Република Србија
МИНИСТАРСТВО ФИНАНСИЈА
Управа за трезор
Сектор за људске и материјалне ресурсе
Број: 404-00-839-11/2014-001-008
02.09.2014. године
Поп Лукина 7-9
Б е о г р а д

ИЗМЕНА КОНКУРСНЕ ДОКУМЕНТАЦИЈЕ

У складу са чланом 63. Закона о јавним набавкама („Службени гласник РС“ број 124/2012) врши се измена конкурсне документације за јавну набавку добара - Софтвер за корелацију логова са имплементацијом, за потребе Министарства финансија – Управа за трезор, ОП број 42/2014, тако што се:

- текст на страни 5 од 43 конкурсне документације ставка 12 Основни захтеви за софтвер за корелацију логова: „Софтвер за корелацију логова треба да омогући прикупљање, анализу у реалном времену и складиштење најмање 5000 догађаја у секунди (*Events per Second* - EPS) и 200000 FPM са могућношћу проширења на истој платформи до 10000 EPS само додавањем лиценци. Ова вредност догађаја у секунди је средња вредност у току једног дана. Софтвер за корелацију логова треба да омогући и прикупљање догађаја у ситуацијама када долази до изненадног (краткотрајног) повећања броја догађаја у секунди (*peak*).“ **мења се и гласи:** „Софтвер за корелацију логова треба да омогући прикупљање, анализу у реалном времену и складиштење најмање 5000 догађаја у секунди (*Events per Second* - EPS) и 25000 FPM (*Flows per Second* - FPM) са могућношћу проширења на истој платформи до 10000 EPS и 200000 FPM само додавањем лиценци. Ова вредност догађаја у секунди је средња вредност у току једног дана. Софтвер за корелацију логова треба да омогући и прикупљање догађаја у ситуацијама када долази до изненадног (краткотрајног) повећања броја догађаја у секунди (*peak*).“

- текст на страни 8 од 43 конкурсне документације ставка 12 у табели:

12	Софтвер за корелацију логова треба да омогући прикупљање, анализу у реалном времену и складиштење најмање 5000 догађаја у секунди (*Events per Second* - EPS) и 200000 FPM са могућношћу проширења на истој платформи до 10000 EPS само додавањем лиценци. Ова вредност догађаја у секунди је средња вредност у току једног дана. Софтвер за корелацију логова треба да омогући и прикупљање догађаја у ситуацијама када долази до изненадног (краткотрајног) повећања броја догађаја у секунди (*peak*).	

мења се и гласи

12	Софтвер за корелацију логова треба да омогући прикупљање, анализу у реалном времену и складиштење најмање 5000 догађаја у секунди (*Events per Second* - EPS) и 25000 FPM (*Flows per Second* - FPM) са могућношћу проширења на истој платформи до 10000 EPS и 200000 FPM само додавањем лиценци. Ова вредност догађаја у секунди је средња вредност у току једног дана. Софтвер за корелацију логова треба да омогући и прикупљање догађаја у ситуацијама када долази до изненадног (краткотрајног) повећања броја догађаја у секунди (*peak*).	

У прилогу се налази страна 5 од 43 конкурсне документације и страна 8 од 43 конкурсне документације са извршеним изменама. Потребно је да потенцијални понуђачи за предметни поступак јавне набавке исте одштампају и приложе као саставни део конкурсне документације.

