# **Příloha č. 2 zadávací dokumentace - Technická specifikace a požadavky zadavatele**

# **Řízení a správa privilegovaných účtů a přístupů**

Nemocnice Pardubického kraje, a.s. (dále jen „**NPK**“ nebo „**Zadavatel**“) je nemocnice krajského typu s pracovišti rozmístěnými na území celého kraje. Hlavní lokality, kde jsou pracoviště nemocnice jsou:

* Pardubická nemocnice, Kyjevská 44, 53203 Pardubice,
* Chrudimská nemocnice, Václavská 570, 537 27 Chrudim,
* Svitavská nemocnice, Kollárova 7, 568 25 Svitavy,
* Litomyšlská nemocnice, J. E. Purkyně 652, 570 14 Litomyšl,
* Orlickoústecká nemocnice, Čs. armády 1076, 562 18 Ústí nad Orlicí.

V NPK je realizován elektronický informační systému IS NPK, v rámci kterého je provozováno velké množství informačních a komunikačních systémů. Technologické prostředí je tvořeno rozlehlou síťovou infrastrukturou s decentralizovanými datovými centry ve všech lokalitách NPK.

NPK je provozovatelem základních služeb státu v oblasti zdravotnictví. To ukládá nemocnici povinnost zajistit **úroveň** **kybernetické bezpečnosti** dle požadavků ***zákona 181/2014 Sb.*** *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*, resp. dle požadavků ***vyhlášky č. 82/2018 Sb.,*** *vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*, a to zejména dle paragrafů vyhlášky:

* §12 Řízení přístupů
* §19 Správa a ověřování identit
* §20 Řízení přístupových oprávnění

Součástí řízení přístupů a přístupových oprávnění je řízení tzv. privilegovaných účtů a přístupů. Privilegované účty jsou určeny pro provádění úkolů správy technické infrastruktury IS NPK a výkon kontrolních činností. Pro zajišťování těchto činností jsou určeny specifické odpovědné osoby, interní či externí správci, administrátoři či auditoři, dále též **privilegované osoby**. Každá privilegovaná osoba musí mít svůj osobní (na její identitě založený) účet, též **privilegovaný účet.** Přístupy těchto privilegovaných osob ke konkrétním aktivům technologické infrastruktury IS NPK musí být řízeny za základě jejich identity a jejich činnost prováděná na aktivech technologické infrastruktury IS NPK musí být kontrolovatelná, auditovatelná.

Privilegované účty představují významné bezpečnostní riziko pro každou organizaci, protože:

* umožňují téměř neomezený přístup a manipulaci s informačními aktivy organizace. V případě kompromitace privilegovaného účtu je organizace vystavena velkému riziku neautorizovaného zneužití nebo vyzrazení kritických informačních aktiv,
* privilegované účty jsou v praxi často sdíleny mezi více administrátory, proto je obtížné určit odpovědnost za případné zneužití ze strany interního zaměstnance,
* hesla u privilegovaných účtů administrátorů a servisních účtů služeb a aplikací nejsou obvykle pravidelně měněna a často na ně není aplikována bezpečná politika hesel,
* je obtížné v reálném čase monitorovat nebo aktivně zasahovat do probíhajících relací u privilegovaných účtů v případě podezření na zneužití oprávnění.

Z výše uvedených důvodů NPK poptává **nástroj pro řízení a správu privilegovaných účtů a přístupů,** tzv. „Privileged Identity Management“ a „Privileged Access Management“ (dále jen „**PIM/PAM**“), který zajistí jednotnou centrální správu privilegovaných účtů, řízení přístupů k aktivům technologické (hardware/software) infrastruktury IS NPK a monitorování operací prováděných privilegovanými osobami (osobami s účty s vyšším oprávněním než user/domain user).

## Specifikace rozsahu díla, dodávky nástroje pro PIM/PAM

Pro dodávku PIM/PAM řešení je požadováno, aby se skládala z minimálně následujících fází:

* **Vstupní analýza** – vytvoření „*Implementačního plánu projektu*“ realizace díla,
* **Instalace** – instalace řešení na prostředky NPK,
* **Implementace** – provedení nastavení, konfigurace, vč. všech provozních nastavení dle požadavků NPK,
* **Testování** – testování funkčnosti dodávaného řešení před akceptací díla,
* **Dokumentace**,
* **Zaškolení** **správců** – odborné zaškolení správců, administrátorů dodávaného řešení,
* **Akceptace –** provedení akceptačních procedur a předání do ostrého provozu.

