# Technická specifikace – Část 5 Aktivita 3 Nástroj pro správu privilegovaných účtů

Obsah

[Popis požadavků na řešení 3](#_Toc197344347)

[a) architektura a řízení přístupů 3](#_Toc197344348)

[b) zabezpečení a správa přihlašovacích údajů 5](#_Toc197344349)

[c) licencování 5](#_Toc197344350)

[d) podpora 5](#_Toc197344351)

# Popis požadavků na řešení

## architektura a řízení přístupů

1. Nástroj bude dodáván jako fully packaged software (obsahuje i OS) s podporou pro virtuální prostředí jako Hyper-V/VMWARE či možností instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure). Možnost instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure).
2. Podpora instalace v režimu vysoké dostupnosti.
3. Systém dokáže fungovat jako jednotný přístupový bod pro několik instancí v necentralizované infrastruktuře.
4. Nástroj bude fungovat jako přístupová proxy.
5. Nástroj bude podporovat protokoly SSH a RDP protokoly pro primární spojení, tedy mezi privilegovaným účtem a proxy.
6. Nástroj bude podporovat protokoly SSH, RDP, VNC, RLOGIN a TELNET pro sekundární spojení, tedy mezi proxy a monitorovaným systémem.
7. Nástroj u nepodporovaných protokolů umožní spuštění klientské aplikace na Jump serveru tak, aby uživateli byla přístupná pouze daná klientská aplikace.
8. Nástroj podpoří integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory/RADIUS/KERBEROS/TACACS+
9. Nástroj podpoří integraci se SIEM/SYSLOG.
10. Nástroj nevyžaduje žádné instalace software agentů na monitorovaný systém.
11. Nástroj podpoří integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory/RADIUS/KERBEROS/TACACS+
12. Nástroj umožní uživatelskou autentizaci pomocí jména / hesla, X.509 certifikátu či SSH klíče.
13. Integrace nástroje s LDAP či Active Directory bude závislet na periodických synchronizacích. Systém mapuje schémata uživatelských skupin z LDAP/AD do lokálních PAM skupin.
14. Nástroj umožní tvorbu účtů s rozdílnými rolemi – minimálně správce, uživatel a auditor.
15. Nástroj umožní definici uživatelů, spravovaných zařízení a jejich skupin, u kterých bude jednotlivým auditorským účtům uděleno oprávnění prohlížet záznamy.
16. Nástroj umožní konfigurace uživatelských profilů se zahrnutím možnosti filtrovat příchozí připojení na základě zdrojové IP adresy, síťové adresy a masky sítě či FQDN.
17. Nástroj umožní definování cílových systémů zadáním IP adresy, DNS nebo zadáním IP adresy a masky.
18. Nástroj umožní definování přístupových politik přiřazováním uživatelských účtů či skupin k cílovým systémům či jejich skupinám.
19. Nástroj podporuje integraci s ICAP pro kontrolu průchozích souborů prostřednictvím antiviru či DLP s možností blokace nežádoucích přenosů.
20. Nástroj umožní zaznamenávání všech zprostředkovaných relací formou videozáznamu s doplňujícími metadaty.
21. Nástroj umožní aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin.
22. Nástroj umožní shlédnutí záznamů relací prostřednictvím webového rozhraní.
23. Nástroj umožní následný export videozáznamu do běžně podporovaného typu souboru (.mp4 či .flv)
24. Nastroj umožní ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS.
25. Nástroj zaznamenává a uchovává všechny uživatelem zadané příkazy v průběhu SSH a RDP relací.
26. Nástroj zaznamenává a uchovává názvy všech oken a procesů otevřených v průběhu RDP relace.
27. Nástroj umožní sběr metadata v průběhu RDP relace alespoň v rozsahu:

1. Změna aktivního okna. 2. Operace s tlačítkem v okně. 3. Volba na radio buttonu či check boxu v okně. 4. Změna obsahu textového pole v okně. 5. Změna rozložení kláves. 6. Začátky a ukončení procesů. 7. Manipulace se soubory prostřednictvím clipboardu.

8. Manipulace se soubory prostřednictvím přesměrovaných lokálních diskových jednotek.

1. Nástroj umožní blokace všech či vybraných TCP spojení zahájených z monitorovaného RDP serveru za účelem navázání neautorizovaných spojení.
2. Nástroj umožní blokování vybraných procesů na systémech Windows Server.
3. Nástroj u relací SSH a RDP umožní definovat vzory regulárních výrazů pro prováděné příkazy, a pokud je takový vzor detekován, umožní nastavit jednu z akcí: ukončení relace nebo odeslání oznámení o detekci vzoru.
4. Nástroj umožní přiřazení definovaných vzorů k monitoringu / ukončování relací k vybraným skupinám uživatelů či systémů.
5. Nástroj poskytuje ochranu hesel zadávaných v průběhu RDP relace prostřednictvím detekce vstupu kurzoru do pole pro vyplnění hesla či UAC (User Account Control) okna.
6. Nástroj umožní schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu:

