PREGLED POSTUPKA #83194

1 PODACI O NARUČIOCU

Naziv naručioca	UPRAVA ZA STATISTIKU
PIB	02011506
E-mail	contact@monstat.org
Telefon	020/230-811, 020/230-961
Internet adresa	www.monstat.org
Fax	020/230-814, 020/230-961
Adresa	IV Proleterske 2
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	Antivirusni softver
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Snežana Obradović
Kontakt	zana.obradovic@monstat.org
Datum objave	29.11.2024. 08:30
Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Antivirusni softver	29.11.2024 08:30	03.12.2024 08:30	03.12.2024 08:30	U toku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne

5 STAVKE PLANA

Ne postoje definisane stavke plana

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
Ponuđač je dužan u okviru podnijete ponude, a u skladu sa članom 9 stav 10 Pravilnika o načinu sprovođenja jednostavnih nabavki ("Sl.list Crne Gore", broj 016/23 od 10.02.2023. godine, broj 020/23 od 22.02.2023. godine, 36/23 od 29.03.2023., 114/23 od 19.12.2023. i 49/24 od 29.05.2024.), dostaviti Izjavu ponuđača (Obrazac 2) o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisanu od strane ovlašćenog lica ponuđača, datu na Obrascu 2, koji se nalazi u prilogu zahtjeva za podnošenje ponuda.	Obavezni uslovi
Mjesto izvršenja ugovora: Uprava za statistiku, Ul. IV proleterske br. 2	Mjesto izvršenja ugovora
Plaćanje je u roku od 20 dana od dana dostavljanja fakture, nakon isporuke i implementacije predmeta nabavke i prijema od strane ovlašćenih lica naručioca.	Rok plaćanja
Način plaćanja: virmanski	Način plaćanja
Rok izvršenja ugovora: 15 dana od dana zaključenja ugovora.	Rok izvršenja ugovora
Rok važenja ponude: 90(devedeset) dana od dana otvaranja ponuda	Rok važenja ponude
Ponuđač mora biti ovlašćen od strane proizvođača za isporuku traženih softverskih licenci na teritoriji Crne Gore (ukoliko nije proizvođač), što se dokazuje autorizacijom proizvođača softvera (MAF).	Stručna i tehnička sposobnost
Ponuđač je dužan da antivirusni softver fizički instalira, poveže i integriše u postojeći sistem naručioca, prema zahtjevu naručioca i u skladu sa najboljom praksom i profesionalnim standardima. Integracija podrazumijeva stavljanje ponuđenog softvera u punu funkciju, kako bi opsluživala klijentske zahtjeve. Nakon implementacije, izabrani ponuđač dužan je da dostavi naručiocu dokumentaciju izvedenog stanja. Ponuđač je dužan da u periodu trajanja licenci pruza tehnicku podrsku naruciocu.	Stručna i tehnička sposobnost

ISO 9001Dokaz o uspostavljenom sistemu upravljanja kvalitetom.	Dokaz odnosno sertifikat, koje izdaju akreditovana sertifikaciona tijela o ispunjavanju uslova kvaliteta predmeta nabavke
ISO 27001 Dokaz o uspostavljenom sistemu menadžmenta bezbjednošću	Stručna i tehnička sposobnost
ISO 20000-1 Sistem menadžemnta uslugom	Stručna i tehnička sposobnost
ISO 27701 - Sistemi menadžmenta informacijama o privatnosti	Stručna i tehnička sposobnost

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **12.000,00 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		Sistem za naprednu zaštitu servera i radnih stanica Mogućnost primjene modula zaštite u različitim varijantama i njihovim proizvoljnim kombinacijama, integrisanim u jednu konzolu u cloud-u: • Extended Detection and Response (XDR) senzor, samo XDR komponenta koja može da radi samostalno (na primjer zajedno sa postojećim antimalverom drugog proizvođača). • Standardna zaštita radnih stanica i servera na Windows i MacOS platformama, sa fokusom na desktop i prenosive računare. • Opciona namjenska zaštita virtualnih okruženja i servera na Windows, Linux i AIX platformama sa naprednim funkcionalnostima fokusiranim na servere i virtualna okruženja. • Opcioni Attack Surface Management (ASRM) senzor, koji može da radi samostalno (na primjer zajedno sa postojećim antimalverom drugog proizvođača). Extended Detection and Response (XDR) • Mogućnost čuvanja logova od 30 do 365 dana. • Instalirani XDR mora imati mogućnost da otkrije softverske ranjivosti na operativnom sistemu i instaliranim aplikacijama	

