



## VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE

### NÁZEV VEŘEJNÉ ZAKÁZKY

### MODERNIZACE ICT PRO ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI - PROJEKT SECURITY ČÁST B – SYSTÉMY PRO OCHRANU INFRASTRUKTURY A ZAŘÍZENÍ ČÁST C – OPATŘENÍ A NÁSTROJE PRO OCHRANU KLÍČOVÝCH SYSTÉMŮ

SPISOVÁ ZNAČKA:	CN/130/CN/24	ČÍSLO JEDNACÍ:	3944/24/CN	SYSTÉMOVÉ ČÍSLO VZ:	P24V00000461 P24V00000462
ODKAZ E-ZAK:	<a href="https://ezak.cnpk.cz/vz00011501">https://ezak.cnpk.cz/vz00011501</a> , <a href="https://ezak.cnpk.cz/vz00011502">https://ezak.cnpk.cz/vz00011502</a>				
ZADAVATEL:	Klatovská nemocnice, a.s.				
SÍDLO:	Plzeňská 929, 339 01 Klatovy	IČO:	26360527		
STATUTÁRNÍ ZÁSTUPCE:	Ing. Zdeněk Švanda, předseda představenstva Ing. Ondřej Provalil, MBA - člen představenstva				
ADMINISTRÁTOR:	Centrální nákup Plzeňského kraje, příspěvková organizace				
SÍDLO:	Vejpřnická 663/56, 318 00 Plzeň	IČO:	72046635		
STATUTÁRNÍ ZÁSTUPCE:	Mgr. Bc. Jana Dubcová, ředitelka				
POVĚŘENÁ OSOBA:	Jan Krondák	E-MAIL:	<a href="mailto:jan.krondak@cnpk.cz">jan.krondak@cnpk.cz</a>		
DRUH VZ:	dodávky	REŽIM VZ:	nadlimitní	DRUH ŘÍZENÍ:	otevřené
FINANCOVÁNO Z EU:	IROP 2021 – 2027, REACT-EU: CZ.06.01.01/00/22_004/0000089 CZ.06.01.01/00/22_004/0000091 CZ.06.01.01/00/22_004/0000092 CZ.06.01.01/00/22_004/0000095				

Zadavatel poskytuje prostřednictvím administrátora v souladu s § 98 a § 99 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále „ZZVZ“), vysvětlení zadávací dokumentace k výše uvedené veřejné zakázce.

Dne 13. 9. 2024 byla doručena žádost o vysvětlení zadávací dokumentace od dodavatele, na kterou zadavatel tímto odpovídá.

#### **Dotazy k části B - SYSTÉMY PRO OCHRANU INFRASTRUKTURY A ZAŘÍZENÍ:**

Zadavatel v dokumentu Příloha\_2 - Technická\_specifikaceKB\_Security.pdf v sekci 3 Část B – Systémy pro ochranu infrastruktury a zařízení, konkrétně 3.1. Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech uvedl technickou specifikaci pro tuto část, přičemž:

1. Zadavatel neuvádí počet serverů (Windows Servers, Linux) a počet koncových stanic (Windows 10, 11, macOS). Tohle rozdělení je nutné pro správné nacenění licencí EDR. Prosíme Zadavatele o specifikaci počtu serverů a koncových stanic z celkového počtu 1610 zařízení.
2. Povoluje Zadavatel pro některé technologie MSSP licence nebo chce výhradně klasické resell licence, které budou v jeho vlastnictví?
3. Zadavatel uvádí v Technické specifikaci, v části Licenční pokrytí požadavek na 60 dní retence telemetrických dat, ale v části EDR funkce požadavek na 30 dní retence telemetrických dat. Prosíme Zadavatele o specifikaci, který ze dvou požadavků je správný.

**Odpověď zadavatele:**

Bod 1) Zadavatel provozuje 220 serverů a 1390 koncových stanic.

Bod 2) Zadavatel požaduje klasické „resell“ licence, které budou v jeho vlastnictví.

Bod 3) Správně je 60 dní retence telemetrických dat.

