POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 24-2017

Poskytovatel	AutoCont CZ a.s.
Správce	
Objednatel	ČESKÁ REPUBLIKA - SPRÁVA ZÁKLADNÍCH REGISTRŮ
Smlouva	Č. SZR-374-74/Ř-2015
Název ZP	**Součinnost při napojení ISZR do DCeGov (SIEM)**
Číslo tiketu (ServisDesk)	1-255023292 / 26898
Katalogový list	**KL 20**
Datum podání	17. 08. 2017
Priorita	-

1. Identifikace vzniku požadavku

zadání požadavku na ServisDesk

2. Zadání požadované změny

Požadavek o nacenění součinnosti na straně ISZR při napojení tohoto systému do DCeGov (SIEM)

Žádáme o nacenění prací vydefinovaných v příloze tohoto požadavku, které souvisí s připojením systému ISZR k DCeGOV. Seznam těchto požadavků byl poskytnut ze strany NAKIT v rámci projektu řízeného ze strany OKB MV. Mezi další relevantní podklady patří kompletní analytické dokumenty k připojení systému ISZR předané formou emailu dne 15. 8. 2017.

Nacenění prosím uveďte min. ve struktuře obsažené v příloze, tedy k jednotlivým požadavkům na součinnost definujte pracnost za jednotlivé role, které se na ní budou podílet a v případě rozdílných sazeb těchto rolí i jejich sazby. Pokud u jakéhokoliv požadavku na součinnost, který definoval NAKIT, nebudete na základě dostupných informací schopni pracnost definovat, bude zajištěna eskalace na OKB.

Děkuji,

Pozadavky na soucinnost_ISZR.do

Emailové podklady z 15.8.2017.zip

3. Popis zajištění realizace změny

3.1 Výchozí předpoklady

Předávané logy – zdrojové systémy:

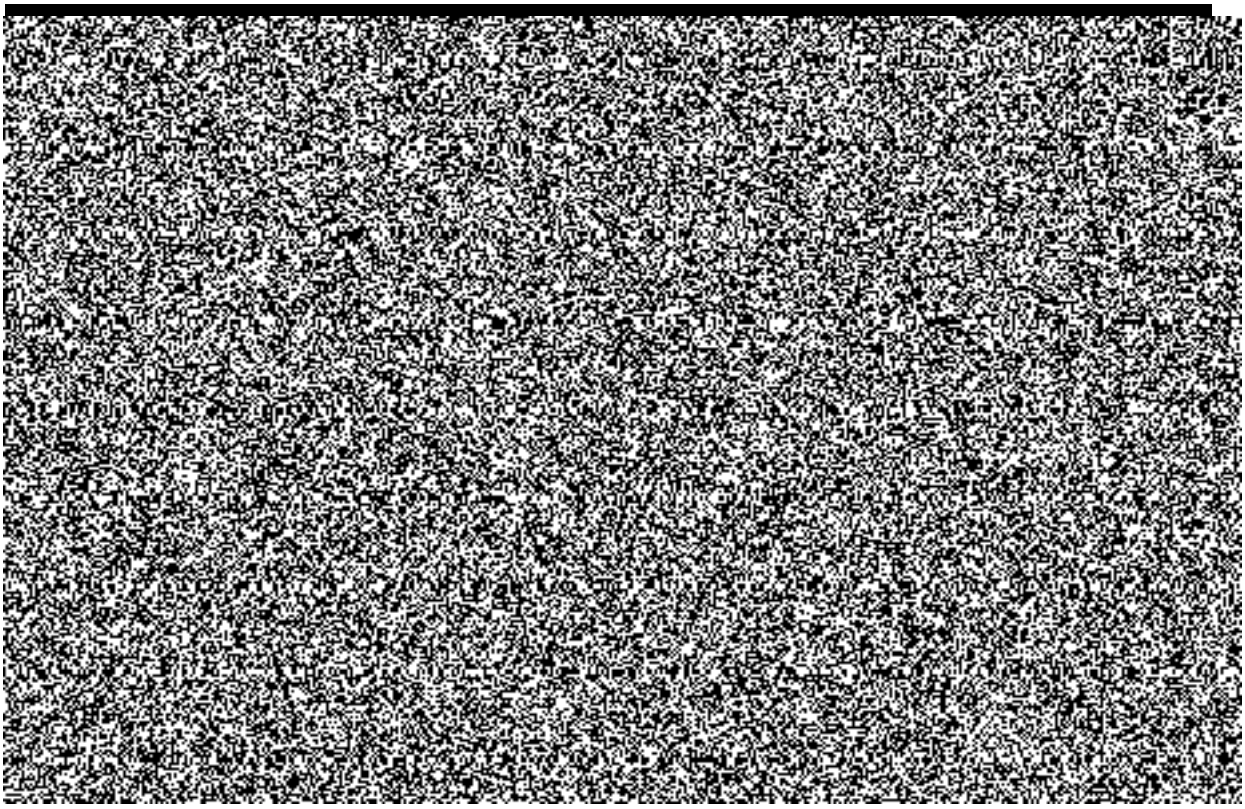
V souladu s výstupy analýzy budou předávány vybrané bezpečnostní logy infrastrukturních komponent, aplikační logy a logy o realizovaných transakcích systému ISZR předávány nebudou.

