

## Zvýšenie úrovne informačnej a kybernetickej bezpečnosti ÚJD SR

Otázka	Dokument/Kapitola	Znenie otázky	Odpoveď
1	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aký je predpokladaný počet obrazov pre inštaláciu Windows OS?	Aktuálna a predchádzajúca verzia operačného systému Windows 10 alebo jeho nasledovníka.
2	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aký je počet unikátnych hardvérových klientskych zariadení, pre ktoré bude vytváraný balíček aktualizácie ovládačov?	Toto sa mení v čase, 10 - 15 rôznych modelov.
3	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	V prípade viacerých lokalít, je požadované vytvorenie distribučného bodu pre dané lokality?	Áno, na pracovisku v Trnave, nakoľko sa tu nachádza väčší počet klientov.
4	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Sú všetky požadované zariadenia na manažment zaradené v Active Directory?	Centrálny manažment PC v rámci tohto projektu sa týka zariadení, ktoré sú zaradené v Active Directory.
5	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Majú byť súčasťou dodávky aj licencie Windows Server user CAL?	Pokiaľ ich vaše riešenie požaduje, treba ich dodať. Riešenie musí byť plne licencované.
6	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aké sú aktuálne používané verzie OS na klientskych stanicích?	Aktuálna a predchádzajúca verzia operačného systému Windows 10 alebo jeho nasledovníka.
7	Príloha č.15 - 1.1 Centrálny manažment PC Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aké sú aktuálne používané verzie OS na serveroch?	Windows Server 2012R2 a novšie, s výhľadom na rok 2023: Windows Server 2016 -2022; Centos podporované verzie podľa "výrobcu" daného OS, podľa EOL definície (príklad: Centos 8 nie: EOL 31.12.2021, Centos 7 áno: EOL 30.6.2024).
8	Príloha č. 15 - 1.2.2 Zálohovací softvér pre zálohovanie samostatných serverov a pracovných staníc používateľov Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aké verzie týchto Vami spomenutých Linux distribúcií a databázových serverov má zálohovací softvér podporovať ? - Linux (Red Hat, CentOS, Fedora, Ubuntu, Debian, SUSE, ClearOS) - Microsoft SQL server -Oracle DB	Vždy aktuálne podporované verzie podľa "výrobcu" daného OS, podľa EOL definície (príklad: Centos 8 nie: EOL 31.12.2021, Centos 7 áno: EOL 30.6.2024).
9	Príloha č. 15 - 1.2.2 Zálohovací softvér pre zálohovanie samostatných serverov a pracovných staníc používateľov V kapitole sa spomína "V rámci predmetu dodávky je požadované zálohovanie pracovných staníc v počte 200 ks"	V dokumente xls "Príloha č.12 Štruktúrovaný rozpočet pre časť č. 1", chýba riadok pre túto položku. Je v tabuľke položka kde by bolo možné zachytiť relevantné náklady ?	Náklady je potrebné zahrnúť do položky "Zálohovací softvér pre zálohovanie samostatných serverov a <b>pracovných staníc používateľov</b> ".
10	Príloha č.15 - 1.2.3 Pásková knižnica a zálohovacie médiá V kapitole v časti "Pripojenie" je uvedená špecifikácia "Minimálne 16Gbit/s Fibre channel pre každú mechaniku Ethernet RJ-45 pre vzdialenú správu"	LTO technológie však aktuálne disponujú len 8Gbit/s rýchlosťou. Ide o možný omyl?	K uvedenej otázke už bola daná odpoveď v systéme JOSEPHINE.
11	Príloha č. 15 - 1.2.4 Diskové pole pre ukladanie záloh V kapitole je uvedená "Požadujeme pripojenie pomocou Fibre Channel, minimálne 16 Gbit/s+B55"	Ako bude pripojené diskové pole na zálohovací server cez FC v druhej lokalite , keď sa SAN prepínače pre virtualizačnú platformu obstarávajú len do primárnej lokality ?	Bude pripojené napriamo, bez SAN switcha.
12	Príloha č.15 - 1.3.4 Firewall vrátane analytických a manažment nástrojov V kapitole v časti "Funkcie antivírovej kontroly" je uvedená "AV kontrola s možnosťou rozšírenia o inšpekciu tzv. sandbox technikou."	Sandbox technika ma byť zahrnutá v licenciách pre navrhované riešenie ?	Požadujeme ako možnosť pre budúce rozšírenie.
