PREGLED POSTUPKA #98725

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	Isporuka i implementacija sigurnosnog softverskog rješenja za napredni monitoring I zaštitu: Integrated Security Information & Event Management (SIEM) Platform, NDR, OPEN XDR sa uslugom MDR
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Snežana Obradović
Kontakt	zana.obradovic@monstat.org
Datum objave	02.09.2025. 09:45

Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Isporuka i implementacija sigurnosnog softverskog rješenja za napredni monitoring I zaštitu: Integrated Security Information & Event Management (SIEM) Platform, NDR, OPEN XDR sa uslugom MDR	02.09.2025 09:45	10.09.2025 10:00	10.09.2025 10:00	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
Nabavka je	
Zelena	Ne
Društveno odgovorna	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2025	**UPRAVA ZA STATISTIKU** **Isporuka i implementacija sigurnosnog softverskog rješenja za napredni monitoring I zaštitu: Integrated Security Information & Event Management (SIEM) Platform, NDR, OPEN XDR sa uslugom MDR** 72000000 - IT usluge: konsalting, izrada softvera, Internet i podrška	21.541,82 EUR	4.523,78 EUR	-	-	-	Jednostavna nabavka

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, 020/23 , 36/23 , 114/23, 049/24, 114/24), dostaviti Izjavu ponuđača(Obrazac 2) o ispunjenosti uslova utvđenih zahtjevom i nepostojanju sukoba interesa, potpisanu od strane ovlašćenog lica ponuđača, datu na Obrascu 2. Izjava mora biti potpisana elektronskim potpisom.	Obrazac 2
Rok važenja ponude je 90 dana od dana otvaranja ponuda.	Rok važenja ponude
EN ISO 9001:2015 – Sistem menadžmenta kvalitetom	Dokaz odnosno sertifikat, koje izdaju akreditovana sertifikaciona tijela o ispunjavanju uslova kvaliteta predmeta nabavke
ISO/IEC 27001:2013 – Sistem menadžmenta bezbjednošću informacija	Stručna i tehnička sposobnost
ISO/IEC 20000-1:2013 – Sistem menadžmenta IT usluga i servisa	Stručna i tehnička sposobnost
Privredni subjekat (Ponuđač) je dužan da posjeduje minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora i to: • Minimum 4 stručna lica koja će biti angažovana na poslovima instaliranja i konfigurisanja ponuđenih softverskih rješenja, što se dokazuje: 1) dokazom o radnom angažovanju (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) i 2)sertifikatom ili potvrdom proizvođača softvera o važećim sertifikatima za stručno lice.	Stručna i tehnička sposobnost

Privredni subjekat (Ponuđač) je dužan da posjeduje minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora i to: Minimum 5 stručna lica za potpuno operativno praćenje SIEM rješenja i ostalih implementiranih bezbjednosnih rješenja po modelu 24x7x365 od strane stručno-specijalističkog osoblja ponuđača sa “CompTIA Security + “sertifikatom ili GIAC GSEC, ISC2 SSCP, ISACA CRISC/CISM, što se dokazuje:1. dokazom o radnom angažovanju (dokazom o radnom angažovanju (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) i 2.sertifikatom.	Stručna i tehnička sposobnost
Privredni subjekat (Ponuđač) je dužan da posjeduje minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora i to: Minimum 3 stručna lica / specijaliste za afektovane tehnologije i eksperte za bezbjednost, za realizaciju dodatnih analiza, izradu i pokretanje plana za otklanjanje problema, sa “CompTIA CASP+ “ (Security X) ili CISSP (Security Operations) ili GIAC GCIH sertifikatom, što se dokazuje: 1.dokazom o radnom angažovanju (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) i 2. sertifikatom .	Stručna i tehnička sposobnost
Privredni subjekat (Ponuđač) je dužan da posjeduje minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora i to: Minimum 3 stručna lica / specijaliste za preporuke za bezbjednosna unaprijeđenja sistema naručioca sa “CompTIA Cybersecurity Analyst - CySA+” ili ISSP, GIAC GSEC/GCIH, CRISC, CISM, CISA sertifikatom, kao i 1sertifikatom “CompTIA PenTest+” ili EC-Council Certified Ethical Hacker (CEH) ili Offensive Security Certified Professional (OSCP) ili GIAC Penetration Tester (GPEN), što se dokazuje:1. dokazom o radnom angažovanju (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) i 2. sertifikatom.	Stručna i tehnička sposobnost
Ponuđač mora da u svojoj ponudi dostavi najmanje 2 potvrde o izvršenim uslugama, Isporuka i implementacija sigurnosnog softverskog rješenja za napredni monitoring I zaštitu: Integrated Security Information & Event Management (SIEM) Platform, NDR, OPEN XDR sa uslugom MDR, sa minimum 100 licenci, tokom prethodnih godina, ali ne duže od 5 godina, računajući i godinu u kojoj je započet postupak javne nabavke. Potvrde treba da sadrže opis i vrijednost predmeta nabavke, vrijeme realizacije ugovora i konstataciju da je ugovor blagovremeno i kvalitetno izvršen.	Stručna i tehnička sposobnost

