# Monitoring privilegovaných účtů (PAM)

Požaduje se dodání nástroje pro monitoring privilegovaných účtů (PAM). Pro účely výběrové řízení uvádíme vysvětlení pojmu PAM, který požadujeme.

PAM je systém řízení privilegovaných účtů. Pojmem privilegovaný účet pro tento účel označuje účet v informačním systému, který má vysoké oprávnění, tj. účty typu root v Linux/UNIX systémech, účty typu Administrátor ve Windows systémech, systémové účty používané aplikacemi nebo sdílené účty, které nejsou vázané na fyzickou osobu.

S těmito účty pracují privilegovaní uživatelé. Pojem privilegovaný uživatel označuje fyzickou osobu, která používá privilegované účty. Jedná se o pracovníky provozu, dodavatele, nebo vývojáře.

Jako cílový systém se označuje systém, na který se privilegovaný uživatel připojuje prostřednictvím privilegovaných účtů.

PAM zaznamenává činnost systémového administrátora, který přistupuje k citlivým datům anebo provádí konfigurační činnost. Systém vytváří auditní stopu. Auditní záznamy mohou být přehrávány jako video, takže je možné sledovat události přesně tak, jak se ve skutečnosti odehrály.

Požadujeme dodání licencí pro 140 monitorovaných systémů.   V rámci implementace bude systém nasazen primárně na monitorování serverové infrastruktury (Windows a Linux).

**Předpokládaný postup nasazení:**

* Zúčastněné osoby vytvoří seznam systémů a uživatelů, kterých se bude týkat nasazení řešení.
* Dodavatel připraví a dodá VM appliance ve formátu .ova, nebo ovf souborů.
* Odběratel provede deploy potřebného počtu VM.
* Zúčastněné osoby provedou finální konfiguraci VM (např. připojení VM do patřičné VLANy)
* Zúčastněné osoby provedou veškerou konfiguraci řešení pro podmínky nasazení nemocnici
* Zúčastněné osoby provedou nasazení řešení minimálně pro systémy typu Linux
* a typu Windows dle výběru objednatele.
* Zúčastněné osoby provedou nastavení systému pro odesílání událostí do systému SIEM a/nebo systému typu logmanagement provozovaném v rámci Kybernetického operačního centra JMK,
* Poskytovatel provede zaškolení pracovníků odběratele.
* Poskytovatel dodá kompletní dokumentaci řešení a nasazení u objednatele, kterou objednatel písemně odsouhlasí.

**Obecné vlastnosti poptávaného řešení**

V rámci výběrového řízení požadujeme dodání on-premise SW appliance, pro její provoz bude využito virtualizace. Nepožadujeme tedy dodání HW appliance. Appliance, musí existovat ve formě Virtual Appliance pro VMWARE prostředí.

Řešení musí podporovat zapojení pro High Availability, tj. vysoká dostupnost.

Požadujeme dodání systému, který bude pro stávající uživatele maximálně transparentní tzn. nemění současný systém práce privilegovaných uživatelů.

Řešení musí být schopné zaznamenávat a řídit přístupy privilegovaných uživatelů a v případě porušení nastavených pravidel o tomto informovat obsluhu.

Řešení musí být schopné vyhodnocovat nestandardní chování privilegované účtu.

**Záruka,implementace a maintenance**

**Maintenance musí být dostupná formou Service Desku v režimu 5 x 8, jehož provozní doba musí být min. od 8:00 do 16:00 v pracovní dny.**

Součástí dodávky je kompletní implementace včetně záruky a maintenance na 2 roky.