1. Privilegovaný uživatel požádá o přístup

2. Definovaní uživatelé obdrží žádost o schválení přístupu.

3. Minimální definovaný počet uživatelů schválí žádost.

4. Privilegovaný uživatel po schvalovacím procesu automaticky získá přístup k monitorovanému systému."

1. Nástroj umožní vyžadování výše uvedených schvalování v určitých časových rámcích- např. Pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení.
2. Správce nástroje/auditor má možnost pozorovat probíhající relace v reálném čase, včetně možnosti pozorovanou relaci ukončit.
3. Při auditu či kontrole proběhlé relace má nástroj možnost zobrazit metadata a videozáznam relace na jedné stránce s časovou osou propojující metadata s vizuální reprezentací.
4. Nástroj dokáže pracovat se sdílenými účty s možností určení, kdo v daný moment tento účet využíval.
5. Nástroj poskytne různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně:
   1. Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na proxy.
   2. Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet).
   3. Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání.
6. Nástroj umožní vyhledávání systémů a privilegovaných účtů formou scanování RDP + SSH portů a importů z AD.
7. Nástroj disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů.
8. Nástroj lze rozšířit o modul umožňující centralizaci přístupu k několika odděleným instancím prostřednictvím jednotného webového HTML5 rozhraní s integrovaným RDP a SSH klientem pro primární spojení.
9. Modul pro centralizaci přístupů podporuje prohlížeče Internet Explorer, Microsoft Edge, Google Chrome a Mozilla Firefox bez potřeby instalace pluginů (java, flash)
10. Modul pro centralizaci přístupů je dodán jako aplikace běžící na jednom z těchto OS: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016 (x64), Red Hat Enterprise Linux, CentOS 6.6, Red Hat Entreprise Linux, CentOS 7.1, Debian 8 (amd64).
11. Modul pro centralizaci přístupů umožní auditorským účtům globální vyhledávání napříč metadaty ze všech realizovaných relací všech instancí nástroje.
12. Technologie umožní automatické rotace hesel a SSH klíčů.
13. Technologie umožní vytvářet různé plány automatické změny hesel a SSH klíčů na cílových systémech.
14. Technologie podporuje přístup pomocí jednorázových hesel s omezenou platností pro RDP a SSH relace
15. Technologie podporuje vlastní zásady/požadavky na změnu hesla:

* Požadovaný minimální počet znaků,
* Vyloučení znaků určených správcem,
* Povinná velká a malá písmena,
* Požadované speciální znaky

1. Technologie umožní nastavit různé zásady změny hesla pro různé skupiny hostů nebo skupiny účtů.
2. Technologie umožní nastavení délky platnosti hesla.
3. Technologie umožní zavedení modulů pro změnu hesel a SSH klíčů pro nativně nepodporované systémy

## zabezpečení a správa přihlašovacích údajů

1. Nástroj se shoduje se standardy ISO 27001, HIPAA, SOX a PCI-DSS.
2. Nástroj bezpečně ukládá citlivá data včetně šifrování hesel pomocí AES 256.
3. Nástroj bezpečně spravuje a distribuuje SSH klíče.
4. Nástroj umožní automaticky měnit hesla a SSH klíče pro specifické systémy či skupiny účtů.
5. Nástroj umožní definovat výjimky pro zamezení automatických rotací hesel a SSH klíčů u určitých účtů.
6. Nástroj umožní definovat časové intervaly pro provádění automatizovaných změn hesel a SSH klíčů.
7. Nástroj umožní iniciovat změnu hesel a SSH klíčů po každém odhlášení.
8. Nástroj umožní definovat komplexitu generovaných hesel dle počtu znaků, využití malých / velkých písmen a speciálních znaků.
9. Nástroj nativně podpoří změny hesel u těchto systémů: AIX, F5 BIG IP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix, Micorsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto PA-500, Grafana.
10. Nástroj musí umožňovat změnu hesel pomocí REST API.

## licencování

1. Nástroj pochází z oficiálního distribučního kanálu výrobce zemích EU.
2. Licencování nástroje není omezeno na počet jeho instancí nasazených v infrastruktuře uživatele.
3. Licence pro minimálně 100 cílových bodů (serverů), základní verze bez omezení počtu uživatelů a současných připojení
4. Licence pro minimálně 6 administrátorů s centralizovaným portálovým přístupem.

## d) podpora

1. Zajištění fyzického a vzdáleného šifrovaného přístupu do kompetenčního centra na území ČR, kde budou předinstalovaný provozované bezpečnostní systémy zadavatele, včetně příslušných reportovacích nástrojů, a kde bude možné minimálně ověřit funkčnost nových verzí, simulovat problémy produkčního prostředí a řešit další rozvoj bezpečnostního perimetru zadavatele.
2. Podpora výrobce min 8:00-17:00 v pracovní dny
3. Záruka na celé řešení dva roky od implementace.