13	Príloha č. 15 - 1.3.4 Firewall vrátane analytických a manažment nástrojov V kapitole je uvedená "Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky."	Predpokladáte nasadenie firewallu v HA režime v móde Active / Active ? Majú byť fw systémy nainštalované v samostatných rozdielnych DC ? Sú dátové centra navzájom prepojené cez linkovú ( L2 ) vrstvu ? Aká je očakávaná sieťová priepustnosť medzi dátovými centrami ? Mate špecifické požiadavky na sieťové zapojenie napr. tip a rozhranie použitých sieťových transceiverov ? Predpokladáte zapojenie LAN / WAN cez 10 Gbps sieťové rozhranie ? Má byť realizované zapojenie WAN ( Internetu ) cez externý switch alebo budú zariadenia zapojene priamo do WAN routerov ?	Návrh architektúry spracuje dodávateľ ako súčasť riešenia. FW budú umiestnené v jednej lokalite. Požadované porty sú uvedené v technickej špecifikácii.
14	Príloha č. 15 - 1.3.4 Firewall vrátane analytických a manažment nástrojov Podpora virtualizácie FW na danom HW. Každý virtuálny FW musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politik, smerovania a pod.	Plánujete používať viac ako 10 virtuálnych FW ?	Návrh architektúry spracuje dodávateľ ako súčasť riešenia.
15	Príloha č. 15 - 1.3.4 Firewall vrátane analytických a manažment nástrojov V kapitole je uvedený počet FW pravidiel - Min. 8000	Očakávate migráciu konfigurácie zo súčasných nastavení alebo sa jedna o úplne nové riešenie ?	Očakávame vytvorenie novej konfigurácie so zapracovaním aktuálnych požiadaviek a pravidiel.

16	Príloha č.15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že riešenie musí umožňovať spojiť prevenciu zaznamenaných hrozieb, kontrolu webového obsahu a prevenciu straty údajov s adresou IP, menom používateľa a kategóriou prístupu na webovú stránku.	Má byť spojenie realizované priamo na webovej bráne v reportoch alebo sa majú uvedené hrozby spojiť v externom systéme?	Návrh architektúry spracuje dodávateľ ako súčasť riešenia.
17	Príloha č.15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že riešenie musí podporovať centralizovanú správu a vykazovanie na viacerých lokalitách vrátane vzdialených používateľov, ktorí sa nenachádzajú v žiadnej z interných sietí.	Prosíme o upresnenie významu "vykazovanie na viacerých lokalitách vrátane vzdialených používateľov" ?	Zmyslom požiadavky je mať možnosť zabezpečiť uplatnenie politik aj pre vzdialených používateľov, ktorí sa nenachádzajú v žiadnej z interných sietí, a to napríklad hybridným riešením on-premises a cloud.
18	Príloha č.15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že riešenie musí detegovať a blokovať odchádzajúcu komunikáciu škodlivého softvéru typu Botnet a Trojan z infikovaných systémov. Systém sa musí prihlásiť a poskytnúť podrobné informácie o pôvodnom systéme dostatočné na to, aby umožnil identifikáciu infikovaných jednotiek na mitigáciu.	Prosíme u presnenie druhej vety "Systém sa musí prihlásiť a poskytnúť podrobné informácie o pôvodnom systéme dostatočné na to, aby umožnil identifikáciu infikovaných jednotiek na mitigáciu." Kam sa ma systém prihlásiť ?	V zmysle technickej špecifikácie; požiadavka smeruje k identifikácii infikovaných jednotiek na mitigáciu.
19	Príloha č.15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že riešenie musí byť schopné zvládnuť riadenie niekoľkých pripojení. V prípade potreby musia byť k dispozícii bezplatné inštancie virtuálneho zariadenia (virtual appliance).	Prosíme o upresnenie významu "riadenie niekoľkých pripojení" ?	Návrh architektúry spracuje dodávateľ ako súčasť riešenia.