Neophodno je da ponudjač pruža usluge MDR sa zaposlenim čije je mjesto angažovanja na teritoriji Crne Gore, što se dokazuje potvrdom o prebivalištu angažavanog lica izdatog od strane nadležnog organa.	Stručna i tehnička sposobnost
Ponuđač je dužan da dostavi potvrdu proizvođača ponuđenih softerskih rješenja ili njenog ovlašćenog predstavnika, kojom potvrđuje da su ponuđene licence sa minimalno 1 godinom tehničke podrške proizvođača.	Garantni rok
Neophodno je da ponuđač ima rješenje i dozvolu za pristup tajnim podacima klasifikovanosti „TAJNO“ izdato od Direkcije za zaštitu tajnih podataka Crne Gore.	Drugi uslovi
Rok isporuke i implementacije ponuđenih softverskih licenci je 30 dana,od dana zaključenja ugovora.	Rok izvršenja ugovora
Tehnička podrška, tražena po zahtjevu naručioca je 12 mjeseci od dana isporuke i implementacije ponuđenih softverskih rješenja.	Drugi uslovi
Mjesto izvršenja ugovora: Uprava za statistiku.	Mjesto izvršenja ugovora
Plaćanje usluge će se vršiti u roku do 30 dana nakon potpisivanja zapisnika o izvršenoj usluzi koji će potpisati predstavnici naručioca i izvršioca. Uredno ispostavljena faktura i zapisnik o izvršenim uslugama potpisan od strane predstavnika Naručioca predstavlja osnov za plaćanje ugovorene cijene.	Rok plaćanja
Način plaćanja: virmanski.	Način plaćanja
Način sprovođenja kontrole kvaliteta: Kvalitet izvršene usluge će se utvrđivati neposredno od strane ovlašćenih lica Naručioca u mjestu izvršenja usluge, prilikom prijema izvršene usluge. Ova lica će prilikom prijema usluge vršiti kontrolu da li izvršena usluga odgovara opisu i bitnim karakteristikama koji su definisani tehničkom specifikacijom Naručioca i ponudom. Ukoliko se ustanovi da je izvršena usluga u svemu u skladu sa opisom i bitnim karakteristikama koji su definisani tehničkom specifikacijom Naručioca i ponudom, Naručilac sačinjava Zapisnik o prijemu. Ukoliko se prilikom prijema ugovorene usluge ustanovi da postoje nedostaci u izvršenoj usluzi, sačiniće se Zapisnik o utvrđenim nedostacima koji potpisuju predstavnici Naručioca i Izvršioca usluge i Izvršilac usluge će biti u obavezi da iste otkloni u roku koji mu odrede ovlašćena lica Naručioca.	Način sprovođenja kontrole kvaliteta