		(npr. Adobe Reader, gdje je instaliran). • Automatsko slanje potencijalno malicioznih uzoraka, na osnovu XDR analize, u Sandbox sa mogućnošću ručnog otpremanja uzoraka (Manual submission). • Podrška za Windows, MacOS i Linux platformame, uz mogućnost rada sa antimalware agentima drugih proizvođača (3rd party). • Mora imati veliki broj modela detekcije kojima upravlja administrator sistema, na osnovu kojih se vrši XDR korelacija podataka, mogućnost postavljanja izuzetaka za date modele detekcije, kao i pravljenje sopstvenih modela detekcije. • Mora sadržavati specijalizovane Indication of Compromise (IoC) kanale kojima upravlja administrator sistema, a koji prate poznate kampanje zlonamjernih napadačkih grupa u svrhu automatske detekcije i čišćenje detektovanih IoC-a. • Mora sadržavati specijalizovane IoC kanale od nezavisnih dobavljača koji se mogu koristiti za isto kao i postojeći (detekcija i čišćenje). • Mogućnost unosa ručnih IoC objekata, i drugih obavještajnih podataka o prijetnji, koji se zatim mogu koristiti za detekciju i čišćenje. • Podrška sledećih formata unosa IoC-a: STIX, TAXII, MISP, csv. • Jasna vizualizacija XDR detekcije/incidenta, međusobne povezanosti objekata i detaljnih informacija o svakom objektu. • Jasna vizuelizacija EDR podataka krajnjeg uređaja, gdje se može vidjeti kako je proces pokrenut, koje promjene je napravio na sistemu, kakva se mrežna komunikacija odvijala, izmjene u registrima itd. • Mora automatski povezivati pojedinačne detekcije u	

		složene incidente na osnovu uobičajenih objekata (kao što su IP adrese, krajnji uređaji, domeni, identične datoteke, detekcije, itd.). • Širok spektar akcija odgovora: računar/server - izolacija iz mreže, slanje datoteke u Sandbox, preuzmanje datoteke za dalju analizu, prijava na komandnu liniju agenta (naknadno, opcija za prekid procesa, pregled registara, sistema datoteka, memorije, itd.), pokretanje skripte (powershell/bash), blokiranje objekata (datoteka, hash, IP adresa, domen, itd.); E-mail - blokiranje elektronske pošte na osnovu pošiljaoca, premještanje elektronske pošte u karantin ili brisanje; Korisnik - odjava korisnika, blokiranje korisnika, promjena šifre korisnika. • Logovanje svih gore pomenutih akcija odgovora. • Mogućnost konfiguracije pristupa administratorskoj konzoli na osnovu uloga i dodjele specifičnih prava (Role Based Access Control – RBAC). • Opciono usluga servisa nadgledanja XDR-a (Managed Detection and Response – MDR): 24x7, slanje redovnih izveštaja, filtriranje lažnih pozitivnih rezultata (False Positive), savjetovanje prilikom suočavanja sa detektovanim incidentom, itd. • Podrška za automatizaciju zasnovanu na Playbook-ovima, npr.: podešavanje automatskih radnji odgovora na osnovu detekcije (mogućnost detaljnih podešavanja na osnovu kritičnosti detekcije ili modela detekcije), automatsko izvršavanje skripte na definisanim štićrnim stanicama pod različitim uslovima (zakazano, detekcija, ručno), upozorenje u slučaju otkrivanja nove kritične ranjivosti (notifikacija), itd. • Mogućnost prikupljanja važnih informacija za forenzičku istragu krajnjih tačaka: informacije o sistemu, informacije o	