20	Príloha č. 15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že riešenie musí umožniť nahlásiť každú použitú cloudovú aplikáciu a nahlásiť rizikové skóre danej aplikácie s popisom (min. 3 000 aplikácií).	Pod významom nahlásiť sú myslené notifikácie o komunikácii? V prípade ak je myslené niečo iné prosíme o upresnenie.	Áno, ide aj, ale nielen iba, o notifikáciu.
21	Príloha č. 15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že riešenie musí podporovať možnosti mobilného zabezpečenia umožňujúceho ochranu používateľov, keď sa nachádzajú mimo hlavnej siete.	V prípade mobilného zabezpečenia sú myslené pracovne stanice alebo aj mobilné zariadenia ?	Aj mobilné zariadenie.
22	Príloha č. 15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že HW záruka výrobcu so servisom najbližší pracovný deň v mieste inštalácie (okamžitá výmena - poskytnutie náhradného hardvéru nasledujúci pracovný deň po uznaní chyby suportom výrobcu).	Je vyžadované aby servis a podpora boli realizované priamo výrobcom alebo to môže byť aj implementátor riešenia ?	Nie, ale požaduje sa HW záruka výrobcu v zmysle technickej špecifikácie.
23	Príloha č. 15 - 1.5.1 Proxy server (webová brána) V kapitole je uvedené, že ak počítač prehľadáva web mimo sieť organizácie, protokoly musia byť synchronizované s ostatnými protokolmi prehľadávania on-premises.	Aké protokoly majú byť synchronizované ?	V zmysle technickej špecifikácie.
24	Príloha č. 15 - 1.5.1 Proxy server (webová brána) V kapitole je spomínané "Riešenie musí podporovať anonymné hlásenie správania a aktivít s odstránením alebo maskovaním citlivých osobných údajov."	Je známe aké citlivé údaje požadujete odstrániť z hlásení?	V zmysle technickej špecifikácie.
25	Príloha č. 15 - 1.6.1 SIEM riešenie V kapitole je v rámci tabuľky „Požadované parametre“ v časti Funkčné požiadavky uvedené „Riešenie musí podporovať monitoring sieťovej komunikácie v rámci virtualizovaného prostredia.“	Môže verejný obstarávateľ upresniť požadovanú úroveň monitoringu, udalosti ktoré majú byť monitorované a vyhodnocované v rámci riešenia? Aký typ a verzia virtualizovaného prostredia sa má monitorovať?	V zmysle technickej špecifikácie.
26	Príloha č. 15 - 1.6.1 SIEM riešenie V kapitole je v rámci tabuľky „Požadované parametre“ v časti Funkčné požiadavky uvedené „Riešenie musí mať schopnosť dodatočne zapojiť umelú inteligenciu do vyšetřovania incidentov v rámci jednotného rozhrania SIEM konzoly.“	Má byť súčasťou cenovej ponuky aj licencia na takúto funkcionálnosť? Ak áno, s akou kapacitou?	V zmysle technickej špecifikácie.
27	Príloha č. 15 - 1.6.1 SIEM riešenie V kapitole je v rámci tabuľky „Požadované parametre“ v časti Funkčné požiadavky uvedené „Riešenie musí umožňovať dodatočné pridanie integrovaného manažmentu rizík na základe sieťových tokov a konfiguráciu aktívnych prvkov do GUI.“	Je toto požadovaná funkcionálnosť riešenia alebo je to chápané ako možnosť integrácie systému tretej strany a jeho výstupov s takouto funkcionálnosťou?	V zmysle technickej špecifikácie.

28	Príloha č. 15 - 1.6.1 SIEM riešenie V kapitole je v rámci tabuľky „Požadované parametre“ v časti Funkčné požiadavky uvedené „Riešenie musí umožňovať pre budúce rozšírenie vzdialený zber logov lokálnym kolektorom s následným preposielaním v komprimovanej a šifrovanej podobe v rámci riešenia.“	Predmetom dodávky je zber logov z koľkých lokalít? Je možné poskytnúť popis topológie siete s ohľadom na umiestnenie monitorovaných systémov a predpokladaného objemu logovaných dát? Bude možné zber logov realizovať na jednom kolektore? Ak áno, je možné v takom prípade použiť riešenie s jedným serverom kde bude realizovaný zber aj vyhodnocovanie udalostí?	V zmysle technickej špecifikácie.