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **21.541,82 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		Isporuka i implementacija sigurnosnog softverskog rješenja za napredni monitoring i zaštitu: Integrated Security Information & Event Management (SIEM) Platform, NDR, OPEN XDR sa uslugom MDR Rješenje mora da ima slijedeće karakteristike: - Rješenje mora biti zasnovano na softveru koje se može instalirati i na lokalnim virtuelnim resursima, javnim okruženjima u Cloudu i takođe da se isporučuje kao Saas rješenje. - Rješenje mora imati sistem za upravljanje predmetima (Case management) sa grafičkim pogledom na slučaj i dokaze. - Sandboxing zasnovan na punoj emulaciji sistema, mora da detektuje napade u više faza i gde je eksploatacija koja se podijelila na više objekata. - Rješenje treba da bude u stanju da identifikuje prijetnje u bilo kom tipu datoteke. - Rješenje mora imati mogućnost praćenje integriteta fajlova. - Predloženo rješenje mora obezbijediti napredne mogućnosti korelacije za otkrivanje bezbjednosnih incidenata kao što su:	

		a. DDOS napadi b. Worm Outbake c. Port Scan d. SQL injection e. Brute Force napad - Rješenje mora imati GUI zasnovan na Webu samo sa HTTPS protokolom - Rješenje mora da koristi algoritme zasnovane na mašinskom učenju. - Rješenje treba da podržava Inline režim blokiranja (ne TCP Reset). - Rješenje treba da podržava integraciju sa forenzičkim alatima. - Rješenje mora da obezbijedi unaprijed upakovan Inteligence modul za sistem baze podataka, kao što su Informix, Mysql, DB2, Oracle i slicno - Rješenje mora da obezbijedi unaprijed upakovan Inteligence modul, kontrolnu tablu i izveštaj za Wind - Rješenje mora doći sa integracijom sa najmanje pet open-source threat inteligence. - Rješenje mora da obezbijedi potpunu zaštitu od APT napada putem mreže, web-a. - Rješenje mora da podržava obavještenje o događaju u XML, JSON ili TEKST formatima. - Rješenje mora biti u stanju da kategorizuje ozbiljnosti incidenta povezane za upozorenja. - Rješenje mora biti u stanju da primijeni Supervised and Unsupervised Machine Learning and Adaptive Machine Learning na logove ili saobraćaj koji prima od: o IDS, Firewall, Network traffic, Windows or Linux systems, AWS Cloudtrail, Office 365, G-Suite, SNMP, OKTA, Nessus, Rapid7, Tenable, Syslogs, CEF, LEEF, Netflow, JSON - Rješenje ima mogućnost primjene Machine Learning na Firewall i IDS	

		- Rješenje mora imati više senzora za prikupljanje podataka, uključujući senzore za bezbjednost mreže i agent sensora. - Rješenje mora da obezbijedi Managed Services za aplikaciju sa stalnim neograničenim ažuriranjem kontrolne table i korelacijskim upitima. - Senzori rješenja moraju da hvataju mrežne podatke i šalju samo relevantne podatke procesoru za analizu. - Rješenje mora da obezbijedi integrisanu analizu mrežnog saobraćaja (NTA). - Rješenje mora da obezbijedi tehnologiju obmane / honeypot-a. - Predloženo rješenje mora biti u stanju da podrži i agent i agentless prikupljanju logova. - Rješenje mora biti sposobno da izvrši nadgledanje servera i mrežne infrastrukture Out of box. - Rješenje mora biti sposobno za obavljanje nadgledanja aplikacija out of box. - Rješenje mora da podrži Geo Location Public IP look up - Rješenje mora da prilagodi in-house bezbjednosne logove i isporuči on-the-fly korelaciju za logove - Rješenje mora biti u stanju da unese sve podatke (korisnike, aplikacije) i učini ih dostupnim za upotrebu - praćenje, upozorenje (alert), istraga, ad hoc pretraživanje. - Rješenje mora da obezbijedi fleksibilnost za integraciju sa 3rd party providers alatima i portalima za izveštavanje - Rješenje će biti u stanju da uhvati novi događaj sa izvornih uređaja bez čitanja kroz cjelokupne podatke od početka. - Rješenje mora da obezbijedi prikaz za sirove podatke koji se čuvaju. - Rješenje treba da uskladi sva upozorenja sa Cyber Security Killchain-om.	

