškeré jemu známé informace, které by Uchazeč mohl potřebovat pro přípravu nabídky. Zadavatel nijak neomezuje způsob licencování nabízeného řešení a zcela jistě umožní licencování i podle jiných metrik, včetně metriky zmíněné v dotazu dodavatel. Zadavatel však připomíná, že daná metrika nesmí být v rozporu s ostatními požadavky zadávací dokumentace a nesmí vést k nedostatečnému licencování.

Dotaz č. 11	Zadání: Testovací prostředí Licence zároveň pokrývá možnost instalace separátního trvalého testovacího prostředí s plnou funkčností a v plném rozsahu. Pro testovací prostředí není potřebný HW součástí dodávky. Veškeré ostatní SW komponenty musí být součástí nabízeného řešení. Dotaz: Přidání tohoto požadavku směřuje na zvýhodnění jednoho výrobce řešení, který testovací prostředí nabízí zdarma v rámci dodávky licencí. Aby nedošlo k zásadnímu finančnímu znevýhodnění ostatních výrobců, je možné upravit požadavek alespoň tak, že prostředí nemusí být zcela totožné s plnou funkčností a v plném rozsahu co produkční prostředí, ale bude možné si na tomto prostředí otestovat veškeré funkcionality v omezeném množství, avšak pro test dostačující? Neuvolnění by

	znamenalo diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 11	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Zadavatel upozorňuje, že je provozovatelem kritické infrastruktury státu, a jako takový je povinný zajistit soulad s VoKB. Požadavek zajištění testovacího prostředí je navíc běžným požadavkem všech klíčových IT standardů, včetně norem ISO. Hlavním cílem požadavku je možnost otestování připravovaných změn a jejich „odladění“ před nasazením změnu do produkčního prostředí. Zadavatel požaduje dodání a licenční pokrytí produkčního i testovacího prostředí. Testovací prostředí musí obsahovat všechny komponenty a funkcionality jako produkční prostředí. Zadavatel v obvyklém režimu očekává testování v počtu 5 uživatelů a 30 cílových systémů všech typů.

Dotaz č. 12	Zadání: Detekce útoků na Kerberos zranitelnosti Řešení umožňuje detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash, PAC attack a Golden ticket. Dotaz: Tento požadavek směřuje pouze na jednoho výrobce řešení PIM/PAM. Je možné případně splnit požadavek integrací na třetí systémy, např. SIEM, případně jiné? Pokud nedojde k úpravě či zrušení tohoto požadavku znamenalo by to diskriminaci ostatních výrobců. V minulém výběrovém řízení na stejný předmět dodávky se tento požadavek neobjevoval.
Odpověď č. 12	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Dle informací Zadavatele podporuje tuto funkcionalitu vícero řešení a požadavku je též možno dosáhnout kombinací vícero produktů. Zadavatel nijak neomezuje možná řešení a zcela určitě připouští možnost splnění požadavku formou integrace nástroje PIM/ PAM s nástrojem SIEM. Současně však dodává, že nástroj SIEM musí být kompletně dodán a integrován v rámci této dodávky, včetně všech potřebných licencí a integrace nástroje SIEM nesmí být v rozporu s dalšími požadavky zadávací dokumentace.

Dotaz č. 13	K nejasným požadavkům na licencování nástroje Zadavatel v bodě 1.5.2 178_20_ZD – PIM PAM a v bodě 178-20_ZD_priloha5_tech – Druh licence uvádí požadavky na druh poptávané licence. Dotaz: Chápe účastník správně, že zadavatel i přes jasné počty spravovaných systémů umožňuje licencování pouze na „administrátora“ systému? Pokud tomu tak je, zadavatel by účelově znemožnil některým hlavním výrobcům PAM řešení účast v soutěži a Zadavatel by v konečném důsledku mohl zcela pozbýt šanci na získání cenově efektivních nabídek.
Odpověď č. 13	Zadavatel má z dotazu za to, že dodavatel chápe požadavek zadávací dokumentace nesprávně. Zadavatel nemá detailní znalost možností licencování jednotlivých výrobců/ dodavatelů. Cílem Zadavatele je v zadávací dokumentaci uvést veškeré jemu známé informace, které by dodavatel mohl potřebovat pro přípravu nabídky. Zadavatel nijak neomezuje způsob licencování nabízeného řešení a zcela jistě umožní licencování i podle jiných metrik. Zadavatel však připomíná, že daná metrika nesmí být v rozporu s ostatními požadavky zadávací dokumentace.