29	Príloha č. 15 - 1.6.2 Riešenie pre centrálny zber logov“ V kapitole je v rámci tabuľky „Požadované parametre“ v časti Funkčné požiadavky uvedené „Riešenie musí licenčne a výkonnovo podporovať spracovanie minimálne 500 EPS (Events per second).“	Aká úroveň spracovania je požadované pre tieto eventy? Nepožaduje sa analýza a korelácia s ostatnými udalosťami, ale iba normalizácia a ukladanie?	V zmysle technickej špecifikácie.
30	Príloha č.15 - 1.8 Systém pre ochranu dokumentov Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Využívate už nejakú službu cloudového providera? Ak áno, akú?	Nie.
31	Príloha č.15 - 1.8 Systém pre ochranu dokumentov Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Používa už UJD kolaboračný nástroj ako napríklad SharePoint, Conference alebo iný?	Nie.
32	Príloha č.15 - 1.8 Systém pre ochranu dokumentov Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aké sú používané verzie Microsoft Office?	Viď súťažné podklady.
33	Príloha č. 15 - 1.8 Systém pre ochranu dokumentov Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Disponujete už nejakými licenciami Office 365 / Microsoft 365 s ktorými sa počíta pri projekte? Majú byť licencie kompletne pokryté projektom alebo je v pláne nákup cez MIRRI?	Nie.
34	Príloha č.15 - 1.9 Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia a iné. Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Existuje už nejaká interná certifikačná autorita, napríklad Microsoft alebo iná ktorá je používaná?	Nie.
35	Príloha č.15 - 1.9 Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Používaný mailový systém je Exchange alebo iný?	HCL Domino.
36	Príloha č.15 - 1.9 Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Môžete prosím uviesť konfiguráciu existujúceho Active Directory - Jeden forest? jedna doména? - Názov DNS - Počet doménových radičov - Počet fyzických lokalít	1 forest, 1 doména, 2 lokality po 1 doménovom radiči. Ostatné informácie na stretnutí po podpise NDA.
37	Príloha č. 15 - 1.9 Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia	Je požadované, aby autentifikačný server bol inštalovaný on-premise?	Áno.
38	Príloha č. 15 - 1.9 Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	V požiadavkách je uvedená certifikačná autorita pre vydávanie a manažovanie digitálnych certifikátov podľa štandardu X.509. Je táto požiadavka relevantná pre dvojfaktorovú autentifikáciu? Certifikačná autorita sa štandardne využíva pre 2FA v prípade využitia čipových kariet (smart cards). Nie je to omyl?	Certifikačná autorita je dodatková súčasť projektu "Systém pre riadenie identít a autentifikačných prostriedkov - dvojfaktorová autentifikácia".
39	Príloha č. 15 - 1.10.1 Operačný systém servera pre riadenie prístupov zo vzdialených sietí V kapitole je v rámci tabuľky „Požadované parametre“ uvedený Typ licencie : MS WINDOWS Server 2019 STD, Množstvo : 1. Zároveň v kapitole „1.10.3 Softvér pre server pre riadenie prístupov zo vzdialených sietí“ je v rámci tabuľky „Požadované parametre“ časť Architektúra je uvedené „Riešenie musí podporovať nasadenie vo vysokej dostupnosti a vlastné technologické možnosti (bez použitia nástrojov/SW tretích strán) na zabezpečenie High Availability,“ Taktiež v časti Funkčné požiadavky je uvedené „Vzdialené pripojenie bude možné nadviazať cez vlastné GUI riešenia, ako aj pomocou štandardných protokolov RDP a SSH a štandardných klientov typu putty a remote desktop manager“, „Riešenie musí umožniť vzdialený prístup prostredníctvom SSH protokolu pomocou SSH Proxy“	Je v rámci požiadaviek záväzný počet serverov (Množstvo : 1) s definovaným operačným systémom? Je pre verejného obstarávateľa akceptovateľné riešenie ktoré navýši počet serverov a licencií vzhľadom na to že nie je z hľadiska najlepšej praxe a bezpečnosti odporúčaná ani realizovateľná prevádzka na jednom serveri? Ak riešenie vyžaduje pre SSH Proxy Linux server ma byť táto licencia súčasťou ponuky, alebo akceptuje obstarávateľ opensource verziu Linux? Umožní obstarávateľ prevádzku riešenia pre riadenie prístupov zo vzdialených sietí na virtualizačnej platforme ktorá je súčasťou ponuky pod kapitolou „1.11 Virtualizačná platforma pre prevádzku bezpečnostných systémov“? Ak áno je to plnohodnotná náhrada za kapitolu „1.10.5 Server pre prevádzku softvéru pre riadenie prístupov zo vzdialených sietí“?	Verejný obstarávateľ požaduje dodržať požadované minimálne parametre riešenia v zmysle technickej špecifikácie.