		- Rješenje mora da obezbijedi opis otkrivenog malvera. - Rješenje mora da obezbijedi supervised and unsupervised machine learning funkcionalnost. - Rješenje mora da obezbijedi Artificial Intelligence and Machine Learning funkcionalnost - Rješenje mora da obezbijedi integrisani IDS. - Rješenje mora imati mogućnost slanja upozorenje odgovarajućem osoblju u vezi sa bezbjednosnim problemom na osnovu koreliranog događaja. - Rješenje mora pratiti promjene i osiguranje okruženje nadgledanjem sumnjivih aktivnosti, promjena korisničkih uloga, neovlašćenog pristupa. - Rješenje mora biti u stanju da otkrije ugrožene računare i servere povezane sa naprednim prijetnjama i malware infekcijama - Rješenje mora izdati upozorenje nakon otkrivanja spoljne IP adrese na crnoj listi. - Rješenje mora biti u stanju da prati nepoznate prijetnje. - Rješenje mora biti u stanju da otkrije sisteme sa ograničenim kapacitetom ili u stanju mirovanja. - Rješenje mora imati mogućnosti analitike ponašanja korisnika. - Rješenje mora imati unaprijed izgrađena pravila detekcije izgrađena na osnovu kompatibilnosti Ciber Security Kill Chain Framework i Mitre Attack Framework - Rješenje mora biti u stanju da maskira (npr. lozinku, broj kreditne kartice) podatke prije nego što ih sačuva. - Rješenje mora automatski pratiti poznate loše događaje i koristiti sofisticiranu korelaciju putem pretrage, kako bi pronašlo poznate obrasce rizika kao što su napadi brute force, curenje podataka, pa čak i prevara na nivou aplikacije.	

		- Rješenje mora biti potpuno prilagodljivo prilikom kreiranja upozorenja ili alarma za događaje visokog rizika. - Predloženo rješenje mora biti u stanju da obezbijedi funkciju pretrage koja podržava jednostavnu pretragu obrazaca u Boolean stilu, kao i složene regularne izraze. - Rješenje mora biti u stanju da omogući analitičaru da napravi upite koristeći kombinovani metod pretrage. Jedan upit može sadržati ključne riječi, uslove zasnovane na polju i regularne izraze. - Rješenje mora biti u stanju da poveže i identifikuje probleme sa performansama aplikacije zbog bezbjednosnih incidenata (npr. DDOS napadi, neovlašćeni pristup sistemu koji izaziva probleme sa performansama aplikacije). - Rješenje mora da podrži mogućnost povezivanja sa Threat Intelligence u Alert-u. - Rješenje mora podržavati podršku za inteligentni interfejs za upravljanje platformom (IPMI). - Rješenje mora omogućiti instalaciju senzora na virtuelnim serverskim instancama. - Rješenje mora biti u stanju da obezbijedi korelaciju događaja sa više tipova uređaja. - Rješenje mora da obezbijedi dubinsku analizu i izveštavanje o trendovima threat actor-a. - Rješenje mora da obezbijedi analizu IP adresa i domena na zahtjev. - Rješenje mora imati potpuno komercijalnu Kibana licencu ugrađenu. - Rješenje mora imati SOAR (Securiti Orchestration Autmation Repsonse) mogućnosti za email, Case management, Firewall i Active Directory - SIEM plugin prenosi događaje i detekcije SOAR dodatka za	