Předávané logy – poskytované události:

Rozsah poskytovaných událostí bude vycházet z dokumentu: *5 Evidence poskytovani udalosti ISZR 20170516_v1.xlsx*. V souladu s tímto dokumentem bude provedeno rozšíření logování událostí v jednotlivých oblastech s výjimkou logování událostí:

- jejichž logování by mělo dopad na výkonnost sledovaných komponent
- jejichž sledování by vyžadovalo programové úpravy (není přímo konfigurovatelné)
- jejichž sledování by vyžadovalo dodatečné investice do programového, nebo HW vybavení

Způsob předávání log záznamů po jednotlivých komponentách:



V souladu s výstupy analytických dokumentů a zadáním tohoto požadavku budou změny realizovány v těchto oblastech:

3.2 Přípravné práce:

- Přípravné práce nutné pro spuštění implementačního projektu

3.3 Předávání souborových logů

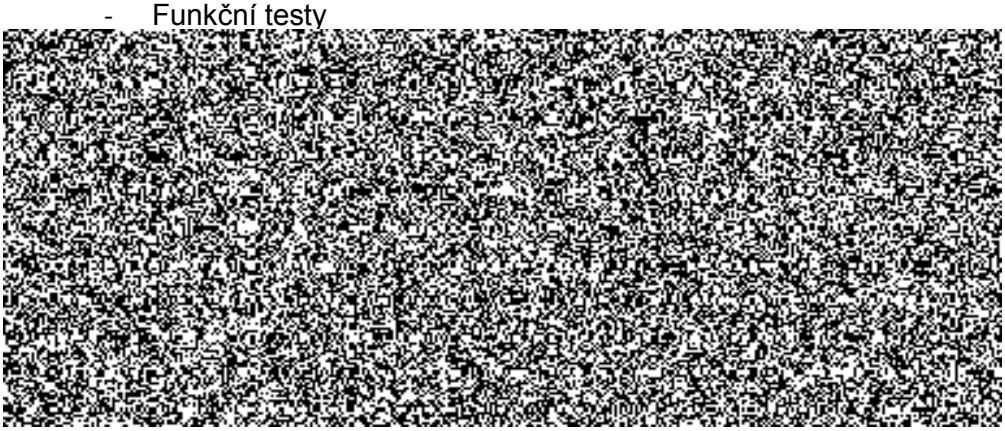
- Bude zřízena speciální síťová zóna – DMZ pro umístění FILE serveru
- Bude nainstalován server pro konsolidaci textových logů – FILE server
- Textové logy ze systému HP Data Protector budou v rámci infrastruktury ISZR konsolidovány na nově instalovaný FILE server v DMZ.
- Na serveru bude vytvořen sdílený adresář s logovými soubory.
- Tento sdílený adresář bude připojen na KSM nebo kolektor serveru, kde jej zpracuje SmartConnector - součinnost NAKIT, neprovádí AC.

Typ zařízení ISZR	Způsob předávání log záznamů
HP Data Protector	Souborový přenos

3.4 Předávání logů MS Windows prostředí

Po posílení HW infrastruktury a změně konfigurace agentů bude pro sběr logů z Windows Event Logu využit sběr těchto logů do SCOM. Data budou zpřístupněna prostřednictvím SCOM ACS.