## Specifikace minimálních požadavků technického řešení

### Systém PAM – 1ks

|  |  |
| --- | --- |
| **ID** | **Technické požadavky** |
| PAM01 | Řešení musí být konfigurovatelné a ovládané přes webové GUI rozhraní. |
| PAM02 | Řešení musí být bezagentové a umožňuje implementaci jako síťové transparentní proxy.  Zároveň má možnost síťové netransparentní proxy implementace typu bastion |
| PAM03 | Řešení musí být nezávislé na verzi OS cílových serverů. |
| PAM04 | Řešení musí podporovat práci přes tyto protokoly:   * + Microsoft RDP   + Citrix ICA   + SSH/SCP   + VNC i z SSL   + TELNET i z SSL   + HTTP/S   + MS-SQL   + SUDO iolog |
| PAM05 | Řešení musí podporovat práci přes tyto protokoly:  •             Microsoft RDP  •             Citrix ICA  •             SSH/SCP  •             VNC i z SSL  •             TELNET i z SSL  •             HTTP/S  •             MS-SQL  •             SUDO iolog |
| PAM06 | Řešení v rámci daných protokolů rozlišuje jejich kanály (např. CLIPBOARD, REMOTE PRINTER, REMOTE DISK, atd.), u kterých je možné definovat:  •             Časové okna  •             Uživatelské skupiny  •             Rozsahy IP adres  •             Blokaci |
| PAM07 | Řešení musí být schopné detekovat pokusy o spuštění aplikace/příkazu a ukončit spojení uživatele. |
| PAM08 | Řešení musí být schopné zaznamenat použité příkazy, titulky oken a použité aplikace |
| PAM09 | Řešení musí být schopné analyzovat stisknuté klávesy a provádět behaviorální analýzu s cílem odhalit zneužití uživatelského účtu |
| PAM10 | Řešení musí být schopné detekovat použití neautorizovaných skriptů |
| PAM11 | Řešení má vestavěny mechanismus pro automatické skórování potencionálně rizikového chování privilegovaného uživatele (použití neobvyklé sekvence příkazů, odlišné chování při použití klávesnice a myši) |
| PAM12 | Řešení musí umožňovat tvorbu black listů a white listů. |
| PAM13 | Logování jak interních akcí, tak informací o „sessions“ pomocí syslog protokolu, podpora TLS nad syslog protokolem. |
| PAM14 | Řešení musí poskytovat indexaci pro rychlé vyhledávaní nejen informací o získaných „session“ dat, ale taky o jejich obsahu (taky nazývané content, nebo OCR indexace). |

|  |  |
| --- | --- |
| **ID** | **Požadavky na vlastnosti Auditní stopy** |
| PAM16 | Přehráváni jako video s přesnou časovou stopou ze signalizací „hluchých míst“ kde se nic neděje. |
| PAM17 | Šifrování auditní stopy. |
| PAM18 | TSA časové razítko. |
| PAM19 | Možnost přehrání online i offilne. |
| PAM20 | Možnost exportu dat v originální formátu. |

|  |  |
| --- | --- |
| **ID** | **Řízení přístupů „sessions“** |
| PAM21 | Řešení musí být schopné řídit přístupy v rámci „session“ dle ověření vůči LDAP/RADIUS. |
| PAM22 | Řešení podporuje režim „čtyř očí“. Tedy přístup k systému je možný, až po schválení další osobou. |
| PAM23 | Řešení podporuje integraci s externími programy typu LM, SIEM, ERPM, IDM. |
| PAM24 | API pro integraci s HelpDesk/ServiceDesk systémy. |

|  |  |
| --- | --- |
| **ID** | **Zálohování, Archivace, Export, Sdílení log dat** |
| PAM25 | Nezávislé zálohovací politiky jak pro konfiguraci/interní databázi, tak pro jednotlivé „sessions“.   * Podpora automatizovaného zálohování dat |
| PAM26 | Nezávislé archivační (data retention) politiky pro jednotlivé úložiště auditních dat.   * Podpora archivace na externí úložiště |
| PAM27 | Podpora exportu auditních stop a exportu strukturovaných metadat. |
| PAM28 | API pro integraci s HelpDesk/ServiceDesk systémy. |

|  |  |
| --- | --- |
| **ID** | **Požadavky na přístupy k samotnému systému:** |
| PAM29 | Podpora GROUP managementu. |
| PAM30 | Podpora autentizace přes   * RADIUS * MS AD * Kerberos * X.509 |
| PAM31 | Podpora lokální /externí databáze uživatelů – LDAP. |

|  |  |
| --- | --- |
| **ID** | **Požadavky na možnosti reportingu** |
| PAM32 | Dashboardy/Statistiky o „sessions“. |
| PAM33 | Uživatelsky konfigurovatelný reporting strukturovaných dat. |
| PAM34 | Možnost tvorby vlastních reportů nad content informacemi. |
| PAM35 | API pro reporting do externích SW. |
| PAM36 | Řešení umožňuje Full text search |
| PAM37 | Možnost exportovat report do CSV, JSON. |
| PAM38 | Možnost reporty vytisknout. |
| PAM39 | Možnost definovat přístupy k reportům pro konkrétní uživatele. |