		automatsko pokretanje Plabook-ova koji se nalaze u orkestraciji proizvoda za obavljanje različitih instrukcija koje mogu uključivati izvršavanje skripti ili integraciju sa drugim alatima u okruženju. - Rješenje mora imati sposobnost za threat hunting i automatizuje threat hunting i primijeni se na SOAR - Rješenje mora da ima već unaprijed izgrađene šablone za opšte izvještavanje i izvještaje o usaglašenosti. - Rješenje treba da bude u stanju da otkrije prijetnje koje ciljaju različite operativne sisteme. - Rješenje mora podržavati Authentication Authorization Accounting (AAA). - Rješenje mora da obezbijedi opis porodice malvera. - Rješenje mora imati sposobnost da izvrši analizu ranjivosti i kill chain analizu najslabije karike. - Ažuriranje sandbox-inga može se obaviti online bez ručne intervencije. Sandboxing koji će se implementirati, održavati i isporučivati od strane vendora proizvoda. - Sandbox mora da koristi emulaciju punog sistema za analizu objekata kako bi se spriječile tehnike Environment Fingerprinting, Network Fingerprinting algorithms, i identification of time-based actions. - Rješenje mora kombinovati potpise i vještačku inteligenciju za suzbijanje alert noise upozorenja i identifikovati high fidelity signature anomalija. SIEM zahtjevi koji moraju biti ispunjeni kao dio ponude: - Rješenje mora biti u stanju da prikupi količine podataka bez ograničavanja broja uređaja za prikupljanje. - Rješenje ne smije da ograničava broj korisnika u sistemu,	

1	Isporuka i implementacija sigurnosnog softverskog rješenja za napredni monitoring i zaštitu: Integrated Security Information & Event Management (SIEM) Platform, NDR, OPEN XDR sa uslugom MDR	pretrage, upozorenja, korelacije, izveštaje, kontrolne table. - Prikupiti sve vrste logova i podataka iz različitih izvora, tj sislog, custom/ in home aplikacija, i logova baze podataka - Konsolidaciju svih prikupljenih logova u centralni repozitorijum. - Obavlja evidencije, agregaciju i normalizaciju. - Analizirati i povezati bezbjednosni događaj. - Poslati upozorenje odgovarajućem osoblju u vezi sa bezbjednosnim problemom na osnovu koreliranog događaja. - Rješenje mora imati integrisanu bazu prijetnji, incidente i upravljanje usklađenošću - Rješenje mora da sadrži senzor za prikupljanje podataka - Predloženo rješenje će biti u stanju da podrži i agent i agentless based prikupljanje logova. - Rješenje mora biti sposobno da izvrši nadgledanje servera i mrežne infrastrukture out of the box. - Rješenje mora biti sposobno za obavljanje nadgledanja aplikacija iz out of the box. - Rješenje mora biti u stanju da maskira (npr. lozinku, broj kreditne kartice) podatke prije nego što ih sačuva. - Rješenje mora biti u stanju da poveže informacije o imovini sa podacima o prijetnji i ranjivosti - Rješenje mora da obezbijedi prikaz za sirove podatke koji se čuvaju - Rješenje mora da konsoliduje prijetnje normalizacijom, reputacijom, znanjem i nosivošću događaja koji je pokrenuo - Rješenje mora imati praćenje integriteta fajlova - Predloženo rješenje mora biti u stanju da izvrši subsearch u odnosu na bezbjednost na vrhu trenutne pretrage - Rješenje mora da obezbijedi vizuelno izveštavanje koje može da pretvori bezbjednosne probleme u poslovni rizik / gubitak i	1,00 komplet

		uticaj. - Rješenje mora biti u stanju da poveže sistemske metrike i podatke o događajima sa podacima iz drugih tehnoloških nivoa - Rješenje mora biti u stanju da pronađe uzročno-posledične veze između problema sa performansama aplikacija i osnovnog OS-a, hipervizora, skladištenja, mreže i serverske infrastrukture - Rješenje mora biti u stanju da unese sve podatke (korisnike, aplikacije) i učini ih dostupnim za upotrebu - praćenje, alert, istraga, ad hoc pretraživanje - Rješenje mora da obezbedi integraciju sa naprednim bezbednosnim advisory modulom. - Rješenje mora da obezbijedi data integraciju za Risk Analytic - Rješenje mora da pruži podršku za Risk and Cyber Threat Advisory Alert. - Rješenje mora imati Case management sistem sa grafičkim pogledom na slučaj i dokazima - Rješenje mora da ima mogućnost konsolidovanog preuzimanja sigurnosnog sadržaja za upravljane uređaje. Network Traffic Analizer - Arhitektura mora biti veoma opsežna u modulu analize mrežnog saobraćaja koristeći i supervised i unsupervised učenje - Mora da obezbjeđuje praćenje interakcije između uređaja, usluga, aplikacija koje se pokreću na mreži u realnom vremenu i istorijski. - Uređaj za NDR funkcionalnost mora da omogući deep packet inspection, da je opremljen sa minimalno 6 x 1 Gbps	

