1 TECHNICKÁ SPECIFIKACE

Cílem zakázky je navrhnout a realizovat zvýšení zabezpečení dat a komunikace uvnitř Policie ČR (dále též PČR) jako veřejné organizace a to v souladu se strategickými záměry Policie ČR a s ohledem na požadavky Zákona o kybernetické bezpečnosti.

Zakázka reaguje na rostoucí počet uživatelů systému a rostoucí objemy zpracovávaných dat, zvýšení datových toků obecně a to zároveň s důležitostí informací, které jsou v datech obsaženy. Vzniká tak i větší riziko bezpečnostních incidentů současně se vzrůstající složitostí identifikace bezpečnostní události.

Zakázka je rozdělena na dvě samostatné části:

část - A řeší vybudování automatizovaného monitorovacího systému pro sběr, korelaci a vyhodnocování bezpečnostních událostí a incidentů v prostředí ICT PČR a to v souladu s požadavky Zákona o kybernetické bezpečnosti a platných vyhlášek, posílení databázové vrstvy a dodávku související HW technologie;

část - B pak řeší vybudování centralizovaného úložiště elektronických dat z trestních řízení s jednotnou správou způsobem s respektováním existující SAN infrastruktury a diskových polí tak, aby došlo k maximálně efektivnímu využití prostředků

Část A

Systém dohledu a analýzy bezpečnostních událostí

Souhrn

Předmětem je vybudování systému pro sběr dat, která se dotýkají IT bezpečnosti, jako základního prvku on-line monitoringu IT bezpečnosti. Architektura systému představuje centralizované vyhodnocení a korelaci bezpečnostních událostí na úrovni Policejního prezidia s tím, že v lokalitě každého krajského ředitelství PČR je instalován prvek pro sběr dat a jejich základní vyhodnocení. Takováto architektura umožňuje nejen okamžité vyhodnocení kritických incidentů v lokalitě krajského ředitelství, ale zároveň korelaci a vyhodnocení událostí přes plochu celé PČR v rámci centrální aplikace v prostředí Policejního prezidia.

Dále je požadována kategorizace a normalizace přijímaných zpráv s následným vyhodnocením korelačními pravidly. Součástí musí být také reporting, incident management a využití dat ostatních informačních systémů, např. Identity Management.

Předmětem je vybudování systému pro sběr dat, která se dotýkají IT bezpečnosti, jako základního prvku on-line monitoringu IT bezpečnosti. Dále je požadována kategorizace a normalizace přijímaných zpráv s následným vyhodnocením korelačními pravidly. Součástí musí být také reporting, incident management a využití dat ostatních informačních systémů, např. Identity Management. Nasazení systému monitoringu je z pohledu Zadavatele požadovaným a nezbytným předpokladem pro zavádění dalších systémů, jako např. elektronický archiv.
Systém monitoringu musí poskytovat následující funkcionality:

- sběr dat ze síťových prvků, operačních systémů a aplikací,
- sběr dat z nestandardních prvků a aplikací,

- normalizace a kategorizace dat,
- zabezpečené centrální uložiště dat a jejich rychlé prohledávání,
- korelace a vyhodnocení dat, pravidelný reporting,
- online dohled nad stavem IT bezpečnosti,
- implementace monitoringu v souladu se standardy a legislativními požadavky,
- reaktivní opatření na události a incidenty.

Systém se bude sestávat z jednak ze samotného jádra sytému představující SW část zajišťující sběr, vyhodnocování a korelaci zaznamenaných událostí, ale dále bude obsahovat i nezbytnou HW infrastrukturu, která bude k provozu tohoto systému nezbytná.

Požadavky na realizaci

Cílem projektu je vybudovat systém bezpečnostního monitoringu – SIEM (Security Information and Event Management), který zajistí sběr událostí relevantních pro bezpečnost ze systémů krajských ředitelství Zadavatele a dvou hlavních datových center, jejich bezpečné uložení a centrální analýzu a korelaci záznamů tak, aby bylo možné efektivně vyhledat události ohrožující bezpečnost Zadavatele. Cílem je výběr, návrh a implementace řešení, které zajistí splnění:

- Zpětné dohledání činnosti v systému
  Systém bezpečnostního monitoringu bude zaznamenávat události, které by mohly narušit nebo ohrozit bezpečnost informačních systémů a chránit tyto záznamy před neautorizovaným přístupem, modifikací nebo zničením. Činnosti provedené v systému musí být zpětně rekonstruovatelné.
- Detekce probíhajícího útoku
  Automatizace kontrol nad auditními záznamy musí zefektivnit kontrolní činnosti a dohled nad bezpečnostní situací v systémech a včas informovat o potenciálních rizicích. Systém pro monitoring musí zefektivnit kontrolní činnost a včas přijmout preventivní opatření na straně Zadavatele a tím minimalizovat ztráty z případných bezpečnostních incidentů a zajistit podklady pro šetření bezpečnostních incidentů.
- Preventivní působení
  Funkční kontrolní systém bude nástrojem zefektivňujícím účinnost implementovaných bezpečnostních opatření v tom smyslu, že bude chránit investice do těchto opatření, ale také preventivně působit na potenciální útočníky.
  V případě výskytu podezřelé události bude nezbytné událost prošetřit, zdokumentovat a poskytnout účastníkům zpětnou vazbu, pro tento účel je cílem implementovat workflow pro rychlé vyšetření událostí umožňující koordinaci a komunikaci s dotčenými pracovníky Zadavatele a jeho dodavatelů.

Požadované kroky nasazení systému

- **Analýza prostředí a interoperability interních systémů a systémů bezpečnostního monitoringu**
  V tomto kroku je po Dodavateli systému požadováno provést analýzu prostředí Zadavatele a vytvoří její datový model, na základě kterého bude následně navržen způsob monitoringu – zejména OS, databázových systémů, vybraných aplikací, síťových prvků a dalších bezpečnostních technologií.
  Současně Dodavatel provede analýzu spolupráce interních systémů a nově navrhovaného systému bezpečnostního monitoringu typu SIEM. Tato analýza musí být zaměřena především na vliv systému bezpečnostního monitoringu na zvýšení zátěže monitorovacích systémů, serverů a velikost diskového prostoru a zmapování nezbytných vazeb budovaného systému.
  Analýza musí obsahovat minimálně tyto činnosti:

- Identifikace a popis komponent a zařízení prostředí zadavatele, které aktuálně vytváří, případně by mohly vytvářet (např. po vhodné rekonfiguraci) záznamy o bezpečnostních událostech
- Identifikace bezpečnostních událostí, ke kterým může docházet
- Identifikace procesů a technického řešení evidence, vyhodnocování a řešení událostí
- Možnosti napojení SIEM na stávající monitorovací systémy
- Upřesnění parametrů požadovaných vlastností SIEM z hlediska možností sběru a ukládání událostí, jejich vyhodnocování a řešení incidentů
- Odhad datových toků EPS a objemu dat GB/den

V průběhu této fáze budou také s pomocí vlastníků a správců (předem definovanými osobami Zadavatele) monitorovacích systémů, databází, aplikací, síťových prvků apod. zrevidovány jejich požadavky na upřesnění rozsahu monitorovaných událostí systému SIEM.