**Dotazy k části C - OPATŘENÍ A NÁSTROJE PRO OCHRANU KLÍČOVÝCH SYSTÉMŮ:**

Zadavatel v dokumentu Příloha\_2 - Technická\_specifikaceKB\_Security.pdf v sekci 4 Část C – Opatření a nástroje pro ochranu klíčových systémů, konkrétně 4.1. Nástroj pro detekci zranitelnosti a hardeningové politiky uvedl technickou specifikaci pro tuto část, přičemž:

4. Zadavatel uvádí požadavek na vytvoření hardeningových politik pro uvedené platformy. Může Zadavatel upřesnit verze níže uvedených platform, které v TS nejsou specifikovány?

Red Hat Enterprise Linux  
CentOS  
Rocky Linux  
VMware vCenter  
VMware ESXi  
Check Point NGFW

Zadavatel v dokumentu Příloha\_2 - Technická\_specifikaceKB\_Security.pdf v sekci 4 Část C – Opatření a nástroje pro ochranu klíčových systémů, konkrétně 4.2. Systém pro správu a monitoring administrátorských přístupů uvedl technickou specifikaci pro tuto část, přičemž:

5. Zadavatel uvádí v rozsahu implementace nástroje Systém pro správu a monitoring administrátorských přístupů následující: „Načítání všech privilegovaných účtů a zařízení na platformách Windows, Linux, databáze, síťová zařízení, bezpečnostní technologie a automatizace vyhledávání zařízení / účtů a jejich automatické členění do skupin dle sítí a účelu zařízení / účtů.“ Prosíme Zadavatele o specifikaci konkrétních platform a verzí, které mají být onboardovány do nástroje (např. MS SQL Server 2019, Cisco síťové prvky, Check Point NGFW R81 apod.).

Zadavatel v dokumentu Příloha\_2 - Technická\_specifikaceKB\_Security.pdf v sekci 4 Část C – Opatření a nástroje pro ochranu klíčových systémů, konkrétně 4.3. Systém pro vzdálený privilegovaný přístup uvedl technickou specifikaci pro tuto část, přičemž:

6. Zadavatel neuvádí, jaké systémy (platformy a verze) chce onboardovat do nástroje Systém pro vzdálený privilegovaný přístup. Prosíme Zadavatele, aby tyto platformy a verze specifikoval.

**Odpověď zadavatele:**

Bod 4) Zadavatel používá tyto platformy:

CentOS 7  
VMware esxi 5.5, 6.0, 6.7, 8.0.2  
Redhat 8.3  
Rocky Linux 8.1, 8.10, 9.2, 9.3, 9.4,  
Ubuntu 14.04.5, 18.04.2, 20.04.3, 20.04.2, 22.04.3, 22.04.4  
VMware vCenter 6.7, 8.0.2  
Check Point Gaia R81.20 631  
ArubaOS 8.10

Bod 5) Zadavatel bude požadovat nastavení pro tyto platformy a verze:

Windows Server 2012 (AD i lokální účty, přístup přes RDP)  
Windows Server 2012r2 (AD i lokální účty, přístup přes RDP)  
Windows Server 2016 (AD i lokální účty, přístup přes RDP)  
Windows Server 2019 (AD i lokální účty, přístup přes RDP)  
Windows Server 2022 (AD i lokální účty, přístup přes RDP)  
Ubuntu 14.04.5 (lokální účty, přístup přes ssh konzoli)  
Ubuntu 18.04.2 (lokální účty, přístup přes ssh konzoli)  
Ubuntu 20.04.2 (lokální účty, přístup přes ssh konzoli)  
Ubuntu 20.04.3 (lokální účty, přístup přes ssh konzoli)  
Rocky Linux 8.10 (lokální účty, přístup přes ssh konzoli)  
Rocky Linux 9.4 (lokální účty, přístup přes ssh konzoli)  
VMWARE vCenter 8.0.2 (lokální účty, webová konzole)  
Veeam 12 (lokální účty, RDP, klient)  
Firebird 2.5 (lokální účty, přístup z aplikace)  
MS SQL standard 2019 (lokální účty, přístup z aplikace nebo SQL Mng. studia)  
MS SQL full standard 2019 (lokální účty, přístup z aplikace nebo SQL Mng. studia)  
MS SQL standard 2017 (lokální účty, přístup z aplikace nebo SQL Mng. studia)  
MS SQL standard 2016 (lokální účty, přístup z aplikace nebo SQL Mng. studia)  
MS SQL express (lokální účty, přístup z aplikace nebo SQL Mng. studia)  
Oracle 11g (lokální účty, přístup z aplikace nebo Oracle SQL developer)  
Oracle 19c patch 19.22 (lokální účty, přístup z aplikace nebo Oracle SQL developer)  
MS SQL 2008 (lokální účty, přístup z aplikace nebo SQL Mng. studia)  
Aruba NetEdit 2.12.0 (lokální účty, přístup přes webovou konzoli)  
Check Point R81.20 (lokální účty, přístup přes SSH a klienta Smart Console)  
Webový aplikační firewall (lokální i AD účty, přístup přes SSH a webovou konzoli)  
Systém pro vyhodnocování a správu logů (lokální i AD účty, přístup přes SSH a webovou konzoli)