		interfejsom, mora da obezbjeđuje funkciju normalizovanja podataka iz inspektovanog mrežnog saobraćaja sa mogućnošću baferovanja i naknadnog dostavljanja neophodni podataka centralnoj platformi. - Network Traffic Analysis mora da uključuje: o Network performance statistics o Server performance o Application detection and performance monitoring o Top sources & Top destinations o Asset throughput o Asset application performance o Application processing time o Network interactions with asset o HTTP i HTTPS statistics o DNS statistics o Asset discovery and statistics o IP address o Device Manufacturer o Application Services o Time discovered and last seen o Asset tag(s) and description o Server certificate visibility. Autokorelacija - Mora da normalizuje različite formate podataka unesene u zajednički format - Mora da može da uradi autokorelaciju više izvore podataka - Mora da uradi autokorelaciju upozorenja o mašinskom učenju visoke vernosti koja se nalaze u cijelom napadu (attack landscape)	

		- Mora da obezbijedi grafički prikaz koreliranih upozorenja o mašinskom učenju visoke vjernosti (high fidelity machine learning alerts). - Mora biti u stanju da unese podatke commom EDR rješenja. - EDR uneseni podaci moraju biti autokorelirani sa drugim izvorima podataka. - Mora da primijeni Mašinsko učenje na EDR unesene podatke. - Mora da prikaže sve povezane EDR detekcije na incident view. Rješenje mora biti licencirano za zaštitu i nadgledanje 150 korisničkih asseta (uređaja i/ili korisnika) na period od godinu dana, sa uključenim svim neophodnim resursima (hardverskim i softevrskim) za isporuku traženih funkcionalnosti. Rješenje mora biti instalirano, konfigurisano, testirano i pušteno u rad uključujuću realizaciju svih integrativnih konfiguracija sa postojećom infrastrukturom i ostalim rješenjima iz ove nabavke. Implementator je dužan izraditi i dostaviti dokumentaciju izvedenog stanja. Implementator je dužan isporučiti 3 dana treninga za dva tehnička lica naručioca za upravljanje rješenjem. MDR usluga Monitoring implementiranih integrisanih sistema 24/7, detekcije, analize, kategorizacije, eskalacije i razrješavanja	

		bezbjednosnih događaja (incidenata), podrške stručno-specijalističkog osoblja na lokaciji naručioca na aktivnostima razrješavanja bezbjednosnih propusta i incidenata na korisničkim platformama, izrade preporuka za bezbjednosna unaprijeđenja sistema naručioca, izvještavanje o uslugama (u trajanju od godinu dana od dana sklapanja ugovora): MDR usluga monitoringa implementiranih integrisanih sistema 24/7: • Obaveza ponuđača je potpuno operativno praćenje SIEM rješenja i ostalih implementiranih bezbjednosnih rješenja od strane stručno-specilističkog osoblja ponuđača po modelu 24x7x365, iz za datu namjenu opremljenog prostora. • Obaveza ponuđača je da omogući pristup SIEM rješenja i ostalim implementiranih bezbjednosnih rješenja u cilju ostvarenja uvida u stanje sistema. Detekcija, analiza, kategorizacija, eskalacija i razrješavanje bezbjednosnih događaja (incidenata): • Obaveza ponuđača je neposredno po detekciji bezbjednosnih incidenata realizuje analizu i kategorizaciju događaja po slijedećem modelu: o Informativni bezbjednosni događaji: Informativni bezbjednosni događaj je događaj koji nema negativan uticaj na bezbjednost, kao npr. manja ranjivost, obavještenje ili upozorenje, itd o Manji bezbjednosni događaj: Manji bezbjednosni događaj predstavlja neusklađenost sa bezbjednosnom politikom, preporučenim popravkama itd. Označava potencijalnu bezbjednosnu prijetnju opremi, korisniku ili uslugama o Veliki bezbjednosni događaj: Veliki bezbjednosni događaj	