Dotaz	K nejasným požadavkům na řízení a správu lokálních administrátorů pro lokální

č. 14	PC (desktopy). Zadavatel v bodě 1.5.2 178_20_ZD – PIM PAM uvádí že „Řízení a správa lokálních administrátorů pro lokální PC (desktopy) koncových uživatelů není v rozsahu tohoto projektu.“ Dále pak Zadavatel v odstavci 178-20_ZD_priloha5_tech – „Zabezpečení koncových bodů“ uvádí požadavky na na správu lokálních administrátorů. Dotaz: Jsou, nebo nejsou tyto požadavky z 178-20_ZD_priloha5_tech – „Zabezpečení koncových bodů“ předmětem jakéhokoliv hodnocení nabídek?
Odpověď č. 14	Zabezpečení koncových bodů není předmětem hodnocení nabídek.

Dotaz č. 15	K nejasnému požadavku na velikost uložiště pro archivaci a souběžných relací Zadavatel v bodě 1.6.1.6 , ZD 178_20_ZD – PIM PAM uvádí požadavky na velikost uložiště pro archivaci a odhad maximálního počtu současně probíhajících relací je – 15. Zadavatel dále uvádí v 178-20_ZD_priloha7_model celkový počet uživatelů systému externích a interních administrátorů a uživatelů na 54. Účastník z dlouholeté zkušenosti na trhu s nástroji pro privilegované účty uvádí, že standardní počet souběžných relací v provozu na jednoho administrátora je mezi 5-15 otevřenými spojeními v jeden moment. To v počtu 54 uživatelů systému udává rozmezí mezi 270-810 spojeními v jeden moment a výrazně nekoresponduje s uvedenými 15 souběžnými spojeními zadavatele. Dotaz: Účastník žádá zadavatele o přepočtení počtu souběžných spojení tak, aby odpovídalo skutečnému stavu. Bez přepočtení reálného stavu souběžných spojení, není účastník schopen adekvátně navrhnout velikost uložiště pro archivaci tak, aby naplnil požadavek z bodu 1.5.7.2 , ZD 178_20_ZD – PIM PAM kdy musí řešení řídit životní cyklus nahrávek na min 18 měsíců. Dále Účastník uvádí, že pokud zadavatel nesprávně uvede počet souběžných relací, bude to mít za následek neadekvátnost podaných nabídek pro naplnění Zadavatelových požadavků na archivaci z bodu 1.5.7.2 a následné výrazné navýšení finančních nákladů s tím spojených.
Odpověď č. 15	Maximální počet současných relací je vztažen k maximálnímu počtu souběžně pracujících uživatelů. Vypsané zadání je platné a odpovídá aktuálnímu stavu prostředí Zadavatele.

Dotaz č. 16	K potřebě licencí třetích stran pro provoz nástroje Některé nástroje pro řízení privilegovaných účtů potřebují pro svůj běžný provoz a umožnění základních funkcionalit systému licence třetích stran. Účastník však nikde v ZD nenašel, zda předmětem poptávky VŘ jsou i tyto licence třetích stran, nutných pro základní provoz systému. Dotaz: Požaduje Zadavatel v rámci nabídek uvést a nacenit i všechny nezbytné licence třetích stran pro základní provoz nabízeného řešení, např. licence MS CAL? Dodavatel pro úplnost uvádí, že bez těchto licencí nebude nástroj funkční a nebude schopný naplnit základní požadavky z 178-20_ZD_priloha5_tech.
Odpověď č. 16	Součástí dodávky a celkové ceny řešení musí být veškeré potřebné licence pro nasazení a provoz serverové části řešení PIM/ PAM včetně (ne však výhradně) licencí operačního systému, databáze, řešení PIM/ PAM, apod. Uživatelské MS CAL licence nejsou předmětem plnění veřejné zakázky.

Dotaz č. 17	K technické specifikaci 178-20_ZD_priloha5_tech 5.1. Požadavek: „Systém poskytuje možnost automaticky vyhodnocovat a označovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Systém zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp.“ Dotaz:

	Je zadavatel ochotný upravit znění požadavku tak, aby řešení nemuselo automaticky vyhodnocovat a označovat nahrávky, případně mohl na tyto podezřelé činnosti alertovat nástroj typu SIEM? Pokud zadavatel bude dále trvat na přesném znění požadavku, jedná se diskriminační kritérium cílené na jednoho výrobce – CyberArk.
Odpověď č. 17	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Zadavatel nijak neomezuje možná řešení a zcela určitě připouští možnost splnění požadavku formou integrace nástroje PIM/ PAM s nástrojem SIEM a připouští možnost, kdy dodané řešení musí být minimálně schopné reportování podezřelých aktivit. Současně však dodává, že nástroj SIEM musí být kompletně dodán a integrován v rámci této dodávky, včetně všech potřebných licencí a integrace nástroje SIEM nesmí být v rozporu s dalšími požadavky zadávací dokumentace.