		korisničkim nalozima, mrežne informacije, informacije o pokrenutim procesima, lista automatski startovanih objekata (Startup programs), AmCache, ShimCache, itd. • Praćenje indeksa rizika za cijelu organizaciju, kao i praćenja rizika pojedinačnih uređaja i korisnika. • Izvještaj o svim datim preporukama za smanjenje indeksa rizika, za cijelu organizaciju, kao i pojedinačnih uređaja i korisnika. • Izvještaj o loše konfugirisanim sistemima za zaštitu istog proizvođača. • Detekcija uređaja koji nemaju aktivne ključne bezbjednosne funkcije (kao što je antimalver). • Analiza kompanijskih IP adresa i domena koji su izloženi Internetu i pregled servisa koji na njima rade, kao i procjena njihovih rizika. • Automatsko upozorenje u slučaju da se kritična ranjivost pojavi na servisu/serveru izloženom Internetu • Analiza korisnika, mreže i uređaja, uključujući procjenu njihovih rizika. • Mapiranje svih događaja u organizaciji na MITRE tehnike i taktike, sa mogućnošću pretrage i filtriranja po njihovom osnovu. Standardna zaštita radnih stanica • Zaštita radnih stanica i servera od svih vrsta zlonamjernih programa (virusi, crvi, špijunski softver, grayware i drugi srodni programi). • Klijentski zaštitni zid (Firewall) sa konfiguracijom parametara prema smjeru, vrsti saobraćaja i aplikacije, potpuno integrisan u klijent antivirusa i upravljačku konzolu, sa jednostavnim definisanjem politike zaštitnog zida iz	

1	Antivirusni softver	upravljačke konzole. • Zaštita od enkripcije računara (Ransomware): proaktivno blokiranje zlonamjernih programa koji preuzimaju kontrolu nad računarom i/ili šifruju datoteke na računaru, sa mogućnošću pravljenja rezervnih kopija za oporavak šifrovanih podataka ako je proces ransomware-a odgovoran za njihovo šifrovanje. • Statična (analiza svojstva datoteka) i dinamička (analiza ponašanja datoteke) analiza korišćenjem algoritama mašinskog učenja. • Integrisana zaštita u realnom vremenu (real-time) od mrežnih crva i otkrivanje iskorišćavanja ranjivosti na IP nivou (npr. Downad/Conficker i srodne varijante mrežnih crva). • Integrisana detekcija zlonamjernog saobraćaja (klijentski IPS/IDS sistem), uključujući tipične napade na IP nivou (Ping of death, SYN flood, Teardrop, itd.); • Automatsko centralizovano čišćenje zaraženih računara bez intervencije administratora; potpuno integrisan u antivirusni klijent (čišćenje zapisa registra, ini zapisa, memorijskih procesa koje su ostavili crvi, itd.). • Automatsko čišćenje špijunskih programa potpuno integrisano u antivirusni klijent. • Zaštita od zlonamjernog koda zasnovanog na vebu (web exploits). • Blokiranje pristupa zlonamjernim veb lokacijama na nivou klijenta na osnovu IP adrese ili URL reputacije, i mogućnost definisanja fleksibilne politike filtriranja u zavisnosti od lokacije i statusa klijenta. • Provjera reputacije fajlova (File Reputation) na klijentu direktnim kontaktiranjem servera ili onlajn servisa proizvođača.	300,00 licenci