40	Príloha č. 15 - 1.10.3 Softvér pre server pre riadenie prístupov zo vzdialených sietí V kapitole je uvedené, že softvér pre server pre riadenie prístupov zo vzdialených sietí“ je v rámci tabuľky „Požadované parametre“ v časti Funkčné požiadavky uvedené „Riešenie musí umožňovať integráciu s ticketingovými nástrojmi tretích strán - žiadosť o schválenie prístupu, prístup na základe existujúceho tiketu, atď.“	Majú by súčasťou ponuky integračné práce, alebo postačuje existencia integračného API ktoré riešenie poskytuje? V čom táto požiadavka rozširuje požiadavku uvedenú v rovnakej časti „Riešenie musí umožňovať konfiguráciu systémov pomocou RestAPI - správa používateľov, vytváranie a editácia účtov, zmeny prihlasovacích údajov, ukončenie spojení, nastavenie oprávnení, zmeny politik, systém Health monitoring, schvaľovanie požiadaviek, autentizácia, atď.“?	V zmysle technickej špecifikácie.
41	Príloha č. 15 - 1.10.3 Softvér pre server pre riadenie prístupov zo vzdialených sietí V kapitole je uvedené, že softvér pre server pre riadenie prístupov zo vzdialených sietí“ je v rámci tabuľky „Požadované parametre“ v časti Licenčný model uvedené „Riešenie musí byť dimenzované minimálne pre 25 používateľov s plným používateľským prístupom (dostupné všetky funkcie riešenia).“	Licenčný model umožňuje rovnakú úroveň prístupu licencovať na základe toho či ide o interného používateľa riešenia alebo externého, ako sa uvedený počet 25 používateľov môže rozdeliť do týchto kategórií pre účely licencovania.	V zmysle technickej špecifikácie poskytnúť plný používateľský prístup pre všetkých požadovaných používateľov (dostupné všetky funkcie riešenia).
42	Príloha č. 15 - 1.10.4 Softvér pre servery, ku ktorým je požadovaný riadený prístup zo vzdialených sietí V kapitole je uvedené, že softvér pre servery, ku ktorým je požadovaný riadený prístup zo vzdialených sietí“ sú v rámci tabuľky „Požadované parametre“ v časti Podpora bezpečných prístupov pre cieľové systémy vymenované požadované cieľové systémy.	Môže verejný obstarávateľ bližšie špecifikovať požiadavky pre prístup na uvedené cieľové systémy - predovšetkým HP iLO, Dell DRAC, IBM, VMware, HyperV, Citrix, Checkpoint, Fortinet, Cisco?  Ide predovšetkým o klientský prístup (akým protokolom) a aj o automatickú zmenu hesla na týchto systémoch? Napríklad pre VMWare sa vyžaduje automatická zmena hesla a prístup cez VMWare vSphere Client (aplikácia) a prístup cez VMWare vSphere Web (webový prehliadač)?	V zmysle technickej špecifikácie riešenie musí umožniť bezpečný prístup administrátorov minimálne k uvedeným systémom.
43	Príloha č. 15 - 1.11.3 Rack s príslušenstvom pre virtualizačnú platformu Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Koľko kusov rackov požadujete dodať ?	Minimálne 1 ks, ostatné informácie na stretnutí po podpise NDA.
45	Príloha č. 15 - 1.11.4 Switch 10G pre virt.platformu Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	V počte 2ks. Rata sa s umiestnením/použitím v jednom DC? Alebo v dvoch geograficky vzdialených a použitie 40Gig na prepojenie?	V jednej lokalite, v jednom DC.
46	Príloha č. 15 - 1.11.4 Switch 10Gbit pre virtualizačnú platformu V kapitole je otázka k Požadovanej funkcionalite - Stohovaná konfigurácia, prepojenie min. 2x40 Gbit/s	Ráta sa s prepojením 10 Gbps switchov rýchlosťou 2x 40 Gbps ?	Áno, vyplýva to zo špecifikácie.