Dotaz č. 18	K technické specifikaci 178-20_ZD_priloha5_tech 5.2. Požadavek „Řešení nabízí možnost automatického pozastavení, nebo terminace potenciálně nebezpečných relací. Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat – typ události, uživatelé (možnost nastavení výjimke na úrovni skupin v AD) a typ reakce.“ Dotaz: „Umožňuje zadavatel naplnit tento požadavek integrací s nástrojem typu SIEM, který primárně slouží těmto účelům? Pokud zadavatel bude dále trvat na přesném znění požadavku, jedná se diskriminační kritérium cílené na jednoho výrobce – CyberArk.“
Odpověď č. 18	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Cílem požadavku Zadavatele je efektivně vynutit bezpečnostní politiku v prostředí kritické infrastruktury a včasně ošetřit identifikované incidenty. V případě, zjištění kompromitace hesla musí, dle soudu zadavatele, dojít k okamžité změně hesla a ukončení všech session, které kompromitované heslo používají. Pokud se toto nestane, vystavuje se Zadavatel riziku dokončení kybernetického útoku, které může mít za následek ztráty na životech, majetku a/ nebo způsobit závažnou ekologickou havárii. Požadovaná terminace/ pozastavení relace je vždy předmětem konfigurace a ochranné tohoto typu bude vždy realizováno v souladu s mírou daného rizika. Zadavatel připomíná, že očekává, že nasazená pravidla bude možné časově ohraničit např. na dobu mimo pracovní dobu, kde doba reakce na přijatý alert v kombinaci s manuálním zásahem může znamenat významné zvýšení rizika úspěšného dokončení útoku. Zadavatel připomíná, že ochrana zdraví zaměstnanců a občanů, majetku, životního prostředí a zajištění kritické infrastruktury státu jsou hlavní zásady Zadavatele a veškeré požadavky ve zadávacího řízení vždy směřují k zajištění těchto fundamentálních zásad. Zadavatel nijak neomezuje možná řešení požadavku ani způsoby, jakými je dodavatel zajistí a připouští možnost splnění požadavku formou integrace nástroje PIM/ PAM s nástrojem SIEM, avšak dodané řešení musí umožnit automatické pozastavení, nebo terminaci potenciálně nebezpečných relací, jak je stanoveno v původním požadavku. Současně však dodává, že nástroj SIEM musí být kompletně dodán a integrován v rámci této dodávky, včetně všech potřebných licencí a integrace nástroje SIEM nesmí být v rozporu s dalšími požadavky zadávací dokumentace.

Dotaz č. 19	K technické specifikaci 178-20_ZD_priloha5_tech 5.3. Požadavek: „Systém umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření - alerting, změna přihlašovacích údajů, terminace/pozastavení relací.“ Dotaz: Nabízené řešení automaticky detekuje podezřelé chování, ale automaticky již nevynucuje nápravná opatření z důvodu, že tato funkcionalita často vede i k přerušování standardních session a do značné míry omezuje práci administrátorů a navyšuje časovou náročnost jejich práce. Umožňuje zadavatel nabídnout i takové řešení, které automaticky nevynucuje tyto nápravná opatření? Pokud ne, jedná se znovu a diskriminační kritérium cílené na jednoho výrobce –CyberArk.

Odpověď č. 19	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Cílem požadavku Zadavatele je efektivně vynutit bezpečnostní politiku v prostředí kritické infrastruktury a včasně ošetřit identifikované incidenty. V případě, zjištění kompromitace hesla musí, dle soudu zadavatele, dojít k okamžité změně hesla a ukončení všech session, které kompromitované heslo používají. Pokud se toto nestane, vystavuje se Zadavatel riziku dokončení kybernetického útoku, které může mít za následek ztráty na životech, majetku a/ nebo způsobit závažnou ekologickou havárii. Požadovaná terminace/ pozastavení relace je vždy předmětem konfigurace a ochranné tohoto typu bude vždy realizováno v souladu s mírou daného rizika. Zadavatel připomíná, že očekává, že nasazená pravidla bude možné časově ohraničit např. na dobu mimo pracovní dobu, kde doba reakce na přijatý alert v kombinaci s manuálním zásahem může znamenat významné zvýšení rizika úspěšného dokončení útoku. Zadavatel připomíná, že ochrana zdraví zaměstnanců a občanů, majetku, životního prostředí a zajištění kritické infrastruktury státu jsou hlavní zásady Zadavatele a veškeré požadavky ve zadávacím řízení vždy směřují k zajištění těchto fundamentálních zásad. Zadavatel nijak neomezuje možná řešení požadavku ani způsoby, jakými je dodavatel zajistí, avšak dodané řešení musí umožnit automatické pozastavení, nebo terminaci potenciálně nebezpečných relací, jak je stanoveno v původním požadavku. V této fázi hrubého nástinu dodavatele však není možné určit, zda dodavatelem zamýšlené řešení bude dostatečně plnit veškeré požadavky tohoto bodu, jakož i ostatních požadavků zadávací dokumentace. K tomuto účelu nemůže ani vysvětlení zadávací dokumentace sloužit. V principu a v obecné rovině však Zadavatel nevidí důvod dodavatelem popsané řešení odmítat.