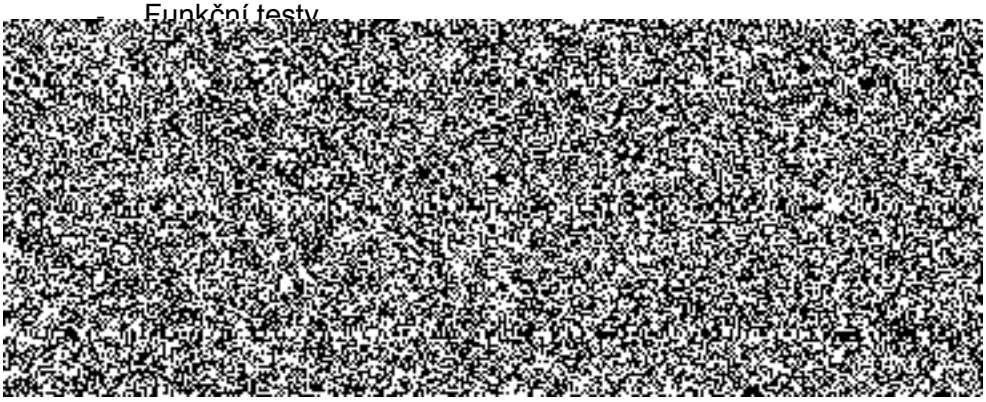
- Nová instalace SCOM infrastruktury na poskytnutý HW.
- Změna režimu připojených SCOM klientů – zajištění přeposílání dat - ACS
- Konfigurace jednotlivých zdrojů logů (Win Event log, MS SQL) pro zaznamenávání vybraných zpráv prostřednictvím SCOM
- Integrační testy
- Funkční testy



3.5 Předávání logů prostřednictvím protokolu SYSLOG

Zařízení, která podporují zasílání logů protokolem syslog budou tyto logy zasílat přímo na syslog server v rámci KSM.

- Konfigurace jednotlivých zdrojů logů pro přeposílání vybraných zpráv prostřednictvím SYSLOG
- Integrační testy
- Funkční testy



4. Odhad pracnosti

Fáze	Provádí	Činnost	Detail	Pracnost MD - AC	Poznámka AC
Přípravné práce					
I.	AC	Zhotovení harmonogramu garantem zdrojového systému (časová a zdrojová náročnost)			Vypracováno v rámci tohoto PnČ
I.	AC	Poskytnutí seznamu logovaných assetů a network modelu ISZR	Dodání seznamu logovaných prvků s jejich IP adresami, jmény a označením umístění v síťové topologii		Bylo poskytnuto v rámci součinnosti při přípravě analýzy
I.	AC	Poskytnutí případných chybějících logů pro flex konektory			Bylo poskytnuto v rámci součinnosti při přípravě analýzy
I.	NAKIT, SZR, AC	Konfigurace síťového prostupu ISZR - KSM (2xDC)	Součinnost při nastavování síťových prostupů na straně SZR, postup dle kapitoly 4.2 v dokumentu Sběr událostí		

I.	NAKIT, SZR, AC	Konfigurace síťového prostupu KSM - DCeGOV (2xDC)	Součinnost při nastavování síťových prostupů na straně SZR, postup dle kapitoly 4.2 v dokumentu Sběr událostí		
Předávání souborových logů					
I.	NAKIT	Příprava HW File Share	Požadavky na HW jsou uvedeny v kapitole 3.5.1 v dokumentu Sběr událostí		Přípravu HW budou provádět zástupci společnosti NAKIT, podle definovaných požadavků.
I.	AC	Instalace OS Windows			
I.	AC	Instalace a konfigurace sběrných míst – FILE SHARE. Instalace a konfigurace, systémový hardening celkem 2 File serverů – jeden v každém DC. Integrace těchto serverů do DFS.			
II.	SZR, HPE, AC	Konfigurace File Share serveru pro přístup z KSM	Součinnosti při nastavení FILE share serveru a kontroly sběru logů.		
	AC				
I.	AC	Konfigurace jednotlivých zdrojů logů pro zaznamenávání vybraných zpráv prostřednictvím FILE SHARE včetně úrovně logování.			
I.	AC, NAKIT	Integrační testy			
I.	AC, NAKIT	Funkční testy			
Předávání logů MS Windows prostředí					
I.	NAKIT	Příprava HW SCOM a SQL	Požadavky na HW jsou uvedeny v kapitole 3.5.1 v dokumentu Sběr událostí		součinnost NAKIT
I.	AC	Základní instalace OS Windows – celkem			

II.	SZR, HPE, AC	Konfigurace SCOM serveru pro přístup z KSM	Součinnosti při nastavení SCOM serveru a kontroly sběru logů.		
I.	AC	Instalace a konfigurace SCOM serveru. Instalace SCOM a MS SQL serverů v obou DC, celkem 2x SCOM server, a 2x MS SQL server. Hardening komponent, nastavení integrací mezi instancemi v jednotlivých DC.			
I.	AC	Záloha nastavení SCOM, logů zařízení - MS SQL server	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Vytvoření klonu DB serverů	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Vytvoření klonu SCOM serverů	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Restore konfigurace DB serverů, databáze	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Restore konfigurace SCOM serverů	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Oživení serverů, kontrola funkčnosti Napojení nových serverů SCOM serverů na klonovanou DB	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Instalace a konfigurace serverové části ACS	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Napojení stávajících klientů na novou SCOM infrastrukturu	Pracnost za obě DC, realizovat je nutné jednotlivě		
I.	AC	Změna režimu připojených SCOM klientů – zajištění přeposílání dat. Bude provedena změna na úrovni instalovaných agentů na všech takto sledovaných			