- **Realizační projekt**
  Na základě datového modelu a analýzy interoperability z předchozí fáze bude Dodavatelem zpracován detailní návrh technického řešení bezpečnostního monitoringu, respektující všechny požadavky na zabezpečení, funkčnost a interoperabilitu systému dle pravidel a požadavků Zadavatele.
  Detailní návrh technického řešení bude obsahovat minimálně:
  - Návrh architektury systému bezpečnostního monitoringu, včetně soupisu potřebného HW a modulů pro provoz SIEM a umístění jednotlivých komponent v síti
  - Soupis nároků na jednotlivé monitorované systémy a prostředky, na kterých systém poběží
  - Soupis nároků na správce jednotlivých serverů, databází, síťových prvků apod. a nároků na správce systému bezpečnostního monitoringu
  - Návrh rozsahu sledování jednotlivých typů logů
  - Vytvoření návrhu rozdělení událostí z hlediska jejich bezpečnostní závažnosti a následného pořadí implementace

  Detailní návrh technického řešení bude upřesňovat požadavky v těchto oblastech:
  - Zdroje logů
    - Požadované zdroje logů síťové vrstvy - síťové prvky (switche, routery, firewall, IDS, IPS...)
    - Požadované zdroje logů vrstvy operačních systémů - OS jednotlivých serverů (Windows, Linux, Unix…)
    - Požadované zdroje logů databázových systémů - databázové servery
    - Požadované zdroje logů aplikační vrstvy - aplikační a webové servery (web aplikační servery, autentizační servery, docházkový systém, identity management, správa přístupových práv, případně další zdroje)
  - Správa logů
    - Možnosti filtrace jednotlivých log záznamů
    - Doporučení parametrů pro archivaci jednotlivých log záznamů
    - Popíše možnosti vyhledávání konkrétních log záznamů
    - Doporučí požadavky pro fyzické ukládaní a zabezpečení dat
    - Doporučí požadavky pro zálohování systémů
    - Identifikuje oblasti s nízkým nebo žádným bezpečnostním logováním a doporučí optimální metodu nasazení logování
  - Zpracování logů
    - Pravidla pro vzájemnou korelaci jednotlivých log záznamů
    - Závažnost události (severity)

- Urgentnost události (priority)
- Návrh způsobu detekce konkrétních typů bezpečnostních incidentů (např. útok na web aplikační server,…) a návrh opatření
- Návrh pravidel pro archivaci a zálohování bezpečnostních incidentů
- Vyhledávaní konkrétních log záznamů a bezpečnostních incidentů

o Návrh testů systému, které budou provedeny po implementace systému

- **Dodávka, nasazení a konfigurace**
  Dodávka, instalace a konfigurace programového vybavení bezpečnostního monitoringu
  V tomto kroku bude rovněž dodán a instalován HW a SW pro implementaci řešení bezpečnostního monitoringu, jehož parametry vyplývají z detailního technického návrhu řešení.

- **Integrace monitoringu do prostředí ICT PČR**
  Bude provedena úprava nastavení jednotlivých komponent infrastruktury Zadavatele včetně konfigurace SIEM řešení a jeho požadovaných vlastností určených detailním návrhem technického řešení a požadavky na vlastnosti řešení.

- **Návrh a provedení testů**
  Po implementaci SIEM řešení a jeho nastavení budou provedeny testy systému z hlediska jeho bezpečnosti, efektivnosti získávání informací, uživatelské náročnosti, spolupráce s dalšími systémy a kvality výstupů.
  Na základě výsledků testů bude řešení nastaveno do finální požadované podoby.

- **Technická a provozní dokumentace a zaškolení**
  Nastavení řešení bude detailně zdokumentováno ve formě dokumentu o nastavení systému bezpečnostního monitoringu. V dokumentu bude dále specifikována správa a údržba systému, která musí ve finální podobě poskytovat dostatek informací o systému, jeho nastavení, zdrojích informací a dále o způsobu, jak systém rozšířit o další požadavky na vyhodnocování a napojené systémy, databáze a aplikace. Dokument bude také popisovat architekturu řešení (i graficky), tok informací systémem, místo a formát jejich uložení, jakož i možné způsoby jejich použití/zpracování. Dokumentace musí mj. obsahovat:
  - Popis fungování a užívání systému (administrátorská + uživatelská příručka)
  - Popis procesu pro vyhodnocování bezpečnostních událostí v rámci implementovaného řešení
  - Požadavky na role a znalosti pro práci se systémem
  - Způsob zajištění podpory při vyhodnocování událostí a podpora provozování systému

  Správci systému budou zaškoleni pro správu a užívání systému SIEM v rozsahu min. 1 pracovní den.

Detailní požadavky na funkcionalitu

Č.	Popis požadavku
1	Data uložená a udržovaná systémem SIEM musí být provozována a udržována v souladu s právními předpisy.
2	Systém SIEM musí dovolovat užití různými uživateli v různých rolích.
3	Řešení SIEM musí být schopné poskytnout uživatelské funkce a uživatelské rozhraní založené na rolích uživatelů. Typy rolí a jim definovaná práva by měly dodržovat

Č.	Popis požadavku
	následující exkluzivní rozsahy: • **Rozsah 1** – Správa systému SIEM, definice bezpečnostní politiky, definice kolekcí, korelace a pravidla vyhodnocování, správa uživatel • **Rozsah 2** – Vyšetřování podezřelých událostí v rámci celého řešení SIEM, optimalizace korelací a pravidel vyhodnocování • **Rozsah 3** – Přezkoumání celkového nastavení SIEM pomocí read-only přístupu • **Rozsah 4** – Zobrazování příchozích událostí (v původní formě - raw) a upozornění podle definovaných pravidel, tj. lokalita původu, uživatelská skupina, role atd. • **Rozsah 5** – Zobrazování předdefinovaných hlášení podle upozornění a jím definovaných pravidel, tj. lokalita původu, uživatelská skupina, role atd. SIEM by měl být schopný poskytnout možnost definovat pravidla přístupu ke konkrétním datům z různých lokalit/místa, např. název lokality, rozsah IP adres, původ dat na základě zdroje (agent, kolektor/sběrač).
4	Systém SIEM by měl být umožňovat napojení na centrální databázi uživatelů a měl by být schopen používat detaily uživatelských účtů ke sledování uživatelů napříč různými prostředími/účty.
5	Systém SIEM by měl podporovat různé metody identifikace a autentizace, např. certifikáty x. 509, MSAD (Kerberos + SPNEGO), přihlašovací jméno a heslo je přenášeno pomocí zabezpečeného kanálu.
6	Systém SIEM by měl poskytovat sběr událostí a jejich analýzu, včetně funkce automatické normalizace, agregace a korelace. Systém by měl sbírat provozní logy a umožňovat korelaci provozních upozornění s bezpečnostními výstrahami. Systém SIEM by měl být schopen získávat události z různých aplikací a systémů, včetně nativní podpory minimálně těchto zařízení: • Checkpoint security suite • Cisco Secure Access Control System • Cisco Identity Services Engine • Cisco routery a switche s funkcionalitou NAC • Cisco FWSM a ASA s FW a IPSec funkcionalitou • Cisco IronPort • Juniper Networks SSL VPN • F5 BIG-IP • IBM ISS Product suite • Infoblox NIOS • RDBM systémy – hlavně MS SQL, Oracle, DB2, MySql, GTM,Sybase, Informix • Windows a Unix/Linux operační systémy, • WEB servery and J2EE aplikační servery • WEB Proxy • SYSLOG servery • NetCool • Qualys Guard • MS Exchange • TAMEB • ITIM • CA Control Minder • TeamQuest • LifeRay Portal
7	Systém SIEM by měl podporovat pořizování událostí bez pomoci agenta minimálně u následujících protokolů:

Č.	Popis požadavku
	• SYSLOG • ODBC • JDBC • OPSec LEA • SNMP • WMI • File/Directory přes SHARE • HTTP/HTTPS
8	V případě, že systém SIEM podporuje sběr událostí pomocí agenta instalovaného na vzdáleném systému nebo aplikaci, musí být splněny následující požadavky: • agent zanechává jen minimální stopu v systému, ve kterém běží, • agent nezvyšuje bezpečnostní stupeň ohrožení systému či aplikace, • agent komunikuje se systémem pro správu zabezpečeným/šifrovaným způsobem, zajišťujícím integritu a důvěrnost přenášených dat, • agent by měl být schopný komunikovat se záložním systémem, pro případ, že nastane problém v komunikaci se systémem primárním, • agent by měl sbírat a ukládat události určené pravidly i v případě, kdy selže komunikace s centrálou systému SIEM. • Velikost úložiště vzdáleného systému by měla být nastavitelná.

9	Systém SIEM by měl pro nasbírané a spravované události/data podporovat následující funkce:
	• filtrování událostí a sběr na základě předkonfigurovaných pravidel,
	• agregace/sumarizace událostí založená na předkonfigurovaných pravidlech, např. 100 událostí konkrétního typu v daném časovém úseku by mělo být vedeno jako nová agregovaná událost,
	• korelace událostí na základě upravitelných předdefinovaných korelačních pravidel pro korelaci
	  ○ propojení událostí z různých zdrojů založené na definovaných klíčích
	  ○ sledování sekvence událostí
	  ○ vytváření statistických modelů fungování
	• přesměrování události do jiného SIEM systému
	• běžný výklad události konkrétního typu definovaného systémem SIEM, **bez ohledu na systém nebo zařízení původu** dané události
	• normalizace a kategorizace – mapování logovacích zpráv z různých systémů do datového modelu
	• automatická kategorizace sbíraných dat/událostí, zahrnující minimálně tyto kategorie:
	  ○ řízení přístupu
	  ○ řízení konfigurací
	  ○ správa a sledování uživatelů
	  ○ vynucování pravidel
	• klasifikace událostí podle úrovně závažnosti
	• přiřazení úrovně závažnosti na základě výsledků korelačních pravidel
	• ohodnocení reputace zdroje události a možnost kontroly proti černé listině zdrojů – identifikace nebezpečné činnosti na základě zdroje
	• transparentní úložiště sesbíraných nezpracovaných původních dat (nenormalizovaných, pokud je to možné)

10	Systém SIEM by měl poskytovat společné prostředí pro správu událostí a jejich stavů.

Č.	Popis požadavku
	Správa událostí by měla umožňovat komunikaci s externím workflow a systémy pro helpdesk.
11	Systém SIEM by měl být schopný spolupracovat minimálně s následujícími technologiemi a systémy: • Vulnerability and policy compliance management systems • Nagios • HP OVO • HP ServiceCentre
12	Systém SIEM by měl být schopný importovat data o IT aktivech ze systémů třetích stran k tomuto určených.
13	Úložiště dat a funkcionalita systému SIEM by měly umožňovat uložení, správu a provoz množství dat nasbíraných za období 1 roku.
14	SIEM data (události) musí být externě archivovány a systém musí umožňovat jejich znovupoužití kdykoli je to potřebné. Archivovaná data musí být zabezpečena silným šifrovacím mechanismem a přístup k šifrovacím klíčům musí být monitorován systémem SIEM.
15	Data událostí musí být uložena v chráněném úložišti.
16	Bezpečnostní pravidla systému SIEM a jejich správa by měla být oddělena a zcela nezávislá na hostujícím operačním systému.
17	Uživatelské a servisní účty operačního systému by neměly mít přístup k systému SIEM bez další úrovně autentizace. Pokud bude povolena funkce SSO, bude tato funkce poskytovat kontrolu autentizace pro povolení specifických účtů operačního systému k zalogování do systému SIEM.
18	Pokud je na vzdáleném systému použit SIEM agent, neměl by být provozován pod účtem root, NT AUTHORITY/XXXX nebo pod jiným vestavěným systémovým účtem.
19	Systém SIEM by měl detekovat a upozorňovat na události, které jsou významně datově pozadu, nebo naopak mají časové razítko z budoucnosti.
20	Systém SIEM by měl poskytovat funkcionalitu ad-hoc dotazování. Pomocí dotazů by mělo být možné adresovat různé části jedné či více událostí. Způsob konstrukce dotazů by měl být dostatečně intuitivní. Pro tvorbu složitějších dotazů by měla existovat určitá podpora systému, např. pro tvorbu regulárních výrazů (regexp). Systém SIEM by měl obsahovat předdefinovanou knihovnu typických nebo více komplexních dotazů.
21	Systém SIEM umožňuje vytváření hlášení/reporting. Jednotlivá hlášení jsou k dispozici ve standardních formátech, např. pdf, xls, doc, html.
22	SIEM by měl mít funkcionalitu automatického generování hlášení. Automatické generování by mělo probíhat podle plánu (možnost nastavení data a času). Vygenerovaná hlášení by měla být k dispozici ke stažení na webovém přístupu, nebo by měla být zasílána pomocí emailu definovanému seznamu příjemců.
23	Systém SIEM by měl mít průvodce tvorby hlášení. Mimo vlastních hlášení by systém měl obsahovat knihovnu předdefinovaných hlášení.
24	Součástí systému SIEM by měly být tyto typy hlášení nebo dotazů: • Sledování konkrétní uživatelské relace napříč monitorovanou bází – sledování aktivit daného uživatele napříč všemi monitorovanými systémy • Sledování seznamu privilegovaných účtů • Hlášení událostí spadajících pod ISO 27001/2 a jejich mapování na příslušné požadavky ISMS. • Hlášení COBIT • Hlášení COSO • Hlášení FISMA • Správa uživatelských účtů (vytváření, úpravy, smazání)