Dotaz č. 20	K technické specifikaci 178-20_ZD_priloha5_tech 5.4 Požadavek: „Řešení musí umožňovat bezpečné zálohování dat systému - zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů.“ Dotaz: Může nám zadavatel blíže specifikovat co myslí pod pojmem „Disaster Recovery klíčů“? Každé řešení má odlišný způsob přístupu k zálohovaným datům, všechny by však měly naplňovat požadavky ZoKB, GDRP a ISO 27 001, které jsou pro zadavatele, jako subjekt do nich spadající relevantní.
Odpověď č. 20	Zadavatel pojmem „Disaster Recovery key“ rozumí jedinečné heslo nebo klíč, který je použit pro dešifrování záloh a následnou obnovu systému v případě havárie. Cílem tohoto požadavku je však zajistit zabezpečení záloh pomocí obecného mechanismu, který je dostatečně robustní a bezpečný pro ochranu zálohovaných dat. Dodané řešení musí být v souladu s požadavky zákona o kybernetické bezpečnosti.

Dotaz č. 21	K technické specifikaci 178-20_ZD_priloha5_tech 5.5. Požadavek: „Veškeré komponenty řešení musí umožňovat automatickou instalaci v cloud i on-premise prostředí. Řešení minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci prerequisite, instalaci komponent, hardening a základní konfiguraci. Automatickou instalaci je možné řešit například pomocí Ansible roles.“ Dotaz: Může zadavatel objasnit co konkrétně myslí automatickou instalací a čeho se instalace týká?

Odpověď č. 21	Hlavním cílem tohoto požadavku je zajištění snadného, rychlého a efektivního procesu instalace a nápravy chybových stavů. Zadavatel cílí na maximální automatizaci instalačního procesu, která je nezbytná pro přípravu, testování a případné využití tzv. DRP plánů neboli plánů obnovy po havárii. Automatickou instalací je myšleno zejména možné využití instalačních skriptů. Součástí těchto skriptů by měla být jak instalace nástroje PIM/ PAM, tak přidání existujících assetů tak, aby nástroj PIM/ PAM mohl být v případě havárie rychle obnoven, nastaven a použit. Součástí instalačního procesu jsou automatické před a post implementační kontroly včetně automatického hardeningu prostředí.

Dotaz č. 22	K technické specifikaci 178-20_ZD_priloha5_tech 5.6. Požadavek: „Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení zadavatele.“ Dotaz: Rozumíme správně že zadavatel požaduje v rámci implementačního týmu mít i technického implementátora výrobce? Dále žádáme o vysvětlení podstaty tohoto požadavku? Standardně výrobci mají síť certifikovaných partnerů, která provádí instalace na lokálním trhu. Certifikace poskytuje dostatečné prokázání kvalifikace a znalosti daného technika disponujícím danou certifikací.
Odpověď č. 22	NE, Zadavatel nepožaduje, aby součástí implementačního Dodavatele byl technický implementátor výrobce. Zadavatel nedisponuje dostatečnou znalostí daného produktů PIM/ PAM a není schopen interně ověřit kvalitu dodaného díla. Cílem požadavku je získat ujištění, že v případě potřeby Zadavatele bude možné provést ověření kvality implementace ze strany výrobce nebo jím certifikovaným partnerem, který je oprávněn provádět audit kvality, a to buď jako celku nebo její části a to z pohledu úplnosti, dodržení výrobcem stanovených postupů a best-practice, optimálnosti prodaných licencí, bezpečnosti, sizingu a/ nebo integrace na okolní systémy. Vlastní konzultace není předmětem veřejné zakázky.