Bod 6) Zadavatel bude požadovat nastavení pro tyto platformy a verze:

Windows Server 2012 (AD i lokální účty, přístup přes VPN a RDP)  
Windows Server 2012r2 (AD i lokální účty, přístup přes VPN a RDP)  
Windows Server 2016 (AD i lokální účty, přístup přes VPN a RDP)  
Windows Server 2019 (AD i lokální účty, přístup přes VPN a RDP)  
Windows Server 2022 (AD i lokální účty, přístup přes VPN a RDP)  
Ubuntu 14.04.5 (lokální účty, přístup přes VPN a ssh konzoli)  
Ubuntu 18.04.2 (lokální účty, přístup přes VPN a ssh konzoli)  
Ubuntu 20.04.2 (lokální účty, přístup přes VPN a ssh konzoli)  
Ubuntu 20.04.3 (lokální účty, přístup přes VPN a ssh konzoli)  
Rocky Linux 8.10 (lokální účty, přístup přes VPN a ssh konzoli)  
Rocky Linux 9.4 (lokální účty, přístup přes VPN a ssh konzoli)  
VMWARE vCenter 8.0.2 (lokální účty, VPN, webová konzole)  
Veeam 12 (lokální účty, VPN, RDP, klient)  
MS SQL std 2019 (lokální účty, přístup z aplikace nebo SQL Mng. studia přes VPN)  
MS SQL full std 2019 (lokální účty, přístup z aplikace nebo SQL Mng. studia přes VPN)  
MS SQL std 2017 (lokální účty, přístup z aplikace nebo SQL Mng. studia přes VPN)  
MS SQL std 2016 (lokální účty, přístup z aplikace nebo SQL Mng. studia přes VPN)  
MS SQL express (lokální účty, přístup z aplikace nebo SQL Mng. studia přes VPN)  
Oracle 11g (lokální účty, přístup z aplikace nebo Oracle SQL developer přes VPN)  
Oracle 19c patch 19.22 (lokální účty, přístup z aplikace nebo Oracle SQL developer přes VPN)  
MS SQL 2008 (lokální účty, přístup z aplikace nebo SQL Mng. studia přes VPN)  
Aruba NetEdit 2.12.0 (lokální účty, VPN a přístup přes webovou konzoli)

Check Point R81 (lokální účty, přístup přes SSH a klienta Smart Console)  
Webový aplikační firewall (lokální i AD účty, přístup přes SSH a webovou konzoli)  
Systém pro vyhodnocování a správu logů (lokální i AD účty, přístup přes SSH a webovou konzoli)

**Upozornění:**

Vzhledem k obsahu vysvětlení zadávací dokumentace zadavatel **prodlužuje** lhůtu pro podání nabídek pro **části B a C do 11. 10. 2024 do 10:00 hodin.**

V Plzni

**Jan Krondák**  
administrátor  
Centrální nákup Plzeňského kraje,  
příspěvková organizace  
v zastoupení Zadavatele