		predstavlja identifikovani bezbjednosni događaj koji može dovesti do bezbjednosnog incidenta. Veliki bezbjednosni događaj čine događaji kao npr ne-blokirani zlonamjerni kod ili neočekivani niz događaja na nivou sistema. Preko ugrožene krajnje tačke, ovi događaji mogu uticati na dostupnost usluga, podataka i ozbiljno uticati na operacije. o Kritični bezbjednosni događaj - incident: Kritični bezbjednosni incident je bezbjednosni incident koji se može ili se već pretvorio u bezbjednosni incident. Kritični bezbjednosni incident je otkrivanje zlonamjernog sadržaja ili softverskog koda koji uzrokuje nedostupnost usluga ili podataka, krađu i zloupotrebu podataka, te posledično veću poslovnu štetu. Događaji ovog tipa se tretiraju prioritetno. • Obaveza ponuđača po kategorijama bezbjednosnih dođaja je: o Za Informativni bezbjednosni događaji: U roku od 24h realizovati dodatnu analizu, izraditi plan za otklanjanje rizika. o Za Manji bezbjednosni događaj: U roku od 12h realizovati eskaliranje događaja na specijaliste za afektovane tehnologije, realizovati dodatnu analizu, izraditi plan za otklanjanje problema. o Za Veliki bezbjednosni događaj: U roku od 5h realizovati eskaliranje događaja na specijaliste za afektovane tehnologije i/ili na eksperte za bezbjednost , realizovati dodatnu analizu, izraditi i pokrenuti plan za otklanjanje problema. o Za Kritični bezbjednosni događaj - incident: U roku od 3h realizovati eskaliranje događaja na specijaliste za afektovane tehnologije i eksperte za bezbjednost, realizovati dodatnu analizu, izraditi i pokrenuti plan za otklanjanje problema. • Obaveza ponuđača je da izradi i sa naručiocem usaglasi komunikacini plan koji će omogućiti blagovremenu	

informisanost naručioca o bezbjednosnim događajima, aktivnostima na razrješavanjeu bezbjednosnih događaja i bezbjednosnom stanju sistema.

Podrške stručno-specijalističkog osoblja na lokaciji naručioca na aktivnostima razrješavanja bezbjednosnih propusta i incidenata na korisničkim platformama:
• Obaveza ponuđača je da obezbjedi naručiocu podršku za realizaciju plana otklanjanja problema angažovanjem stručno-specijalističko osoblje koje će na lokaciji korisnika realizovati planske i ostale aktivnosti u cilju otklanjanja utvrđenih ranjivosti, otklanjanja utvrđenih bezbjednosnih propusta u konfiguraciji sistema ili otklanjanja poslijedica prouzrokovanih bezbjednosnim događajima - incidentima. Sve aktivnosti se raliziju u saradnji sa naručiocem.

Izrade preporuka za bezbjednosna unaprijeđenja sistema naručioca:
• Obaveza ponuđača je da prati preporuke vendora korištenih sistema te da ih blagovremeno pretoči u preporuke za bezbjednosna unaprijeđenja sistema naručioca.

Izvještavanje o uslugama:
• Obaveza ponuđača je blagovremeno izvještavanje naručioca o bezbjednosnom stanju sistema, a prema gore navedenom komunikacionom planu, a podrazumjeva obavezu:
o Izrade redovnog mjesečnog kumulativnog izvještaja o bezbjednosnom stanju sistema.
o Izradu izvještaja o Manjim bezbjednosnim događajima, Većim bezbjednosnim događajima i Kritičnim bezbjednosnim događajima u roku od 24h po događaju.

		o Izradu izvještaja o Podršci stručno-specijalističkog osoblja na lokaciji naručioca u roku od 24h po isporučenoj usluzi.	