Dotaz č. 23	K technické specifikaci 178-20_ZD_priloha5_tech 5.7. Požadavek „Výrobce poskytuje vlastní implementační služby v rámci projektů implementace PAM řešení na lokálním trhu.“ Dotaz: Mají být tyto implementační služby výrobce součástí implementace projektu, nebo se jedná o obecný požadavek? Může případně zadavatel objasnit podstatu tohoto požadavku?
Odpověď č. 23	Zadavatel nedisponuje dostatečnou znalostí daného produktů PIM/ PAM a není schopen interně ověřit kvalitu dodaného díla. Cílem požadavku je získat ujištění, že v případě potřeby Zadavatele bude možné provést ověření kvality implementace ze strany výrobce nebo jím certifikovaným partnerem, který je oprávněn provádět audit kvality, a to buď jako celku nebo její části a to z pohledu úplnosti, dodržení výrobcem stanovených postupů a best-practice, optimálnosti prodaných licencí, bezpečnosti, sizingu a/ nebo integrace na okolní systémy. Vlastní konzultace není předmětem veřejné zakázky.

Dotaz č. 24	K technické specifikaci 178-20_ZD_priloha5_tech 5.8. Požadavek „Výrobce zákazníkům poskytuje nástroj, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí zadavatele, vzhledem k předem definovaným rizikům. Celý koncept PAS Assessment nástroje

	umožňuje zákazníkům postupné povyšování bezpečnosti a případné porovnání aktuálního stavu s anonynmním údaji tísíců zákazníků po celém světě.“ Dotaz: Jaká je metrika pro naplnění tohoto požadavku zadavatele? Případně je požadavek naplněn, pokud zadavatel dostane přístup k anonymním informacím údajům o řešení v rámci knowledge base výrobce?
Odpověď č. 24	Cílem požadavku je zajistit soulad s VoKB, která jasně požaduje zajištění procesu řízení zranitelností. Vzhledem ke specifické oblasti PIM/ PAM nedisponuje Zadavatel interním nástrojem pro tuto oblast a dle názoru Zadavatele by bez odpovídajícího nástroje nebyl schopen efektivně plnit požadavky VoKB. Zadavatel proto požaduje, aby součástí dodávky byla též metodika, dle které může Zadavatel na pravidelné bázi ověřit způsob používání nástroje vzhledem k privilegovaným účtům a best-practice výrobce. Cílem druhé části požadavku na porovnání stavu bezpečnosti s jinými společnostmi je snaha odhadnout a optimálně řídit bezpečnostní rizika, získat informace pro rozhodování na taktické a strategické úrovni organizace. Porovnání s dosaženou úrovní bezpečnosti je klíčový vstup pro řízení dalších investice do oblasti PIM/ PAM ve společnosti. Zadavatel jako řešení přidělení přístupu do znalostní databáze/ Knowledge base výrobce v zásadě a v obecné rovině neodmítá, avšak v této fázi nelze rozhodnout, zda dodavatelem zamýšlené řešení bude dostatečné pro splnění všech podmínek zadávací dokumentace. K tomuto účelu nemůže ani vysvětlení zadávací dokumentace sloužit.

Dotaz č. 25	K technické specifikaci 178-20_ZD_priloha5_tech 5.9. Požadavek „Licence zároveň pokrývá možnost instalace separátního trvalého testovacího prostředí s plnou funkčností a v plném rozsahu. Pro testovací prostředí není potřebný HW součástí dodávky. Veškeré ostatní SW komponenty musí být součástí nabízeného řešení.“ Dotaz: Může zadavatel blíže specifikovat jak vypadá jeho testovací prostředí tak, aby bylo možné jej adekvátně zalicencovat a tento požadavek byl naplněn? Tzn. min: počet koncových aktiv testovacího prostředí, výčet všech typů aktiv v testovacím prostředí, počet uživatelů, specifikace HW testovacího prostředí, síťová prostupnost testovacího prostředí na okolní systémy, případně další relevantní informace a způsobu užívání testovacího prostředí.
Odpověď č. 25	Zadavatel upozorňuje, že je provozovatelem kritické infrastruktury státu, a jako takový je povinný zajistit soulad vyhláškou o kybernetické bezpečnosti č. 82/2018 Sb. Požadavek zajištění testovacího prostředí je navíc běžným požadavkem všech klíčových IT standardů, včetně norem ISO. Hlavním cílem požadavku je možnost otestování připravovaných změn a jejich „odladění“ před nasazením změnu do produkčního prostředí. Zadavatel požaduje dodání a licenční pokrytí produkčního i testovacího prostředí. Testovací prostředí musí obsahovat všechny komponenty a funkcionality jako produkční prostředí. Zadavatel v obvyklém režimu očekává testování v počtu 5 uživatelů a 30 cílových systémů všech typů.