Č.	Popis požadavku
	• Správa privilegovaných účtů (vytváření, úpravy, smazání) • Aktivity týkající se správy systému nebo aplikace • Sumarizace aktivit správy systému nebo aplikace • Aktivity týkající se odemykání/zamykání účtů • Aktivity týkající se systémových zdrojů a přístupů • Aktivity týkající se zdrojů aplikací a jejich přístupů • Hlášení všech událostí pro konkrétní systém • Hlášení všech událostí pro konkrétní aplikaci • Hlášení všech událostí/upozornění podle konkrétní úrovně závažnosti • Vizualizace konkrétní události v čase – např. histogram • Aktivity týkající se neúspěšné autentizace s nespecifikovaným nebo nepřípustným počtem pokusů • Hlášení o úspěšné autentizaci • Hlášení o úspěšných/neúspěšných pokusech o změně hesla • Hlášení o manipulaci s daty • Změny konfigurace systému • Změny konfigurace aplikace • Konfigurace síťových zařízení • Hlášení o selhání síťových zařízení • Hlášení o aktivitách síťových zařízení • Souhrnné hlášení síťových aktivit • Hlášení o zamítnutí přístupu bránou firewall • Hlášení o povolení přístupu bránou firewall • Sumarizace aktivit brány firewall • Firewall activities summary • Zvýšení oprávnění uživatele v průběhu relace (su, runas atd.) • Hlášení o aktivitách nad bezpečnostním úložištěm • Hlášení o instalaci SW • Hlášení o konfiguraci SW • Hlášení o aktivitách virtuálních systémů/aplikací (vytvoření, smazání atd.) • Hlášení o aktivitách správy virtuálních systémů • Hlášení o detekci nebo smazání virů • Hlášení o úspěchu/neúspěchu aktualizace virové databáze • Hlášení o aktivitách ohodnocení zranitelnosti • Hlášení o detekci zranitelnosti • Hlášení v souladu se standardním zabezpečením sítě a analýzou statistiky provozu • Monitorovaná zařízení | Zařízení neodesílající události • Síťová zařízení | Události týkající se konkrétního účtu • Síťová zařízení | Události týkající se konkrétní komunikační dvojice zařízení • Síťová zařízení | Nejvíce komunikující dvojice zařízení Systém by měl být schopen sledovat trendy týkající se dat v hlášeních.
25	Báze obsahu/znalostí by měla být dostupná jako implicitní funkce systému SIEM. Aktualizace parsování a mapování pravidel podporovaných aplikací, zařízení a systémů, stejně jako nová hlášení a dotazy, by měly být dostupné bez dalších poplatků.
26	Systém SIEM by měl obsahovat průvodce pro vytvoření parsovacích/mapovacích pravidel pro všeobecná zařízení. Systém by také měl umožňovat testování pravidel pomocí určitých vzorových typů událostí.
27	Systém SIEM by měl být schopný exportovat definice hlášení, parsovací/mapovací

Č.	Popis požadavku
	pravidla nebo dotazy ve formátu čitelném pro lidi.
28	Systém poskytuje verzování hlášení, mapovacích/parsovacích pravidel a pravidel pro třídění dat do kolekcí.
29	Systém SIEM umožňuje zálohování/export celé báze obsahu/znalostí. Pokud budou exportovaná data naimportována do nové instalace systému, nově nainstalovaný systém bude obsahovat kompletní sbírku a nastavení hlášení, politik, parsovacích/mapovacích pravidel a dotazů předchozího systému, ze kterého byl proveden export.
30	Dodavatel SIEM systému by měl poskytnout transparentní popis hlášení a jejich provázanost na standardy nebo předpisy (např. ISO 27001/2). Popis by měl transparentně informovat o tom, jak je hlášení mapováno na konkrétní paragrafy nebo kapitoly daného předpisu.
31	Klasifikace událostí systému SIEM by pro určité kategorie měla být také transparentně a detailně popsána. Dokumentace by měla obsahovat seznam klasifikací událostí, implicitní mapovací a parsovací pravidla a detailní popis jejich významu. Klasifikace by měla obsahovat kategorie událostí, např. *Zabezpečení systému, Správa přístupů, Správa zranitelností, Zabezpečení sítě* apod.
32	Uživatelské rozhraní by mělo být intuitivní a logické. Vstupní pole by měly umožňovat vkládání hodnot z historie.
33	Uživatelské rozhraní by ke své funkčnosti nemělo vyžadovat konkrétní nastavení systému. Preferovaným rozhraním je grafické webové uživatelské rozhraní.
34	Uživatelské rozhraní respektuje vymezené typy rolí uživatelů. Menu, objekty, hlášení, grafy a další součásti uživatelského rozhraní jsou dostupné na základě pravidel pro roli aktuálně přihlášeného uživatele.
35	Uživatelské rozhraní poskytuje logický a smysluplný popis existujících objektů a příslušnou funkci kontextové nápovědy.
36	Systém SIEM poskytuje transparentní informace o stavu systému hostitele (např. procesor, vytížení disků a paměti, dostupná disková kapacita...)
37	Systém SIEM poskytuje transparentní informace o hodnotě EPS – aktuální úroveň a graf historie. Informace o EPS by měly obsahovat statistiku jednotlivých zdrojů (agenti, sběrná místa, aplikace, systémy, zařízení...)
38	Systém SIEM by měl poskytovat relevantní zpětnou vazbu o chybových stavech jednotlivých komponent – např. komunikace s agentem nebo sběrným místem není možná, proces nebo jiná SIEM komponenta neběží...
39	Systém SIEM by měl poskytovat informace o stavu úložiště událostí – dostupnost, stav kapacity, stav integrity.
40	Systém SIEM by měl poskytovat návod jak integrovat systémy třetích stran, které nejsou implicitně podporovány.
41	V případě, že integrace systémů třetích stran vyžaduje programování, měly by být nástroje pro vývoj součástí produktu bez dalších poplatků. Návod „Jak vytvořit integraci produktů třetích stran“ by měl být také součástí, bez dalších poplatků.
42	Systém SIEM by měl být modulární a měl by podporovat efektivní škálovatelnost komponent. Komponenty řešení by měly být hierarchicky uspořádané tak, aby bylo možné celé řešení škálovat podle požadavků vyplývajících z růstu infrastruktury. Funkce škálovatelnosti by měla být logická a nákladově efektivní.
43	Systém SIEM by měl podporovat funkcionalitu vysoké dostupnosti bez nutnosti klastrového řešení třetích stran nebo speciálního HW řešení.
44	Systém SIEM by měl podporovat rotování zdrojových logů. Informace o tom, že nad úložištěm logů byla provedena rotace, by měly být oznámeny pomocí specifické události. Systém SIEM by měl být schopný pokračovat ve čtení logu historických dat zdroje bez nutnosti zásahu uživatele. Tok nasbíraných událostí by měl být transparentní vzhledem k předchozímu stavu. V průběhu obnovy by neměly vznikat duplicitní události. Na odchylky od transparentního stavu (např. generování událostí s rozdílným časovým razítkem) by mělo být upozorněno.
45	Musí být zajištěna integrita zaznamenaných událostí, žádná informace se nesmí ztratit, systém bude obsahovat řešení archivace.
46	Systém musí detekovat výpadek vlastních komponent a komunikace, hlídat vlastní integritu. Musí nahlásit, kde došlo k problému (a jakému).