### **Vstupní analýza**

Zhotovitel provede v rámci realizace díla vstupní analýzu a vytvoření „*Implementačního plánu projektu*“ pro následnou realizaci díla. Součástí Implementačního plánu projektu bude technický popis řešení, vč. finální podoby implementace (nastavení) dodávaného řešení, testovací scénáře, popis akceptačních procedur a akceptační protokoly, harmonogram realizace projektu, potřebné instalační postupy a požadavky na zajištění součinnosti.

### **Instalace**

* Zhotovitel realizuje dodávané řešení PIM/PAM v prostředí IS NPK ve shodě s Implementačním plánem projektu,
* veškeré náklady související s dopravou a instalací jdou na vrub Zhotovitele,
* instalace řešení PIM/PAM bude provedena do vyhrazené infrastruktury Zadavatele.
* Technici Zhotovitele splňují veškeré podmínky dané výrobcem PIM/PAM pro jeho instalaci.
* Popis architektury instalovaného PIM/PAM řešení a popis verzí bude součástí dokumentace.

### **Implementace**

Zhotovitel provede potřebnou konfiguraci a nastavení systému PIM/PAM a všech komponent dle níže uvedených požadavků. Implementace bude zahrnovat, zejména:

* nastavení politik pro PIM/PAM,
* nastavení nahrávání privilegovaných relací s retencí tři měsíce,
* integrace koncových zařízení, včetně zachování neovlivněného hesla nejvyšší úrovně oprávnění (v obálce do trezoru)
* minimálně pro níže uvedené systémy bude provedena integrace řízení hesel privilegovaných účtů včetně bezheslového přihlášení se na integrované zařízení/systém (SSO)

OS Windows (MS Server 2008 a vyšší, včetně rolí: IIS, DHCP, DNS, AD)

prostředky (switche, routery, firewally, …) počítačové sítě NPK

VMWare ESXi

VMWare vCenter

MS SQL

Vzdálená správa (iLO, iDRAC, …)

TeamViewer

Office 365

a dále včetně programového a technického vybavení dodaného jako součást tohoto projektu

* integrace na systém centrálního logování,
* za součást implementace je považována také součinnosti při konfiguraci sítě a bezpečnostního monitoringu.

### **Testování**

Zhotovitel zajistí řádné otestování řešení PIM/PAM dle navržených testovacích scénářů v Implementačním plánu projektu. Zejména budou provedeny následující testy:

* funkční testy,
* bezpečnostní testy,
* DR testy,

### **Dokumentace**

Součástí dodávky musí být dokumentace v následujícím rozsahu:

* Implementační plán projektu, vč. popisu architektury řešení a finální konfigurace.
* Produktová dokumentace výrobce ke všem dodávaným modulům PIM/PAM,
* Instalační dokumentace (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj systému PIM/PAM) a dokumentace k integrovaným systémům
* Administrátorské a uživatelské příručky (manuály),
* Popis havarijních plánů pro obnovu služeb PIM/PAM systému,
* Dokumentace ke všem logům – hlavně popis struktury logů, seznam událostí s jejich významem a vazbou na jednotlivé operace.

Uvedená dokumentace je požadována v českém jazyce. Produktová dokumentace výrobce, včetně dokumentace výrobce popisující strukturu a význam logů, je akceptovatelná v anglickém nebo českém jazyce.

Pravidelná aktualizace dokumentace bude prováděna v rámci služeb servisní podpory, a to pravidelně při jakékoliv změně, např. aktualizacích (patchování, upgrade) realizovaného PIM/PAM řešení, pokud nebude dohodnuto jinak.

### **Školení a zaškolení**

* Zajištění školení i zaškolení ICT specialistů proběhne v prostorách NPK. Konkrétní termíny a místo bude určené po vzájemné dohodě. Školení i zaškolení proběhne v českém jazyce.
* Základní školení pro předem definovaný počet lidí se zaměří na základní seznámení s produktem, jeho instalací, konfigurací a uvedením do provozu. Cílem je porozumění dané technologii pracovníky Zadavatele, srovnání pojmů pro další komunikaci.
* Zaškolení pro správce tohoto řešení poskytne určeným pracovníkům komplexní informace v takovém rozsahu, aby tito pracovníci dokázali samostatně a dlouhodobě administrovat a provozovat dodané řešení. Součástí zaškolení bude i obnova řešení po havárii.
* Školitel bude disponovat certifikací výrobce dodávané technologie, resp. výrobců všech technologií, ze kterých bude složena dodávka (pokud výrobci takové certifikace vystavují) a bude mít praxi v oboru minimálně 5 let. Certifikát je možno nahradit čestným prohlášením výrobce o způsobilosti daného školitele.