Dotaz č. 26	K technické specifikaci 178-20_ZD_priloha5_tech 5.10. Požadavek: „Řešení umožňuje detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash, PAC attack a Golden ticket.“ Dotaz: Umožňuje zadavatel naplnění tohoto požadavku integrací s nástrojem typu SIEM? Pokud zadavatel neumožní naplnění zmíněného požadavku integrací, jedná se znovu o diskriminační kritérium cílené na jednu technologii – CyberArk.

Odpověď č. 26	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Dle informací Zadavatele podporuje tuto funkcionalitu vícero řešení a požadavku je též možno dosáhnout kombinací vícero produktů. Zadavatel nijak neomezuje možná řešení a zcela určitě připouští možnost splnění požadavku formou integrace nástroje PIM/ PAM s nástrojem SIEM. Současně však dodává, že nástroj SIEM musí být kompletně dodán a integrován v rámci této dodávky, včetně všech potřebných licencí a integrace nástroje SIEM nesmí být v rozporu s dalšími požadavky zadávací dokumentace.

Dotaz č. 27	Jak detailní je očekáváný audit Remote desktop relací? Očekává se nahrání videosekvence, nebo i záznam stisknutých kláves, otevření oken či jiných aktivit administrátora v textové formě? Je možné k auditu těchto aktivit použít předinstalovaného agenta?
Odpověď č. 27	Zadavatel očekává jak nahrání videosekvencí, tak k tomu odpovídající záznamy stisknutých kláves, zadaných příkazů, otevřených oken. Zadavatel dále očekává, že textový záznam bude časově odpovídat uložené videosekvenci, půjde v něm fultextově vyhledávat a videosekvenci půjde posunovat a vyhledávat v ní pomocí indexovaných textových záznamů. Na některá velmi citlivá zařízení nebude možné agent instalovat, a tak je nezbytné, aby vše mohlo být zaznamenáno a indexováno i bez použití agenta. Agent na endpoint zařízení tedy není přípustný.

Dotaz č. 28	Očekává se možnost využití běžných nástrojů systémových administrátorů, pro přístup ke koncovým systémům, jakými jsou např. Putty (pro přístup k příkazové řádce) a WinSCP (pro přenos souborů) přímo ze stanice administrátora? Očekává se auditování těchto spojení bez použití agenta na cílovém zařízení, a to jak ve vizuální, tak v textové formě?
Odpověď č. 28	Zadavatel požaduje možnost využití běžných nástrojů pro přístup a administraci jako Putty, WinSCP, popř. dalších (RDP, SQL Management studio apod.). Zadavatel požaduje řešení bez-agenta na zdrojovém i cílovém zařízení.

Dotaz č. 29	Zadavatel požaduje, aby řešení umožňovalo detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash, PAC attack a Golden ticket. Tato funkcionalita je obsažena pouze u jednoho výrobce řešení PAM. Ostatní výrobci tuto oblast řeší integrací na systémy, k tomu určené. Je možné splnit požadavek integrací na nástroj SIEM?
Odpověď č. 29	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Dle informací Zadavatele podporuje tuto funkcionalitu vícero řešení a požadavku je též možno dosáhnout kombinací vícero produktů. Zadavatel nijak neomezuje možná řešení a zcela určitě připouští možnost splnění požadavku formou integrace nástroje PIM/ PAM s nástrojem SIEM. Současně však dodává, že nástroj SIEM musí být kompletně dodán a integrován v rámci této dodávky, včetně všech potřebných licencí a integrace nástroje SIEM nesmí být v rozporu s dalšími požadavky zadávací dokumentace.

Dotaz č. 30	Zaavatel v technické specifikaci požaduje možnost instalace separátního trvalého testovacího prostředí s plnou funkčností a v plném rozsahu. Testovací prostředí jako součást řešení je vlastností jednoho výrobce řešení PAM. Ostatní výrobci musejí tuto oblast řešit dodávkou identického řešení, jako je produkční, což značně navyšuje cenu. Trvá Zadavatel na tomto požadavku? Je případně možné detailněji vyspecifikovat požadavky na testovací prostředí?