Č.	Popis požadavku
45	Možnost tvorby agentů pro monitoring aplikací, nativně nepodporovaných.
48	Možnost “agent-less” monitoringu pro platformy, které toto umožňují (SNMPv3 trap forward, log forward)
49	Sbírat a ukládat všechny uvedené informace v nezbytném rozsahu o všech požadovaných typech událostí (viz též níže).
50	Získané informace musí být transformovány do jednotné/unifikované struktury.
51	Možnost snadno, za chodu, doplňovat pravidla vyhodnocování, na základě detekovaných událostí a jejich kombinací či posloupností.
52	Možnost postupné tvorby databáze znalostí (knowledge base), m.j. na základě předchozího bodu a použití knowledge base ve vyhodnocování událostí.
53	Nativní podpora (předdefinovaní agenti/adaptéry) pro Windows security log a Unix syslog, standardní logy databází Oracle a MS SQL.
54	Možnost šifrované komunikace mezi monitorovacím systémem (serverem) a monitorovanými systémy (agenty).
55	Uživatelská vstřícnost, přívětivost systému a jeho správy je podmínkou.
56	Reportovací systém, grafické zobrazení dat.
57	Uživatelské role – správce vlastního systému, uživatel,…jsou optimalizovatelné, aby nikdo nebyl zahrnován nepodstatnými údaji a zároveň měl dostatek důležitých údajů.
58	Kdykoli musí být možné zpětně dohledat činnost uživatele.
59	Detekce přihlášení na cizí účet (kde to je možné).
60	Detekce přihlášení uživatele na počítači, kde se obvykle nepřihlašuje.
61	Komunikace s jinými systémy (zjištění nadřízeného, jejich mailových adres, čísel pro SMS; ideálně i zjištění nepřítomnosti, dovolených).
62	Možnost zaslání e-mail, SNMP trap (i v3), spustit skript, SMS, jako reakce na daný stav, událost, překonaný práh hodnot/threshold..
63	Zálohování a archivace dat, automatická, nesmí nastat okamžik, kdy by se přicházející události nezaznamenávaly.
64	Možnost snadného obnovení ze zálohy a zpracování archivních dat bez narušení chodu monitoringu nových dat.
65	Podpora IPv6.
66	Online analyzovat jen vybranou část událostí, tj. takové události, které lze vyhodnotit a reagovat na ně v reálném čase.
67	Možnost detekce přihlášení na cizí účet
68	Možnost vymezit určité části sítě jako nemonitorované (např. podle network masky)
69	Kategorizace ud8lost9
70	Vlastní definice hodnocení závažnosti (podle typu události, zdroje, času, frekvence výskytu,…)
71	Sumarizace / agregace událostí
72	Korelace ud8lost9

Č.	Popis požadavku
73	Detekce sekvence událostí
74	Sumarizace musí probíhat jak ve vztahu ke zdroji (např. x pokusů o přihlášení z daného PC), tak vzhledem k subjektu (x pokusů o přihlášení na nějaký účet) nezávisle (data se nesmí ztratit).
75	Možnost některými událostmi (uplatnění pravidel) vyvolat workflow, žádost o vysvětlení (vazba na knowledge base).
76	Možnost tvorby vlastní knowledge base, na základě již řešených incidentů.
77	Z prostředí on-line monitoringu musí být možné vyvolat off-line analýzu „podobných“ událostí k události vybrané.
78	Grafické uživatelské rozhraní s možností definice jednotlivých operátorů s různými oprávněními, podpora rolí operátorů, s možností autentizace proti LDAP serveru.
79	Řešení musí být škálovatelné s možností distribuce zátěže mezi několik uzlů/nodes.
80	Řešení musí umožňovat interní audit (login, logout, spouštění pravidel, akcí, počet zpracovaných událostí atd.).
81	Pravidelná offline analýza širšího rozsahu typů událostí podle předdefinovaných profilů.
82	Kontrola konzistence a úplnosti sebraných dat.
83	Možnost filtrování a třídění podle libovolné informace včetně údajů získaných při on-line monitoringu (kategorizace, závažnost,…)
84	Monitoring privilegovaných uživatelů (administrátoři, správci aplikací, vlastníci citlivých dat)
85	Možnost vyhodnocovat vzájemnou souvislost informací, následnost; definovat typické sekvence událostí a ty pak vyhledávat nebo naopak ignorovat.
86	Zpětně dohledat činnost uživatele / činnost z PC / nad daným objektem (vyšetřování incidentu).
87	Možnost prohledávat výsledek předchozí filtrace nebo naopak jen mimo tento výsledek.
88	Vlastní reportovací systém, s možností tvorby vlastních, uživatelských, reportů, bez nutnosti psaní kódu. Možnost napojení na externí reportovací systém.
89	Podpora standardů (ISO 27001 apod.)
90	Obecné požadavky na strukturu informací: • Datum a čas vzniku události • Zdroj události (kde sedí uživatel) • Kdo je přihlášen (obsahuje-li tuto informaci) • Kde byla událost zjištěna • Zprostředkovatel (existuje-li, hlavně u databázových aplikací) • Protokol • Cíl události • Předmět události (na jaký druh předmětu událost působí) • Konkrétní předmět události (jméno souboru, jméno účtu kam se uživatel přihlašuje…) • Úspěch/neúspěch • Kód události (podle zdroje, pokud zdroj kódy používá) • Původní stav • Nový stav (u změnových událostí povinné) • Důvod chyby, je-li znám

Č.	Popis požadavku
	• Další specifické údaje a upřesnění
91	Informace navíc sledované: • Spuštění a zastavení tvorby auditních záznamů, modifikace nastavení • Smazání záznamů auditu, manipulace s auditním záznamem • Zapnutí a vypnutí počítače • Autentizace uživatele – úspěch/neúspěch/zablokování účtu, případně odhlášení uživatele • Útok identifikovaný bezpečnostními technologiemi (IDS, IPS, Antivir, ...)
92	Informace navíc sledované z pohledu správy: • Správa uživatelů (zřízení, změna, blokace, deblokace, zrušení uživatele) - kdo, kdy, jméno stanice případně IP adresa, co/činnost (původní/nová hodnota), výsledek činnosti (úspěch/neúspěch) • Správa rolí/změna přístupových práv uživatelské skupiny nebo uživatele (zřízení, změna, blokace, deblokace, zrušení role) - kdo, kdy, jméno stanice případně IP adresa, co/činnost (původní/nová hodnota), výsledek činnosti (úspěch/neúspěch) • Aktivní (transakce) a vybrané pasivní operace v systému; • Změny vybraných systémových proměnných a parametrů (mající dopad na bezpečnost) • Události dálkové správy systémů (včetně Remote access na plochu jiného uživatele) • Neobvyklé trendy (počty vyžádaných SMS, hádání autentizačních kódů nebo klientských čísel, ...)