### **Akceptace**

Zhotovitel a Zadavatel provedou společně akceptační testy a procedury. Akceptace díla je stvrzena podpisem akceptačních protokolů oběma stranami.

Podpisem akceptačních protokolů:

* přebírá Zadavatel dílo do užití (do ostrého provozu),
* ukončuje platnost Smlouvy o dílo,
* vzniká Zhotoviteli nárok na úhradu ceny díla,
* spouští platnost Smlouvy o poskytování servisních služeb.

### **Licenční zajištění**

Součástí dodávky musí být licence systému PIM/PAM pro uživatele, a to v počtu pro 50 ks licencí pro interní administrátory a 70 ks licencí pro externí administrátory uživatelů při neomezeném počtu připojovaných zařízení.

Licenčně musí být řešení rozšiřitelné na dvojnásobek bez dalších technických změn.

### **Technická a funkční specifikace**

Dodávané řešení musí splňovat minimálně tyto požadavky:

| *Požadavek na funkcionalitu systému PIM/PAM* | *Splněno: ANO / NE* |
| --- | --- |
| Bezpečné úložiště - veškeré informace o účtech, heslech, vlastnících, přístupech a veškeré nahrávky a logy budou uložené v centrálním zabezpečeném úložišti, které musí být chráněné alespoň těmito mechanismy" - Firewall nakonfigurovaný tak, aby se systémem mohly komunikovat pouze autorizované komponenty řešení - Restriktivní konfigurace systému - tzv. hardening - Komunikace s dalšími komponenty, externími systémy, nebo uživateli je šifrovaná použitím algoritmů splňující mezinárodní normu FIPS 140-2 - Silný mechanismus řízení přístupů "ACL" - na úrovni bezpečného úložiště a to až na úroveň jednotlivých objektů - Řízení vzdáleného přístupu - Integrace silné autorizace - Ověřování verzí |  |
| Vysoká dostupnost – Produkční prostředí je nainstalováno v režimu vysoké dostupnosti. Každá komponenta řešení musí obsahovat minimálně dvě samostatné instance v režimech active/active nebo active/passive. Řízení vysoké dostupnosti musí být plně automatické.  V případě vzniku nedostupnosti některé z komponent řešení za běžného bezporuchového stavu tak musí dojít k automatickému přepnutí provozu/aktivaci druhé nebo záložní komponenty (failover). Řešení, které vyžaduje manuální zásah je nepřípustné a řešení se nesmí spoléhat na zajištění vysoké dostupnosti pomocí virtualizačních funkcí. Po sjednání opravy komponenty je však přípustné provést její aktivaci (failback) manuálně.  Bezpečné úložiště musí být instalovatelné na fyzický - nevirtualizovaný – hardware (dodávka HW není součástí dodávky projektu) , aby byl možný přístup k zabezpečeným datům i v případě nedostupnosti virtuálního prostředí. Ostatní komponenty řešení musí být nainstalované z bezpečnostních a provozních důvodů na jiném systému, než je bezpečné úložiště. |  |
| Zálohování - Úložiště privilegovaných účtů a jejich přihlašovacích údajů, a nastavení řešení je možné pravidelně zálohovat, aby byla zaručená jeho dostupnost. Zálohy jsou zabezpečené šifrováním proti neoprávněnému přístupu. Je implementovaný proces zajišťující bezpečný přístup k heslům uloženým v systému v případě částečné, nebo úplné nedostupnosti systému. |  |
| Uživatelské prostředí poskytující funkce uživatelům je přístupné přes webové rozhraní s plnou podporou následujících prohlížečů v OS Windows, Mac, a Linux: Internet Explorer   * Edge * Chrome * Firefox * Safari |  |
| Auditní záznamy a logy veškerých aktivit v zabezpečeném úložišti jsou chráněné proti změnám a vymazání všemi uživateli (včetně administrátora řešení) |  |
| Data a objekty jako hesla, SSH klíče, video nahrávky, logy, definice přístupových oprávnění jsou uložené v zabezpečeném úložišti a zašifrované. Přístup k nim má pouze vlastník a jím určené osoby. Administrátor zabezpečeného úložiště ani jiný nepověřený uživatel, nemá práva přístupu ke čtení, používání, modifikace, nebo smazání. |  |
| Řešení podporuje integraci s LDAP pro správu uživatelů. Nabízené řešení musí podporovat synchronizaci změn a aktualizovat záznamy. Například uživatel přidaný/odebraný ze správy LDAP - řešení automaticky propaguje/odstraní uživatele ze systému správy. |  |