Odpověď č. 30	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Zadavatel upozorňuje, že je provozovatelem kritické infrastruktury státu, a jako takový je povinný zajistit soulad vyhláškou o kybernetické bezpečnosti č. 82/2018 Sb. Požadavek zajištění testovacího prostředí je navíc běžným požadavkem všech klíčových IT standardů, včetně norem ISO. Hlavním cílem požadavku je možnost otestování připravovaných změn a jejich „odladění“ před nasazením změnu do produkčního prostředí. Zadavatel požaduje dodání a licenční pokrytí produkčního i testovacího prostředí. Testovací prostředí musí obsahovat všechny komponenty a funkcionality jako produkční prostředí. Zadavatel v obvyklém režimu očekává testování v počtu 5 uživatelů a 30 cílových systémů všech typů.

Dotaz č. 31	Zadavatel požaduje, aby výrobce zákazníkům poskytuje nástroj, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí zadavatele, vzhledem k předem definovaným rizikům. Celý koncept PAS Assessment nástroje umožňuje zákazníkům postupné povyšování bezpečnosti a případné porovnání aktuálního stavu s anonymními údaji tisíců zákazníků po celém světě. Tento požadavek směřuje na jednoho výrobce PAM řešení. Je pro splnění dostačující zpřístupnění anonymních informací ve znalostní bázi výrobce?
Odpověď č. 31	Zadavatel jako řešení přidělení přístupu do znalostní databáze/ Knowledge base výrobce v zásadě a v obecné rovině neodmítá, avšak v této fázi nelze rozhodnout, zda Uchazečem zamýšlené řešení bude dostatečné pro splnění všech podmínek zadávací dokumentace. K tomuto účelu nemůže ani vysvětlení zadávací dokumentace sloužit.

Dotaz č. 32	Zadavatel požaduje, aby systém poskytoval možnost automaticky vyhodnocovat a označovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Tento požadavek takto splňuje pouze jeden výrobce PAM. Je možné splnit požadavek tím, že systém bude alertovat nástroji SIEM, kde bude moci dohledat potencionálně nebezpečné činnosti?
Odpověď č. 32	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Zadavatel nijak neomezuje možná řešení a zcela určitě připouští možnost splnění požadavku formou integrace nástroje PIM/ PAM s nástrojem SIEM a připouští možnost, kdy dodané řešení musí být minimálně schopné reportování podezřelých aktivit. Současně však dodává, že nástroj SIEM musí být kompletně dodán a integrován v rámci této dodávky, včetně všech potřebných licencí a integrace nástroje SIEM nesmí být v rozporu s dalšími požadavky zadávací dokumentace.

Dotaz č. 33	Zadavatel požaduje, aby výrobce řešení PAM poskytoval vlastní konzultační služby v rámci projektů implementace PAM řešení. V rámci služeb mají být poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení zadavatele. Proč jsou tyto činnosti možné plnit pouze výrobcem? Z tohoto důvodu si výrobci vytváření partnerskou síť, která se o tyto služby stará. Tato formulace směřuje na jednoho výrobce PAM na českém trhu a diskriminuje ostatní, celosvětové výrobce. Je možné upravit požadavek tak, aby byl splněn, kdyby tyto služby poskytnul výrobce řešení či Dodavatel?
Odpověď č. 33	Zadavatel nedisponuje dostatečnou znalostí daného produktů PIM/ PAM a není schopen interně ověřit kvalitu dodaného díla. Cílem požadavku je získat ujištění, že v případě potřeby Zadavatele bude možné provést ověření kvality implementace ze strany výrobce nebo jím certifikovaným partnerem, který je oprávněn provádět audit kvality, a to buď jako celku nebo její části, a to z pohledu úplnosti, dodržení výrobcem stanovených postupů a best-practice, optimálnosti prodaných licencí, bezpečnosti, sizingu a/ nebo integrace na okolní systémy.

	Vlastní konzultace není předmětem veřejné zakázky.

Dotaz č. 34	Zadavatel požaduje, aby zálohy byly šifrované a přístup k zálohovaným datům byl umožněn pouze pomocí zabezpečených Disaster Recovery klíčů. Pojem Disaster Recovery klíče, je pojem používaný jedním výrobcem řešení. Splní Uchazeč požadavek zadáváním hesla?
Odpověď č. 34	Zadavatel pojmem „Disaster Recovery key“ rozumí jedinečné heslo nebo klíč, který je použit pro dešifrování záloh a následnou obnovu systému v případě havárie. Cílem tohoto požadavku je však zajistit zabezpečení záloh pomocí obecného mechanismu, který je dostatečně robustní a bezpečný pro ochranu zálohovaných dat.