Požadované výstupy
(D – dokument, S – služba, P - produkt)

(D) analýza prostředí - datový model prostředí zadavatele se specifiky jednotlivých zařízení, která mohou ovlivňovat fungování systému bezpečnostního monitoringu a posouzení spolupráce interních systémů ve smyslu zátěže a možností propojení se systémem bezpečnostního monitoringu,
(D) realizační projekt – návrh realizace bezpečnostního dohledu v produkčním a záložním datovém centru, detailní návrh technického řešení, definice systémů a aktivních prvků, pro které je vhodné monitoring nasadit, upřesnění časové náročnosti a požadavků na součinnost pro realizaci implementace řešení a návrh testů
(P) dodávka technického a programového vybavení SIEM systému,
(S) instalace a konfigurace technického a programového vybavení SIEM systému,
(S) integrace monitoringu do prostředí ICT PČR,
(S) provedení testů za účelem ověření a zdokumentování naplnění funkčních požadavků na systém bezpečnostního monitoringu,
(D) technická a provozní dokumentace,
(S) zaškolení.

Serverová infrastruktura související se zvýšením bezpečnosti systému

Server typ 1

Položka	Parametry
Počet kusů	6
Požadavky na CPU dle testů SPEC CPU2006	
SPECint_2006	min. 42
SPECfp_2006	min. 75
SPECint_rate 2006	min. 540
SPECfp_rate 2006	min. 458
Provedení	Blade kompatibilní se stávající infrastrukturou blade šasi c7000
CPU	Min. počet – 2
Paměť	256 GB RAM DDR3 1866 MHz
Interní úložiště	min. 2 GB USB flash nebo SD karta pro instalaci hypervizoru
Řadič	HW RAID 0,1;
Síťový adaptér	2 x 10 Gb/s TCP/IP Offload Engine; každý s možností rozdělení na úrovni HW až na 4 virtuální adaptéry
FC rozhranní	Dvouportový Fibre Channel 8Gb adaptér, SW pro redundantní připojení serveru s MS Windows 2008/2003 k dodávanému diskovému poli
Vzdálená správa	pomocí LAN (grafická konzole i bez nainstalovaného OS, možnost vypnout napájení, reset systému, klávesnice, myš, 128bitové šifrování, monitorování stavu HW bez nainstalovaného OS SW pro vzdálenou správu musí umožňovat: centralizovanou vzdálenou správu HW a shromažďování informací o konfiguraci a stavu jednotlivých HW komponent serverů (včetně ukládání těchto informací do databáze k dalšímu využití), detekci a zasílání zpráv (minimálně pomocí protokolu SNMP) o chybových stavech
Kompatibilita	Microsoft Windows 2003/2008/2012 (32b, 64b), Red Hat EL4, SuSe Linux, VMWare ESX 5.x
OS	Včetně OS Windows Server 2012R2 DC

Instalace	HW instalace, kompletní zprovoznění a oživení
Záruka	min. 5 let na všechny komponenty s odezvou 4h v místě plnění, pokrytí 24 x 7; dodavatel nepožaduje vrácení vadných HDD

Server typ 2

Položka	Parametry
Počet kusů	4
Provedení	Blade kompatibilní se stávající infrastrukturou blade šasi c7000
Procesor	1x CPU 64 Bit RISC/EPIC Procesor 8 jader (min 2 GHz)
	Počet osaditelných CPU: min. 2 ks
Paměť	48 GB RAM DDR3 1333MHz
Interní úložiště	2x 146GB 6G SAS 15krpm
Řadič	HW RAID 0,1; 512 GB Cache
Síťový adaptér	4 x 10 Gb/s TCP/IP Offload Engine; každý s možností rozdělení na úrovni HW až na 4 virtuální adaptéry
FC rozhraní	Dvouportový Fibre Channel 8Gb adaptér, SW pro redundantní připojení serveru do stávající SAN
Vzdálená správa	pomocí LAN (grafická konzole i bez nainstalovaného OS, možnost vypnout napájení, reset systému, klávesnice, myš, 128bitové šifrování, monitorování stavu HW bez nainstalovaných OS SW pro vzdálenou správu musí umožňovat: centralizovanou vzdálenou správu HW a shromažďování informací o konfiguraci a stavu jednotlivých HW komponent serverů (včetně ukládání těchto informací do databáze k dalšímu využití), detekci a zasílání zpráv (minimálně pomocí protokolu SNMP) o chybových stavech
OS	HP-UX včetně clusterových licencí kompatibilních s používaným HP-UX SW
Virtualizace	V rámci fyzického serveru systém umožní provozování virtuálních serverů, každý s vlastní instancí OS, host name a IP adresou. Virtualizační technologie musí být uznaná jako „hard partitioning“ pro produkty Oracle
Instalace	HW instalace, kompletní zprovoznění a oživení
Záruka	min. 5 let na všechny komponenty s odezvou 4h v místě plnění, pokrytí 24 x 7; dodavatel nepožaduje vrácení vadných HDD

Součástí dodávky musí být 1 blade šasi plně vybavené duální síťovou infrastrukturou (Ethernet + FC switche nebo virtual connect, SFP), kompatibilní s dodanými servery.

Virtualizační SW

Počet kusů	12
Položka	Parametry
Provedení	software – licence na CPU
Parametry	funkce automatického vyvažování výkonnosti mezi fyzickými servery. Přesun virtuálních serverů za běhu podle jejich vytížení a výkonnostní potřeby HW. Automatický náběh virtuálních serverů v případě výpadku fyzického serveru
	Implementovaná správa virtualizačního systému z jednoho centra, zařazení do stávající správy virtualizačního řešení, která je realizována produktem VMware vCenter Server.
	funkce vyšší dostupnosti - virtuální server může mít spuštěnu záložní kopii na dalším HW serveru. V případě havárie primárního HW serveru dojde k automatické bezvýpadkové aktivaci záložní kopie
	funkcionalita virtuálního distribuovaného switche
Instalace	SW instalace, kompletní zprovoznění a konfigurace
Záruka	min. 5 let SW podpora produktu

Rozšíření diskového prostoru pro ukládání dat systému dohledu a analýzy bezpečnostních událostí

Detail
Rozšíření V800 32x 480GB SSD (8 magazine) OS Remote Copy pro dodávanou kapacitu Virtual Copy pro dodávanou kapacitu Optimization Suite pro dodávanou kapacitu Thin Suite pro 10TB kapacity Podpora v rozsahu obdobném stávajícího diskového pole dodavatel nepožaduje vrácení vadných HDD

Posílení databázové vrstvy

Stávající stav

SQL server je v současnosti nasazen na PP PČR především ve verzi 2012. V několika posledních verzích představuje Enterprise řešení, srovnatelné s jinými velkými databázovými systémy např. Oracle, přitom ovšem je dostupnější ekonomicky, jak co do ceny licencí, tak provozu a TCO. Díky integraci především s nástroji Microsoft Office, s dalšími systémy

především na platformě Microsoft, ale i s konkurenčními datovými úložišti poskytuje uživatelům některé výhody, které ostatní databázové systémy nemohou plně poskytnout. Je srovnatelně bezpečnostně i výkonově certifikován s konkurencí a má řadu nástrojů pro zajištění bezpečnosti a šifrování dat v úložištích a přístupu k nim, jakož i nástroje pro sledování a audit prováděných operací a jeho vyhodnocení.