Комисија за јавну набавку

Cisco рутери и свичеви	6+6
Cisco ACS сервери	3
Vmware ESXi	6
Proxy	3
Storage	3
DataDomain	1
RecoverPoint	4

Основни захтеви за софтвер за корелацију логова:

- Решење треба да буде скалабилно (могућност даљег проширења без одбацивања постојећих уређаја и лиценци).
- Прикупљање логова и network flow записа са уређаја и апликација врши се у реалном времену као и корелације логова и network flow записа.
- Чување логова у изворној форми (*raw logs*), у трајању од најмање три месеца, након чега се архивирају.
- Преглед архивираних логова у нормализованом облику уз обезбеђивање интегритета
- Потребно је да постоји могућност дефинисања различитих периода чувања логова за неке групе логова.
- Мора постојати могућност правовременог обавештења и идентификације безбедносних претњи у ИТ систему уз надгледање и корелацију различитих мрежних догађаја.
- Софтвер за корелацију логова треба да омогући дефинисање различитих периода времена складиштења појединих логова.
- Софтвер за корелацију логова треба да обезбеди интегритет података, односно да спречи промене лог записа на систему.
- Прикупљање логова са уређаја врши се примарно без агената (agentless), односно уз помоћ агената на уређајима уколико је то неопходно.
- Софтвер за корелацију логова треба да обезбеди интегритет података у транспорту, односно криптовану комуникацију између агената и централног сервера.
- Праћење исправности рада агената.
- Софтвер за корелацију логова треба да омогући прикупљање, анализу у реалном времену и складиштење најмање 5000 догађаја у секунди (*Events per Second* - EPS) и 25000 FPM (*Flows per Second* - FPM) са могућношћу проширења на истој платформи до 10000 EPS и 200000 FPM само додавањем лиценци. Ова вредност догађаја у секунди је средња вредност у току једног дана. Софтвер за корелацију логова треба да омогући и прикупљање догађаја у ситуацијама када долази до изненадног (краткотрајног) повећања броја догађаја у секунди (*peak*).
- Нормализација, корелација и анализа логова.

10	Софтвер за корелацију логова треба да о езбеди интегритет података у транспорту, односно криптовану комуникацију између агената и централног сервера.	
11	Праћење исправности рада агената.	
12	Софтвер за корелацију логова треба да омогући прикупљање, анализу у реалном времену и складиштење најмање 5000 догађаја у секунди (*Events per Second* - EPS) и 25000 FPM (*Flows per Second* - FPM) са могућношћу проширења на истој платформи до 10000 EPS и 200000 FPM само додавањем лиценци. Ова вредност догађаја у секунди је средња вредност у току једног дана. Софтвер за корелацију логова треба да омогући и прикупљање догађаја у ситуацијама када долази до изненадног (краткотрајног) повећања броја догађаја у секунди (*peak*).	
13	Нормализација, корелација и анализа логова.	
14	Претрага лог записа путем регуларних израза.	
15	Софтвер за корелацију логова треба да поседује могућност „претраге у дубину“ (тзв. *Drill down search*)	
16	Софтвер за корелацију логова треба да препознаје структуру логова минимално за наведене системе: - Оперативни системи: *Windows* и *Unix/Linux* (*Red Hat, CentOs, Fedora / HP-Unix*) - Microsoft Active Directory - Web сервиси: *Apache, IIS* - DNS сервиси: *Bind, Microsoft* - Базе података: *Microsoft SQL Server, Oracle, MySQL* - Proxy сервери: *Squid* - Mail сервери: *Sendmail* - Ftp сервери: *VSFTP* - Мрежна опрема: *Cisco* рутери и свичеви, *Cisco ASA* и *PIX firewall* уређаји, ACS сервери - IPS уређаји: *Cisco IPS* - Антивирусна решења: *Symantec* - Виртуелна инфраструктура: *VMware* - Storage системи: *EMC,EVA* - Appliance уређаји: *DataDomain, RecoverPoint* - Backup решење: *NetWorker* - Апликативни сервери: *SAP, Oracle Application, Oracle BI, MQ*	
17	Прикупљање и чување лог записа које не уме да парсира и анализира. За такве записе треба да постоји могућност да се дефинишу структура записа и значења лог атрибута.	
18	Грануларни приступ логовима, односно могућност дефинисања права приступа одређених корисника одређеним лог записима у систему.	
19	Слање упозорења администраторима система у случајевима када се са уређаја прима неуобичајени број лог записа (записи не долазе одређено време, нагли скок и друго).	