		• Automatsko prikupljanje informacija o prijetnjama i automatsko ažuriranje baze reputacije proizvođača. • POP3 Mail Scan provjerava da li ima virusa i neželjene pošte integrisane u klijentu. • Praćenje ponašanja klijenta (Behavior Monitoring) sa „In The Cloud“ provjerom da li je aplikacija poznata i bezbjedna (provjera na nivou starosti i zastupljenosti aplikacije). • Mogućnost vraćanja datoteka koje su stavljene u karantin kao sumnjive, centralno preko administratorske konzole i uz definisanje izuzetaka od budućeg karantina. • Mogućnost definisanja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) za praćenje ponašanja aplikacija , što uključuje sumnjive radnje kao što su: promjene u hosts fajlu, kreiranje duplikata poznatih sistemskih datotekeka, instaliranje novog dodatka za Internet Explorer, promjena podešavanja u Internet Explorer-u, promjena Windows Security Policy podešavanja, umetanje novog dll-a, stvaranje novog startup programa itd. Za svaku od ovih sumnjivih radnji treba da bude moguće definisati različite odgovore: od blokiranja, preko upozorenja i logovanja do dozvole za rad. • Mogućnost definisanja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) za kontrolu pristupa eksternim uređajima na klijentu (prenosivi medijumi povezani preko USB-a). • Blokiranje funkcije Autorun pri povezivanju USB diskova sa klijentom. • Kontrola pristupa mrežnim resursima i dijeljenim diskovima (network shares). • Provjera web saobraćaja, koja sprječava pokretanje zlonamjernih veb skripti i iskorišćavanje bezbjednosnih propusta u pretraživaču, u realnom vremenu.	

		• Otkrivanje i evidentiranje aktivnosti C&C komunikacije sa granularnom konfiguracijom akcija po detekciji mrežne komunikacije prema C&C serverima. • Podrška za VDI okruženja (virtuelizacija desktopa): mogućnost ograničavanja potrošnje resursa virtuelnih radnih stanica na nivou host-a - VMware vCenter (VMware View), Citrix XenServer 5.5 (Citrix XenDesktop 4). Mogućnost prethodnog skeniranja Master VDI image-a i kontrolisanog postavljanja komponenti za ažuriranje na pojedinačnim VDI host-ovima • DLP dodatak koji se može naknadno uključiti, integrisan u identično administrativno okruženje sa sledećim funkcionalnostima: o mogućnost napredne kontrole USB uređaja prema proizvođaču (ID dobavljača, serijski brojevi) o Mogućnost napredne kontrole informacija poslatih preko perifernih uređaja (COM/LPT port, IEEE 1394, uređaji za obradu slike, modem, PCMCIA port, Bluetooth, mobilni uređaji, print screen) o Mogućnost kontrole sadržaja na različitim transportnim kanalima uključujući: elektronsku poštu (SMTP), Veb (HTTP, HTTPS), FTP i SMB protokoli o Kreiranje politika u zavisnosti od lokacije klijenta/računara. o Kontrola informacija kroz: unaprijed definisane politike koje uključuju: PCI DSS pravila za otkrivanje prenosa brojeva kartica ili bankovnih računa; lične podatke kao što su OIB ili JMBG brojevi; izvorni kodovi često korišćenih programskih jezika i drugi; definisanje sopstvenih politika korišćenjem proizvoljnih ključnih riječi ili regularnih izraza. o Moguće radnje u slučaju kršenja pravila: blokiranje prenosa, omogućavanje prenosa sa evidentiranjem incidenata,	

		prikazivanje poruke upozorenja korisniku sa opcijom da se dozvoli slanje. o Mogućnost provjere cijelog računara na osjetljive informacije, uz mogućnost evidentiranja pronađenih informacija. o Mogućnost propuštanja osjetljivih podataka na osnovu rezonovanja korisnika (unos razloga). • Podrška za ograničavanje opterećenja CPU-a prilikom zakazanog antimalver skeniranja (Scheduled Scan). • Integrisana podrška za distribuciju komponenti ažuriranja u scenarijima sa nižim propusnim opsegom (Update Relay). • Podrška za više izvora ažuriranja komponenti na osnovu IP adrese klijenta. • Verifikacija digitalnog potpisa MSI paketa prije instaliranja programa i mogućnost zabrane instalacije nepoznatih programa preuzetih preko Veb ili email kanala. • Automatska integracija sa rješenjem za otkrivanje naprednih prijetnji kroz Sandbox: automatska prevencija napada na krajnju tačku na osnovu informacija dobijenih od Sandbox-a (sumnjivi saobraćaj, promjene sistema itd.). • Podrška za rad sa nekoliko zasebnih korisnika/organizacija na istom sistemu (multi-tenancy). • Podrška za zaštitu Microsoft Windows (Server i Desktop) i MacOS, 32 i 64-bitne operativne sisteme.	