SQL Server umožňuje nasazení v rámci geograficky rozprostřených vysoce dostupných řešení – serverových clusterů:

- umožňující automatický přechod databázové části aplikace na jiný server, pokud dojde k selhání HW, nebo některé klíčové části SW vybavení,
- umožňující provádět údržbu serverů bez potřeby odstávky při instalacích záplat (včetně bezpečnostních) a restartech serverů, tím že úlohu převezme jiný server
- rozkládat výkon podle potřeby mezi jednotlivé servery
- pokrytí výpadku celé lokality

Na PP PČR je vybudován jeden databázový cluster sestávající ze tří serverů BL460 2 CPU x 6 core, 128 GB RAM provozující SQL Server 2012 Enterprise Ed v multiinstančním režimu, zalicencovaný jako Active-Active-Passive(záložní server).

Toto databázové řešení poskytuje v jedné lokalitě službu vysoce dostupného trvale spravovaného databázového úložiště pro řadu aplikací. Vedle vlastní databáze je k dispozici i reportovací nástroj, služba zálohování a pravidelné údržby databází (kontrola konzistence a defragmentace dat), samostatné administrátorské přístupy, bezpečně izolovaná data různých aplikací atd. V současné době na produkčním clusteru běží, nebo jsou nasazovány následující aplikace:

- Sharepoint
- Project Server
- LYNC (komunikační nástroj)
- FIM propojení mezi EKIS(SAP) a Active Directory
- Očista
- IMC
- Plánuje se nasazení AISU
- Microsoft SCCM
- CRZ
- Matrix (správa serverů) v obou lokalitách
- CDO
- KSU
- TFS (úložiště zdrojových kódů)
- a na provozní instanci jsou data malých aplikací např. Předběžná opatření, Registrace IMZ

V současné době je stávající cluster již téměř zaplněn.

Požadavky na řešení

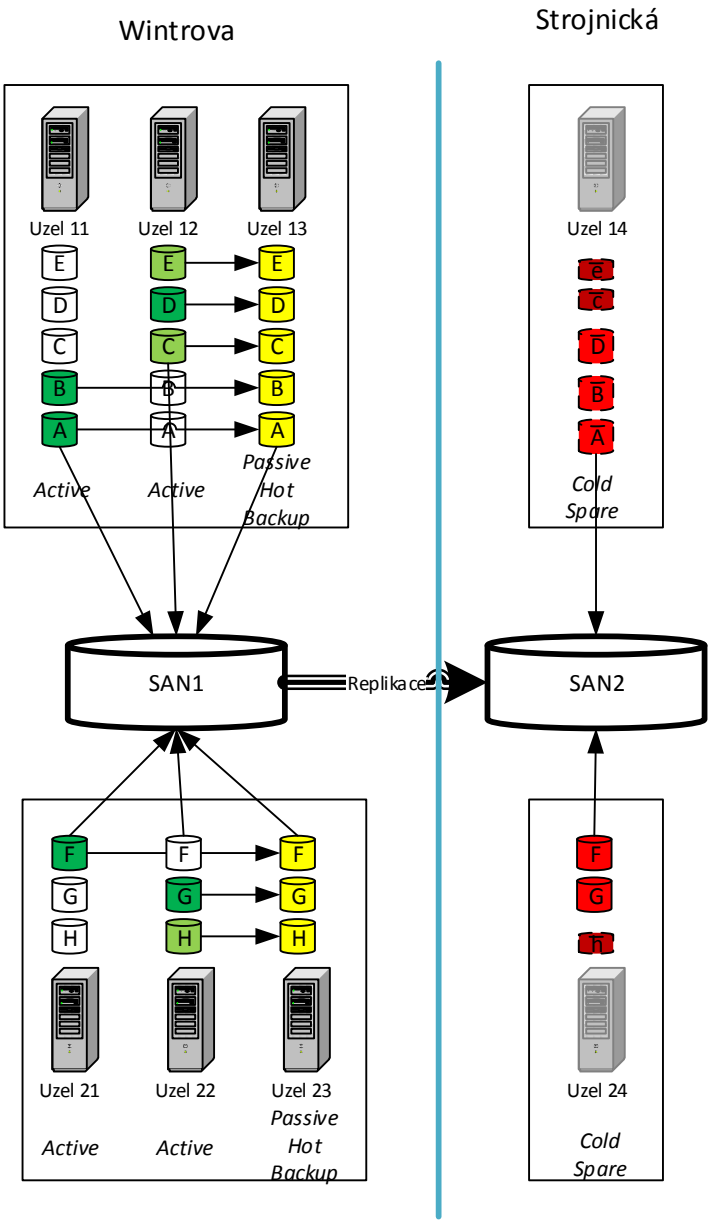
Požadavkem na řešení je rozšíření současného clusterového řešení o další 3 nody na opět v módu Active-Active-Passive čímž dojde k znásobení možných instancí a zajištění vyšší bezpečnosti v rámci provozu kritických aplikací.

Dále pak v rámci záložní lokality musí být možné vytvořit cold zálohu s plnou replikací dat v rámci diskového pole opět pro vybrané kritické aplikace, jež umožní v případě výpadku primární lokality přepnout do záložní.

- V původní lokalitě Bubenečská je cílem posílit cluster o 3 servery obdobného typu jako stávající, avšak s 256 GB RAM.
- V nové lokalitě Strojnická by se do clusteru zapojily 2 servery obdobného typu jako stávající, se 128 GB RAM.

Replikace dat musí být zajištěna prostředky SAN.

V době běžného provozu záložní lokalita bude sloužit pouze jako cold záloha, v případě výpadku přechod záložní lokality do plného záložního provozu bude znamenat off-line spuštění nodu clusteru v záložní lokalitě a převzetí dat z diskového pole.



Jako nedílnou součást řešení bude Policie ČR požadovat rovněž dodávku kompletní dokumentace a proškolení dotčeného personálu.