| Nabízené řešení podporuje dotazy a řízení přístupu k heslům i pro "vnořené" globální skupiny, podporuje komplexní Active Directory infrastruktury - geografické lokality, sofistikované prohledávání LDAP. |  |
| Autentizace a autorizace uživatelského přístupu k veškerým komponentám je řízená pomocí LDAP, Radius a Active Directory. |  |
| Pro autentizaci uživatele je možné využít automatické přihlášení (SSO) na základě přihlášení k doméně AD Integrated Windows Authentication. Řešení také podporuje dvoufaktorovou autentizaci PKI, OTP a LDAPS. |  |
| V rámci řešení jsou definovatelné minimálně tyto role" a) administrátor řešení – může upgradovat systém, přidávat uživatele a řídit povolené objekty b) auditor - má přístup k auditním informacím a nahrávkám c) uživatel - má umožněný přístup k řešení a jeho běžné užívání |  |
| Řešení musí logovat auditní záznamy o administrátorských a uživatelských aktivitách. Minimálně musí logovat následující typy událostí vykonaných v rozhraní aplikace: • úspěšné a neúspěšné (pokusy o) přihlášení a odhlášení • konfigurační změny (musí být zřejmé, kdo provedl, jakou konfigurační změnu)  • získání hesla  • přístup k nahrané session |  |
| Řešení podporuje zasílání notifikací pomocí emailu pro definované události, a to minimálně při následujících akcích: • Přístup a ukončení práce v systému • Změny v systému • Použití hesla • Požadavek na heslo a schválení požadavku |  |
| Řešení disponuje vlastními předdefinovanými reporty o aktivitách uživatelů a auditech používání spravovaných přihlašovacích údajů. Podporuje plánování automatického generování těchto reportů: • Oprávnění uživatelů • Veškeré aktivity uživatelů • Přehled privilegovaných účtů  • Přehled spravovaných aplikací • Přehled zadaných/schválených požadavků  • Přehled provedených změn na konkrétním systému  • Přehled činností konkrétního uživatele |  |
| Řešení je možné integrovat s externím ticketovacím systémem a zároveň má integrovaný vlastní interní ticketing systém pro schvalování požadavků na přístup k objektům (privilegované účty, záznamy, logy). |  |
| Řešení je napojeno na dodávaný centrální logovací systém, který je také součástí tohoto projektu a přenáší data v reálném čase a v těchto formátech: • Syslog • SNMP Trap • Textový soubor • JDBC  • CEF nebo LEEF • Microsoft Event Log |  |
| Řešení PAM umožňuje komplexní centrální evidenci a správu privilegovaných osobních, sdílených, servisních a aplikačních účtů |  |
| Řešení PAM umožňuje definovat, kterým uživatelům mají být k dispozici jaké privilegované účty, na kterých systémech, jakým způsobem se mají uživatelé k vybraným privilegovaným účtům moci připojit. |  |
| Uživatel se do systému autentizuje přes webové rozhraní a po přihlášení je uživateli zobrazen seznam jenom těch privilegovaných účtů, ke kterým má přidělený přístup. Veškeré ostatní privilegované účty zůstávají v systému pro uživatele skryté a nedostupné. |  |
| Řešení umožňuje správu neomezeného počtu privilegovaných účtů na neomezeném počtu zařízení. |  |
| Řešení PAM se připojuje k spravovaným systémům a umožňuje změnu hesel privilegovaných účtů na koncových systémech bez instalace agenta atp. Připojení probíhá tak, aby minimálně zatěžovalo spravovaný systém a je možné plánovat čas připojení. |  |
| Řešení PAM umožňuje také evidovat hesla pro nespravované privilegované účty. Změna hesel u takových účtů se provádí manuálně. |  |
| Řešení PAM podporuje proces pro automatické vyhledávání 'discovery' nespravovaných účtů na cílových systémech. Takovéto účty jsou v rámci navrhovaného procesu zařazeny do systému řízení PAM. Výsledky Discovery jsou zaznamenány a jsou dostupné v přehledném a interaktivním zobrazení. |  |
