

## **C) SPECIFIKACIJA ZAHTEV NAROČNIKA - popravek**

### **Predmet javnega naročila: Zakup programske rešitve PAM**

Access Management (PAM)

#### **1. Namen in cilj**

Ponujena rešitev PAM mora omogočati centralizirano, varno in sledljivo upravljanje privilegiranih računov IT okoljih. Cilj je zmanjšati napadalno površino, uveljaviti načelo najmanjših privilegijev, nadzorovati privilegirane seje ter zagotoviti skladnost z internimi in regulativnimi zahtevami.

#### **2. Funkcionalne zahteve**

##### **2.1. Upravljanje Privilegijev Sej (PSM)**

- Rešitev mora delovati v načinu PROXY, brez potrebe po nameščanju agentov na ciljne sisteme.
- Rešitev mora zagotavljati snemanje in revizijo privilegiranih sej do strežnikov Windows in Linux, mrežnih naprav (stikala, požarne pregrade, itd) in drugih naprav po protokolih SSH, RDP, HTTP/HTTPS, VNC, Telnet, z možnostjo predvajanja in iskanja po metapodatkih.
- Rešitev mora zagotavljati izvedbo sej preko posredniškega strežnika (proxy), z zaščito dejanskih poverilnic.
- Rešitev mora zagotavljati shranjevanje vseh posnetkov sej in revizijskih podatkov v varni obliki.
- Rešitev mora zagotavljati podporo za realno-časovni nadzor sej ter možnost prekinitve aktivne seje.
- Zagotovljena mora biti podpora za oblačna okolja: AWS, Azure, GCP ter virtualne platforme (KVM, VMware, Hyper-V, OpenStack).
- Delovanje v obliki namenske strojne naprave s programsko opremo ali virtualne izvedenke z enim dobaviteljem odgovornim za celoten sistem (OS + aplikacija).
- Zagotavljati mora izvirno podporo protokolom SSH in RDP do Proxy in SSH/TELNET/RLOGIN/RDP/VNC od PROXY do zaščitenih sistemov.
- Podpora določanju uporabniških profilov (administrator, uporabnik, revizor) ter določitvi dostopnih pravic.
- Možnost omejevanja pravic revizorja samo na izbrane posnetke sej in ciljne sisteme.
- Možnost samodejne prekinitve seje, ki se omejuje z naborom prepovedanih aktivnosti
- **Določanje ACL-jev po ponornih IP-jih ali FQDN-ju.**
- Določanje ciljnih sistemov po IP-ju, DNS-u ali naslovu omrežnega razreda.
- Predogled posnetkov sej kot video zapis + metapodatki + prikaz za SSH.
- Dostop do sej preko spletnega portala (HTML5), brez vtičnikov.
- Integracija z Microsoft Active Directory (brez potrebe po sinhronizaciji uporabniških podatkov).
- Avtentikacija uporabnikov s poverilnicami (AD/LDAP), geslom ali certifikatom.

## 2.2. Upravitelj gesel

- Centralizirano varno shranjevanje privilegiranih gesel in SSH ključev.
- Samodejno menjavanje gesel in ključev na podprtih ciljnih sistemih.
- Določanje urnikov menjave gesel.
- Določanje pravilnikov gesel (dolžina, kompleksnost, posebni znaki, izključeni znaki).
- Nastavitev različnih politik za različne skupine sistemov.
- Ustvarjanje enkratnih gesel (OTP) in rotacijo po uporabi.
- Podpora za menjavo gesel preko REST API.

## 2.3. Portal Access Manager

- Omogočanje dostopa do SSH in RDP sej preko HTML5 spletnega brskalnika brez dodatnih vtičnikov.
- Podpora glavnim brskalnikom (Edge, Chrome, Firefox).
- Globalno iskanje po metapodatkih posnetih sej.
- Dobavljivost za Windows Server ali Linux platforme, ki so podprte v Core licenciranju.
- Podpora avtentikaciji preko AD in LDAP.
- Možnost zagona več instanc portala (dostopni portal + revizijski portal).

Tehnična rešitev mora omogočati dostop za:

- **najmanj dvesto (200) naprav ali najmanj štiri tisoč (4000) uporabnikov – ponudi se lahko kakršnakoli licenca, ki to pokrije in**
- **vkjučeno licenčnino za pripadajočo programsko opremo za obdobje 12 mesecev**

## 3. Tehnična podpora

- Podpora dobavitelja najmanj 12 mesecev.
- Razpoložljivost tehnične podpore v rednem delovnem času od 8:00 do 16:00 od ponedeljka do petka.
- Odzivni čas največ 4 ure
- Odpiranje incidentov preko portala in telefona.
- Neomejeno število incidentov.