Dotaz č. 35	Požaduje Zadavatel, aby uchazeč nacenil i licence typu Microsoft CAL, pokud jsou pro fungování systému PAM důležité, či je Zadavatel dá k dispozici?
Odpověď č. 35	Součástí dodávky a celkové ceny řešení musí být veškeré potřebné licence pro nasazení a provoz serverové části řešení PIM/ PAM včetně (ne však výhradně) licencí operačního systému, databáze, řešení PIM/ PAM, apod. Uživatelské MS CAL licence nejsou předmětem plnění veřejné zakázky.

Dotaz č. 36	Zadavatel požaduje, aby systém umožňoval export auditních záznamů pro nástroje typu Crystal reports atp. Z jakého důvodu Zadavatel požaduje takovýto požadavek? Takovýmto přístupem by docházelo ke snížení bezpečnosti, jelikož citlivá data, která mají být pouze v systému PIM/PAM budou exportována do systémů, které nejsou pro jejich správu určeny. Jakým způsobem by Zadavatel zamezil úniku těchto exportů, dat? Je tento požadavek splněn, pokud veškeré tyto auditní záznamy jsou zpracovávány v systému PIM/PAM, kde je možné s nimi dále pracovat? Tento požadavek pro export směřuje na jednoho výrobce řešení, který tuto oblast má řešenou tímto způsobem.
Odpověď č. 36	Cílem požadavku je umožnit práci s auditním záznamem mimo prostředí PIM/ PAM a to zejména v případech nutné externí forenzní analýzy/ šetření, vyšetřování incidentů a nestandardních činností v rámci společnosti, včetně možnosti využití pokročilých analytických metod softwarů třetích stran, které již Zadavatel vlastní. Zadavatel je toho názoru, že v případě auditních záznamů je kritická zejména jejich integrita a nepopiratelnost, která se exportem jejich kopie nijak nesnižuje. Dodavatel ve svém dotazu naznačuje, že řešení PIM/ PAM je jediným správným nástrojem pro správu auditních záznamů, což dle názoru Zadavatele naopak limituje ostatní řešení, které by pro správu auditních záznamů mohli použít jiné systémy. Dále, Zadavatel je toho názoru, že v oblasti IT je běžná analýza logů mimo řešení PIM/ PAM, jako jsou řešení typu SIEM nebo BI řešení, která umožňují využití tzv. machine-learning algoritmů nebo artificial inteligence, a významným způsobem tak zjednodušují jejich analýzu a korelaci. Zadavatel dále považuje za běžnou praxi, že společnost pracuje s citlivými údaji (údaji kde je kritická důvěrnost dat) ve formě elektronických a tištěných dokumentů, tedy mimo nástroj PIM/ PAM a při dodržení odpovídajících požadavků na zabezpečení, nepovažuje export auditních záznamů z nástroje PIM/ PAM za nijak problematický. Způsob, jakým Zadavatel schrání data společnosti mimo řešení PIM/ PAM není předmětem této veřejné zakázky.

Dotaz č. 37	Jako součást dodávky uvažujeme licence Microsoft Windows Server v minimální verzi 2016. Z tohoto důvodu vzniká požadavek na pokrytí všech uživatelů, kteří budou systém používat také Microsoft Windows Server Client Access License (CAL) o minimální verzi 2016. Přípustné jsou tedy verze 2016 a 2019. Protože se jedná dnes o běžně provozované operační systémy, lze předpokládat, že tyto licence již zadavatel vlastní a z licenčních

	důvodů jsou pokryti všichni uživatelé, nebo zařízení jakkoli využívající IT infrastrukturu provozovanou na technologii Microsoft Windows Server. V tomto případě není nutné Microsoft Windows Server CAL licence nakupovat. Vlastní zadavatel Microsoft Windows Server Client Access License ve verzi 2016 nebo 2019 v počtu pokrývajícím uvažované počty uživatelů?
Odpověď č. 37	Zadavatel preferuje Microsoft Windows Server ve verzi 2019, verze 2016 je přípustná. Uživatelské MS CAL licence nejsou předmětem dodávky.

Zadavatel s ohledem na povahu dotazů k zadávací dokumentaci a skutečnost, že obdržel druhou, třetí a čtvrtou žádost o vysvětlení ZD dne 15. 10. 2020 a pátou žádost dne 22. 10. 2020 a na tyty žádosti podal vysvětlení až v den uveřejnění tohoto vysvětlení, tedy 18 pracovních dnů poté, **prodlužuje v souladu s § 98 odst. 4 zákona lhůtu pro podání nabídek do 4. 12. 2020 do 10:00 hodin.**

V Praze

Milan Trnka

Digitálně podepsal Milan Trnka
Datum: 2020.11.11 10:07:40 +01'00'

ČEPRO, a.s.
oddělení centrálního nákupu