| Řešení PAM umožňuje automaticky vyhledávat a přidávat nové privilegované účty do správy PAM. Řešení dle charakteristiky privilegovaného účtu automaticky přiřazuje definovanou bezpečnostní politiku. |  |
| Vlastnosti hesel – Řešení PAM umožňuje definovat vlastnosti hesel pro jednotlivé privilegované účty, nebo skupiny privilegovaných účtů: • nastavení komplexnosti hesel – počet znaků a podpora různých znakových sad a kombinace znaků • periodicita výměny hesla na cílových systémech • věk hesla • unikátnost hesla v definovaném počtu posledních výměn a pro veškeré spravované privilegované účty, nebo skupiny |  |
| **Výměny hesel** – Řešení musí poskytovat možnost změny jednoho nebo skupiny hesel: • Automaticky, když je stáří hesla větší než... • Manuálně uživatelem – pro vybrané účty nebo skupiny účtů • Automaticky, když heslo není synchronizované (heslo v bezpečném úložišti nesouhlasí s heslem na spravovaném systému) |  |
| Přístup k privilegovaným účtům – Řešení PAM umožňuje definovat vlastnosti přístupů k přihlašovacím údajům pro jednotlivé privilegované účty a pro skupiny privilegovaných účtů: • Přístup bez omezení – uživatel si může heslo zobrazit, zkopírovat a přímo se transparentně připojit k cílovému systému s využitím privilegovaného účtu • Dvojí kontrola – heslo nebo připojení je uživateli poskytnuto až po schválení přístupu schvalovatelem. Pro přístup k heslu se vytvoří žádost, generuje se automaticky emailová notifikace pro schvalovatele, nebo skupině schvalovatelů, kteří musí přístup/y schválit • Exkluzivní přístup: umožňuje využít privilegovaný účet pouze jedinou osobou v jeden čas – ostatní uživatelé nemají možnost přístupu k heslu  • Jednorázový přístup (one time password): po využití hesla řešení PAM vymění heslo privilegovanému účtu |  |
| Ověření správnosti hesel - Řešení PAM pro jednotlivé privilegované účty, nebo skupiny privilegovaných účtů ověřuje shodu hesla uloženého v bezpečném úložišti a na spravovaném systému (může být například změněno lokálně administrátorem): • Systém je sám schopný ověřit, jestli je heslo uložené v bezpečném úložišti stejné jako na koncovém systému • V případě, že je heslo na koncovém systému jiné, než v bezpečném úložišti, musí být řešení schopné danou událost zalogovat, vytvořit notifikaci a zajistit automatickou výměnu hesla za nové • Generuje report se všemi účty, kde jsou hesla jiná na spravovaných systémech a v bezpečném úložišti |  |
| Historie hesel - Řešení zaznamenává a uchovává historii hesel (například poslední tři hesla, nebo podle časového období) a umožňuje jednoduchý přístup k historii přes webové rozhraní. |  |
| Systém podporuje Single Sign On (SSO) pro privilegované účty, tedy možnost automaticky se přihlásit ke koncovému systému prostřednictvím privilegovaného účtu bez nutnosti zadávání hesla. Podporované jsou minimálně následující aplikace/protokoly:  • Windows RDP  • SSH (např. PuTTY) • HTTP(s)/Web aplikace  • Libovolný "tlustý klient pro aplikace instalované ve Windows prostředí |  |
| Během SSO je heslo automaticky zadané do aplikace na pozadí bez možnosti jeho odhalení. |  |
| Existuje mechanismus zajišťující bezpečný přístup k heslům uloženým v systému i v případě jeho částečné, nebo úplné nedostupnosti. |  |
| **Operační systémy** - Systém řízení privilegovaných účtů musí umožňovat měnit hesla, bez instalace agenta na koncový bod, pro privilegované účty v následujících Operačních systémech: - Microsoft a) Windows desktopové systémy od verze Windows 7 a vyšší b) Microsoft Windows serverové systémy Windows Server 2008 a vyšší c) podporované je řízení lokálních a doménových účtů prostřednictvím protokolů WMI, SSH, remote PowerShell - Linux - Red Hat, Ubuntu, Fedora, CentOS, Novell SUSE, Debian  - BSD  - VMware - ESX, ESXi Server - Apple - OS X - Citrix – XenServers  - Cisco – všechny OS - EMC - Unix d) Včetně systémů dodávaných v rámci plnění |  |
