

NADOGRADNJA VATROZIDNOG SUSTAVA UREĐAJEM ZA ANALIZU PROMETA S VATROZIDNOG CLUSTERA I ZAŠTITU OD ZERO-DAY NAPADA

UVOD

Ovim projektom nabavlja se nadogradnja postojeće vatrozidne infrastrukture uređajem za analizu prometa s postojećih vatrozidnih uređaja u svrhu detektiranja i zaštite od Zero-Day prijetnji. Postojeća vatrozidna infrastruktura temelji se na opremi proizvođača Check Point, a sastoji se od vatrozidnog clustera s 5600 uređajima (dva uređaja u cluster konfiguraciji) te centralni upravljački sustav za vatrozide s licencom za upravljanje do 5 uređaja.

TEHNIČKE SPECIFIKACIJE OPREME

Ponuditelj iskazuje potpunu sukladnost ponuđene opreme (konstatacijom DA ili NE) za svaki zahtjev. Svi navedeni tehnički zahtjevi su eliminacijski. Ponuditelj dokazuje sukladnost pokazivačem na ključne podatke iz tehničke dokumentacije proizvođača (Referenca na stranicu iz kataloga), koja može biti na hrvatskom ili engleskom jeziku. Ukoliko je na nekom drugom jeziku osim hrvatskog ili engleskog jezika, Ponuditelj je dužan u ponudi priložiti i prijevod dokumentacije na hrvatski jezik izvršenog po ovlaštenom sudskom tumaču.

TABLICA FUNKCIONALNIH I TEHNIČKIH ZAHTJEVA

Uređaj za analizu prometa s vatrozidnog clustera i zaštitu od Zero-Day napada - minimalno kao Check Point SandBlast TE Appliance TE250X (ili jednakovrijedan)

Minimalne zahtijevane karakteristike		Zahtjev ispunjen (DA/NE)	PONUĐENO	Referenca na stranicu iz kataloga
Proizvođač				
Ponuđeni model				
Količina	1 komad			
Općenito	Uređaj za naprednu zero-day zaštitu uz detekciju i prevenciju naprednih malicioznih aktivnosti, u potpunosti kompatibilan s postojećim vatrozidnim clusterom proizvođača Check Point. Integracija s postojećim centralnim sustavom za upravljanje vatrozidnim sustavom proizvođača Check Point.			
	Uređaji u obliku appliance rješenja (hardver i softver od istog proizvođača), maksimalan visina 1RU			
Podržane datoteke	Minimalno podržano 250000 datoteka mjesečno			
Propusnost	Minimalna propusnost od 700 Mbps			

Virtualni strojevi	Uređaj mora imati minimalno 8 virtualnih strojeva			
Disk	Kapaciteta diska od minimalno 1TB			
Sučelja	Minimalno 9 x 10/100/1000Base-T RJ45 mrežna sučelja			
	Minimalno jedan utor za proširenje mrežnim sučeljima uz opciju naknadnog dodavanja: - 4x1GbE bakrenog sučelja s fail-open bypass funkcionalnošću, - 4x1GbE optičkog sučelja s fail-open bypass funkcionalnošću, - 2x 10GbE sučelja s fail-open bypass funkcionalnošću			
Funkcionalnosti	Sprečavanje novih i nepoznatih napada u dokumentima i izvršnim datotekama			
	Podržana identifikacija novih malwarea u minimalno 40 tipova datoteka uključujući Adobe PDF, Microsoft Office, Java, Flash, izvršnih datoteka i arhiva			
	Sposobnost micanja potencijalno malicioznog sadržaja iz datoteka i isporuka takvih čistih datoteka korisnicima bez kašnjenja			
	Tehnologija otkrivanja zlonamjernog softvera na nivou CPU-a prije nego što zlonamjerni softver dobije priliku za svoju implementaciju i izbjegavanje otkrivanja			
	Podržano minimalno inspekcija e-mail prometa (SMTP) te web (HTTP) prometa, web kriptiranog (HTTPS) prometa i CIFS prometa			
	Potpuna integracija postojećim vatrozidnim clusterom proizvođača Check Point na način da vatrozidni cluster šalje datoteke na inspekciju Uređaju za zaštitu od Zero-Day napada			
	Dodatne podržane vrste implementacije rješenja: kao inline MTA, ICAP server implementacija			
Jamstvo	Uređaj mora biti nov i neupotrebljavan. Hardver i softver mora biti s minimalnim jamstvom od 12 mjeseci. Jamstvo proizvođača u minimalnom trajanju od 12 mjeseci mora obuhvaćati pristup tehničkoj službi (TAC), nove nadogradnje operativnog sustava uređaja, zamjena pokvarenog			

	ili neispravnog uređaja.			
Implementacija rješenja	Instalacija, konfiguracija i integracija rješenja u postojeći vatrozidni sustav proizvođača Check Point			

IZJAVA

Kojom prihvaćamo ponuđene Tehničke uvjete.

U, 2018.

Ponuditelj:

(pečat i potpis ovlaštene osobe)