Požadované výstupy
(D – dokument, S – služba, P - produkt)

(D) Revize architektury systému (postup vývoje, klientská část, HW, SW, sítě, disky, prostupnosti)
(P) Dodávka požadovaných licencí
(S) Vlastní implementace a instalace SQL licencí
(S) Spolupráce na návrhu testů, testování, ladění
(S) Podpora nasazení ve vývojovém, testovacím a produkčním prostředí
(S) Proškolení uživatelů

Požadované licence

Detail
12 ks Licence MS SQL server enterprise 2core, business critical support 5y

Část B

Systém pro ukládání dat z evidence trestního řízení

Datové centrum bude poskytovat sdílené úložiště pro ukádání velkého množství dat přes protokoly CIFS, NFS, případně Http.Bude se jednat o klasický adresářový systém, do jehož struktury na základě oprávnění budou mít přístup vybrané útvar, jež tato data pořídila případně následně zpracovávala. Toto úložiště budou sloužit k ukládání zpracovávaných dat z vybrané lokality, což umožní poté uvolnit kapacitu na lokálním pracovišti, data budou archivována po potřebnou dobu a zároveň k nim bude možné kdykoliv online přistoupit.
Datové úložiště musí být plně redundantní, řešící výpadek každé své jednotlivé komponenty.
Předpokládaná dostupnost datového úložiště bude 99.995%

Parametr	Požadovaná hodnota
provedení disk. pole	diskové pole musí být možné instalovat do 19” racku, součástí dodávky musí být rackové lyžiny
Napájení celého diskového pole	Pouze AC
Architektura systému	Plně redundantní architektura v režimu Active-active cluster mode, kde nody nasového clusteru sdílí diskový prostor a mohou simultáně přistupovat do adresářů Celý system musí umožňovat připojení přes NAS, FC SAN, a IP SAN.
NAS nody musí podporovat protokoly	NFS v2/v3, CIFS SMB 1.0, FC, FCoE, iSCSI, FTP, and HTTP
Škálovatelnost	Vyžadujeme možnost rozšíření počtu NAS nodů až na 8, minimální počet NAS nodů musí být 2
Diskové police	podpora pro diskové police na 2,5" a 3,5" disky, možnost mixovat disky stejného typu ale jiné kapacity a rychlosti v jedné polici
Velikost Cache NAS nodu	min. 96GB
požadovaná kapacita	Minimální požadovaná čistá kapacita v RAID 6 (po odečtení Spare disků a parity) musí být 5,6 PB
Typ připojení back-endu	6Gbps SAS porty
Podporované disky	SAS (10k i 15k), SSD, NL-SAS, SATA
počet host. Portů per NAS node	min. 4x 1Gbps Ethernet, 4x 8Gbps FC a 4x 10Gbps Ethernet možnost variantně rozšířit o: 4x 1Gbps Ethernet 4x 10Gbps Ethernet
RAID	0, 1, 5, 6, 10, 50
rozšíření kapacity	Kapacita musí být rozšiřitelná pouhým přidáním diskových polic a to na minimálně 8PB

spolehlivost	Vysoce dostupná architektura v rámci jednoho logického zařízení, kde výpadek jakékoliv jedné komponenty neznamená nedostupnost přístupu k datům ani ztrátu IO operace. Diskové pole je navrženo na dostupnost minimálně 99,995%.
Počet File systémů	Minimálně musí být podporováno 250 file systémů
Kapacita File systému	Musí být podporována maximální velikost file systému 255TB
Počet souborů	Musí být podporováno minimálně 1 bilion souborů v jednom file systému
Počet souborů v adresáři	Minimálně 100 000
MTBF (Mean Time Between Failures)	min. 120.000 hodin
výkon	Min. 50 000 OPS na jeden node
RAS	Veškerý vadný HW lze vyměnit za běhu diskového systému, aniž by byla způsobena jeho nedostupnost. Toto platí zejména pro výměnu vadných disků jakéhokoliv typu a výměnu celého kontroléru nebo jakékoliv jeho součásti. Veškerý upgrade software/firmware musí být proveditelný za běhu diskového pole, aniž by byla způsobena nedostupnost. Po dobu upgrade mohou být nedostupné některé SW funkce. Předpokládá se provádění těchto změn mimo provozní špičku Kromě standardní RAID ochrany pole disponuje technologií, která je po výpadku libovolného jednoho disku schopná poškozený prostor automaticky nahradit z rezervní kapacity (tato vlastnost je některými výrobci nazývána „hot-spare disk“ nebo „spare capacity“) Při výpadku elektrické energie musí být Cache data ochráněna nejméně po dobu 50 hodin Pole musí disponovat Cache synchronization mechanismem
Software pro ovládání pole	Součástí nabídky musí být licence pro lokální správu diskového pole pomocí grafického rozhraní (GUI) a příkazové řádky (CLI), včetně licence na multipathing Přístup zabezpečeným (šifrovaným) protokolem (např. HTTPS pro GUI a SSH pro CLI). Možnost mapování jednotlivých interních rolí a oprávnění na uživatelské skupiny v adresářové službě LDAP Přístup založený na rolích (Role Based Access Control), jejichž oprávnění je možné manuálně konfigurovat Možnost autentizace uživatelů proti adresářové službě LDAP Kromě veškerých konfiguračních dat management diskového pole pořizuje a ukládá výkonnostní statistiky pomocí CLI nebo GUI

	Management musí být schopen zasílat události, které vznikají spontánně uvnitř pole za běžného provozu (např. chybové stavy, přihlášení uživatele, apod.), pomocí standardních protokolů SNMP nebo pomocí emailu Pokud management obsahuje SNMP agenta, Dodavatel poskytne MIB popisující dané zařízení
Load Balancing	NAS nody musí umět Inteligentně alokovat spojení ke klientům na základě CPU zátěže, využití paměti, network flow, a počtu připojení
Lokální časové snímky	Diskové pole musí podporovat vytvoření lokálního časového snímku („snapshotu“). Tato technologie musí splňovat následující mandatorní požadavky Zadavatele: Počet snímků z jednoho zdrojového file systému je minimálně 128 a maximální počet Snapshotů na celé pole je 512
Tiering	Diskové pole musí podporovat Dynamický Tiering (tzn.možnost nastavení automatického přesunu dat mezi jednotlivými typy disků dle stanovených kritérií transparentně pro klientský OS). Tato technologie musí splňovat následující mandatorní požadavky: Musí být možné nastavit Tiering policy a data musí být migrovatelná mezi jednotlivými tiery tam i zpět. Na základě statistik o přístupech musí být možné konfigurovat jak automatickou tak manuální relokaci.
Quota Management	Quota management musí být možné konfigurovat na uživatele nebo uživatelskou skupinu
Přidělování uživatelských práv	Musí být podporováno přidělování uživatelských práv prostřednisctvím Active Directory, NIS, a LDAP.
Podporované OS a aplikace	Dodavatel garantuje kompatibilitu s následujícími operačními systémy: · Microsoft Windows Server Standard/Datacenter, 2008 (32/64bit) · Microsoft Windows 7 a Windows 8 (32/64bit) · Red-Hat Enterprise Linux 5, 6 x86 · SUSE Linux Enterprise Server 10, 11; · VMware vSphere 5 s podporou VAAI a VASA provider; · Red-Hat Enterprise Virtualization (RHEV - KVM) 5, 6; · HP-UX 11i v1, 11i v2, 11i v3; · IBM AIX 5, 6, 7; · Cent OS 5,6 · Oracle Solaris 10, 11 · Mac OS X 10.x · Free BSD · Symantec NBU 7 · CommVault Simpana 9.0 · EMC Networker 7 · IBM TSM 5, 6
Podpora a servis	servisní podpora typu 5x9 NBD po dobu minimálně 5 let , oprava v místě instalace zařízení v ceně dodávky DMR – dodavatel nepožaduje vrácení vadných HDD