| **Adresářové služby** - Systém řízení privilegovaných účtů musí umožňovat bezagentsky řídit hesla pro privilegované účty v následujících Adresářových službách: - Microsoft Active Directory, Azure Active Directory |  |
| **Microsoft Windows Aplikace** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Windows aplikacích bez nutnosti instalace agenta na koncový bod: - Windows Services - Windows Scheduled Tasks - IIS Application Pool - IIS Directory Security - Windows Registry COM+ - Cluster Service   * SharePoint |  |
| **Aplikace** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Aplikacích bez nutnosti instalace agenta na koncový bod: HP desktop BIOS passwords - Cisco Call Manager   * Apache, nginx |  |
| **Databázové systémy** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Databázových systémech bez nutnosti instalace agenta na koncový bod: : - Oracle - Microsoft SQL Server - MySQL  - FireBird - Všechny ODBC kompatibilní databáze a hesla uložená v tabulkách |  |
| **SAAS a Webové stránky** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících SaaS službách a webových stránkách bez nutnosti instalace agenta na koncový bod: - Amazon Web Services - Microsoft Azure - Microsoft Office365 - Facebook - Google Gmail - Linkedin - Twitter - Pinterest  - SalesForce |  |
| **Bezpečnostní systémy** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Bezpečnostních systémech bez nutnosti instalace agenta na koncový bod: - Checkpoint Firewall, SPLAT, Provider, GAIA - Cisco PIX, ASA, IronPort, ISE - Juniper Netscreen - Fortinet FortiGate, FortiManager - BlueCoat Proxy SG, CAS, MAA - Palo Alto Panorama - IBM DataPower - SourceFire 3D - TippingPoint IPS, SMS - WatchGuard Firebox - Intel Security/McAfee ePolicy Orchestrator - Symantec Messaging Gateway - Safenet Luna HSM  - SEP manager |  |
| **Síťové zařízení** - Systém řízení privilegovaných účtů musí umožňovat řídit a měnit hesla pro privilegované účty v následujících Síťových zařízení bez nutnosti instalace agenta na koncový bod: - Cisco Router, ACS, Switch Catalyst, Nexus Switch, JMC, Wireless LAN Controller, WAAS, ONS - Juniper (JUNOS) - Nortel - Alcatel - F5 BigIP - HP ProCurve - 3com - Enterasys - Aruba - BlueCoat - Brocade  - Avaya - Radware |  |
| Automatické řízení privilegovaných účtů v těchto systémech musí být dodáno v rámci implementace a podporováno po dobu platnosti zakoupené licence řešení |  |
| Podporuje detekci SSH klíčů a mapování vztahů veřejného a soukromého SSH klíče používaného pro přihlášení k systémům. |  |
| Řešení podporuje reporting o stavu klíče, jako je jeho platnost, délka klíče apod. Zároveň identifikuje nesoulad s politikou. |  |
| Řešení musí bezpečně uchovávat SSH klíče v centrálním zabezpečeném úložišti a zároveň kontrolovat a řídit přístupy k těmto klíčům. |  |
| Řešení musí podporovat automatickou výměnu klíčů. Podporuje také rotaci páru SSH klíčů (výměnu privátního a veřejného klíče na cílovém zařízení). |  |
| Řešení musí spravovat a chránit SSH klíče, které jsou používané aplikacemi pro autentizaci. |  |
| Řešení umí posílat notifikace při použití vybraného SSH klíče. |  |
| Řešení zabezpečuje správu SSH klíčů a je integrováno do stejné infrastruktury jako zabezpečení privilegovaných účtů a hesel. |  |
| Nástroj umožňuje nahrávání privilegovaných relací v rámci celého počtu licencí. Minimálně ve formě:  a) textové relace (např. SSH, telnet)  b) relace prostřednictvím vzdálené plochy (např. RDP, VNC) |  |
| Nástroj umožňuje vyhledávat v nahraných relacích dle zadaných slov. |  |
| Nástroj umožňuje během privilegovaného přístupu oddělit prostředí klienta od cílového systému, pro zvýšení zabezpečení a minimalizaci rizika nákazy. Stejně tak je možné znemožnit kopírování informací a dat z cílového systému na klienta. |  |
| Nástroj umožňuje monitorovat aktivní relace jinou osobou, např. bezpečnostními správci, auditory apod. Včetně možnosti do aktivní relace zasáhnout. |  |