		komponentech cca 200 zařízení. Změny budou muset být provedeny i na úrovni stávající funkcionality provozního dohledu, tak aby tato v novém režimu fungovali ve stejných parametrech jako před změnou.			
I.	AC	Konfigurace jednotlivých zdrojů logů pro zaznamenávání vybraných zpráv prostřednictvím SCOM včetně úrovně logování. Konfigurace rozšíření sledovaných a zaznamenávaných událostí na úrovni sledovaných OS a aplikací.			
I.	AC, NAKIT	Integrační testy			Integrační testy budou realizovány v definované pracnosti.
I.	AC, NAKIT	Funkční testy	AC bude poskytovat součinnost při vygenerování bezpečnostních událostí ve scénářích kde je toto možné.		
Předávání logů prostřednictvím protokolu SYSLOG					
II.	AC	Konfigurace jednotlivých zdrojů logů pro přeposílání vybraných zpráv prostřednictvím SYSLOG. Konfigurované zdroje: Solaris OS, F5 síťové prvky F5 BIG GTM, F5 BIG GTM, virtualizační komponenty, Cisco Nexus, Cisco ASA.	Součinnosti při nastavení syslog zařízení a kontroly sběru logů.		
II.	NAKIT, SZR	Integrační testy			
II.	NAKIT, SZR	Funkční testy			
I a II	AC	Projektové řízeni			
I a II	AC	Dokumentace provedených nastavení. Provedené změny v úrovni logování se týkají fakticky každé typové komponenty systému ISZR,			

		kromě vlastní dokumentace PnČ bude nutné revidovat i dokumentace jednotlivých komponent.			
I a II	AC	Nastavení rutin pro správu a dohled nových serverů, funkcionalit			
CELKEM (MD)					
Celková cena: 1 537 500,- Kč bez DPH					

4.1 Služby spojené s provozem datového úložiště

Bude řešeno jiným RFC / PnČ.

4.2 Nutný HW

Nad rámec dostupného HW – seznam:

4x Server 2 U v konfiguraci:

- 2x CPU AMD celkem 24 jader
- 512 GB RAM
- 4x 1 Gbps LAN
- 2x 10 Gbps LAN
- 5x 300 GB SAS 10k rpm

5. Návrh harmonogramu změnového požadavku

Vlastní harmonogram realizace je závislý na termínu objednání realizace tohoto požadavku (T)

Fáze realizace požadavku	Termín – týdny
Přípravné práce	T+1
Předávání souborových logů	T+8
Předávání logů MS Windows prostředí	T+10
Předávání logů prostřednictvím protokolu SYSLOG	T+12

6. Dopady do provozu / dopady do provozní dokumentace

Bude nutná úprava provozní dokumentace, nastavení rutin pro správu a dohled nových serverů a funkcionalit. Bude nutné stanovení provozovatele nově implementovaných komponent/funkcionalit. Je nutné dořešit následnou zodpovědnost za zajištění a správu SW a HW maintanance pro nově přidané komponenty.
Po dobu mezi odstavením stávající a dointegrací upgradované dohledové platformy bude nedostupný monitorovací systém. Instalace bude nutné provádět v rámci rizikové operace, event. pouze v neaktivním DC spolu se SWITCHOVER zpracování.

Vzhledem ke snaze minimalizovat prvotní pořizovací náklady, není systémová architektura řešení tohoto požadavku stavěna na redundantních komponentech v rámci jednoho DC. Zajištění vysoké dostupnosti tak bude využívat pouze omezené možnosti, které nabízí virtualizační vrstva systému a částečná zastupitelnost komponent mezi instancemi ve dvou DC.

7. Návrh testovacího scénáře

Probíhá předávání logových souborů na FILE share server DMZ

Probíhá sběr vybraných logů MS Windows prostředí prostřednictvím SCOM.

Probíhá předávání logů prostřednictvím protokolu SYSLOG.

8. Požadavky na součinnosti

Poskytnutí HW a SW pro rozšíření SCOM platformy podle specifikovaných požadavků.

Zajištění odpovídajících datových prostupů pro integrace s KSM a integrace komponent mezi sebou.

Zajištění součinnosti při testování.

9. Výstupy změnového požadavku

Odesílání vybraných logových záznamů do prostředí DCeGOV,

	Schválil (AutoCont CZ)	Schválil (zákazník)
Jméno	[redacted]	[redacted]
Datum	26. 9. 2017	26. 9. 2017
Podpis		