47	Príloha č. 15 - 1.11.4 Switch 10Gbit pre virtualizačnú platformu V kapitole je napísané "Požadujeme použitie 2ks prepínačov na zabezpečenie redundancie, pričom všetky zariadenia musia byť pripojené do každého z týchto prepínačov."	Toto je protichodná požiadavka s požiadavkou , že LAN prvky majú byť umiestnené v 2 lokalitách ( Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia , Inštalácia a konfigurácia sieťových komponentov LAN – 2 lokality ). Prosíme vysvetliť ako zapojiť zariadenia do každého z prepínačov ak majú byť prepínače v dvoch rôznych lokalitách	10Gbit switche budú v jednej lokalite, 1 Gbit budú v 2 lokalitách. Z toho vyplývajú požiadavky na súvisiace činnosti.
48	Príloha č. 15 - 1.11.6 Diskové pole pre virtualizačnú platformu Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Koľko kusov diskového poľa požadujete dodať ?	podľa súťažných podkladov.
49	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	V prípade riešenia helpdeskového systému sa vyžaduje automatické vytváranie incidentov z monitorovacieho systému?	Nie.
50	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Aký počet používateľov bude využívať monitorovací systém?	V tejto fáze do 25 používateľov.
51	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	UJD ma vlastnú Certifikačnú autoritu pre prípad generovania SSL certifikátov?	Nie.
52	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Za aké časové obdobie je požadované udržiavať výkonnosťné dáta?	Aspoň 3 mesiace.
53	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Licenčné pokrytie pre neobmedzený počet používateľov – čo znamená, na akú časť sa vzťahuje táto podmienka	Týka sa konzoly Monitorovacieho systému.

54	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Príprava štandardných obrazoviek a dashboardov pre jednotlivé skupiny používateľov – predstava o skupinách (napr. HW team , Backup team, Windows /UX/Linux team .... atď.)	Toto bude súčasťou návrhu riešenia.
55	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia, časť Monitorovací systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Preferuje sa OnPrem,Cloud alebo hybridné riešenie monitorovacej platformy alebo ich kombinácia?	On-premises.
56	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia V kapitole časti Inštalácia a konfigurácia sieťových komponentov LAN – 2 lokality je uvedené	Nie je nám jasné umiestnenie 10Gbps switchov pre virtualizačnú platformu. V každej lokalite má byť jeden 10 Gbps switch ?	Nie, iba v jednej lokalite.
57	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia V kapitole časti Inštalácia a konfigurácia sieťových komponentov LAN – 2 lokality je uvedené	Aká je použitá technológia prepojenia dátových centier ? Jedná sa o dark fibre, alebo o konektivitu od ISP ?	ISP...50Mbps:50Mbps
58	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia V kapitole časti Inštalácia a konfigurácia sieťových komponentov LAN – 2 lokality je uvedené	Ak je použitá technológia prepojenia dátových centier dark fibre, aká je vzdialenosť dátových centier po optickej trase ?	Irelevantné.
59	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia V kapitole časti Inštalácia a konfigurácia sieťových komponentov LAN – 2 lokality je uvedené	Ak je použitá technológia prepojenia dátových centier ako nakúpená konektivita od ISP aká je rýchlosť prepojenia ?	ISP...50Mbps:50Mbps
60	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia V kapitole v časti "Inštalácia a konfigurácia SAN siete – 1 lokalita" sú spomenuté SAN prepínače	Oba SAN prepínače pre virtualizačnú platformu budú umiestnené v jednom dátovom centre ?	Áno.
61	Príloha č. 15 - 1.11.8 Inštalácia HW a systémového prostredia Upresnenie k časti "Inštalácia a konfigurácia serverov – 1 lokalita"	Všetky 4 servery pre virtualizačnú platformu budú umiestnené v jednom dátovom centre ?	Áno.
62	Príloha č. 15 - Helpdesk systém Všeobecná otázka ku kapitole dotýkajúca sa viacerých bodov	Je akceptovateľné z Vašej strany, ak by bol Helpdesk systém postavený ako cloud riešenie?	Áno.