

## PREGLED POSTUPKA #100567

### 1 PODACI O NARUČIOCU

Naziv naručioca	UPRAVA ZA IZVRŠENJE KRIVIČNIH SANKCIJA
PIB	02000458
E-mail	tina.perovic@ziks.me
Telefon	020/243-100
Internet adresa	www.ziks.gov.me
Fax	020/243-567
Adresa	Velje brdo bb
Grad	Podgorica
Poštanski broj	81000

### 2 OSNOVNI PODACI

Opis predmeta javne nabavke	Implementacija sistema za automatizaciju zaštite informatičkog sistem (prvi ponovljeni postupak)
Status	U izradi
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Nevena Mentović
Kontakt	020/243-100
Datum objave	29.09.2025. 12:00

Napomena

SOAR sistem i zavisne komponente moraju biti zasnovane na rješenjima otvorenog koda (open source). SOAR rješenje mora biti implementirano kroz sledeće module:

Modul 1: Detekcija i Odgovor na Krajnjim Tačkama i Sistemima

Modul 2: Upravljanje Log Podacima sa Naprednom Detekcijom

Modul 3: Platforma za Orkestraciju i Automatizaciju

Modul 4: Platforma za Obavještajne Podatke o Prijetnjama

### 3 FAZE U POSTUPKU

Nema faza u izabranom postupku

### 4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
<b>Posebni oblici javne nabavke</b>	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
<b>Nabavka se sprovodi kao</b>	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne
<b>Nabavka je</b>	
Zelena	Ne
Društveno odgovorna	Ne

### 5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2025	<b>UPRAVA ZA IZVRŠENJE KRIVIČNIH SANKCIJA</b> <b>Implementacija sistema za automatizaciju zaštite informatičkog sistema</b> 48214000 - Softverski paket za mrežni operacionalni sistem 48219500 - Softverski paket za svič ili ruter 48900000 - Razni softverski paketi i kompjuterski sistemi 72260000 - Usluge vezane za softver	20.000,09 EUR	4.199,91 EUR	-	-	-	Jednostavna nabavka

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

Opis	Tip uslova / zahtjeva
U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja ili potvrde nadležnog organa izdatog na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište.	Obavezni uslovi
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje. Dokaz: uvjerenje, potvrde ili drugi akt koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište, radi utvrđivanja ispunjenosti uslova iz člana 99 stav 1 tačka 2 Zakona o javnim nabavkama.	Obavezni uslovi
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je upisan u Centralni registar privrednih subjekata ili drugi odgovarajući registar u državi u kojoj privredni subjekat ima sjedište što se dokazuje dostavljanjem dokaza o registraciji u Centralnom registru privrednih subjekata ili drugom odgovarajućem registru, sa podacima o ovlašćenom licu privrednog subjekta.	Uslovi za obavljanje djelatnosti
Izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, koja se sačinjava na Obrascu 2 iz Pravilnika o načinu sprovođenja jednostavnih nabavki („Službeni list CG“, broj 16/23 i 20/23,36/2023,114/2023,49/2024 i 114/2024).	Obrazac 2

Mjesto izvršenja ugovora Uprava za izvršenje krivičnih sankcija, Velje brdo bb Podgorica.	Mjesto izvršenja ugovora
Rok plaćanja: 30 dana od dana dostavljanja fakture sa otpremnicom.	Rok plaćanja
Način plaćanja je: virmanski Na žiro račun Dobavljača žiro račun: _____. Banka: _____ (Ponudač je obavezan navesti broj žiro računa i banke).	Način plaćanja
Period važenja ponude je 60 dana od dana javnog otvaranja ponuda	Rok važenja ponude
Ponudač treba da priloži dokaz kojim dokazuje da posjeduje minimum 2 reference za implementaciju sistema koji je predmet nabavke (SOAR) zasnovanih na open-source rješenju zajedno sa zavisnim modulima zasnovanih na open-source rješenjima.	Stručna i tehnička sposobnost
Ponudač treba posjedovati minimum stručnih i kadrovskih kapaciteta koji su potrebni za izvršenje ugovora i to: minimum jedno lice sa CISM (Certified Information Security Manager) ili CISSP (Certified Information Systems Security Professional) ili C-CISO (Certified Chief Information Security Officer) sertifikatom. Dokaz o angažovanju radne snage (prijava na osiguranje zaposlenog, ugovor o radu, sporazum o preuzimanju zaposlenog, ugovor o korišćenju sposobnosti drugog subjekta ili drugi akt u skladu sa zakonom) sa odgovarajućim referencama koje su potrebne za izvršenje predmeta nabavke	Stručna i tehnička sposobnost
Rok izvršenja ugovora: U roku od maksimalno 45 dana od dana zaključenja ugovora.	Rok izvršenja ugovora

## 7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

## 8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **20.000,09 EUR**

### TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		<p>Modul 1: Detekcija i Odgovor na Krajnjim Tačkama i Sistemima</p> <p>Otvoreno-kodna sigurnosna platforma koja obezbjeđuje objedinjenu prevenciju, detekciju i odgovor na prijetnje u različitim okruženjima uključujući krajnje tačke, servere i kontejnere. Modul omogućava centralizovano upravljanje sigurnošću, pružajući vidljivost i kontrolu kroz infrastrukturu, i olakšava brzo otkrivanje i odgovor na prijetnje putem automatizovane analize i alarma, a na osnovu toga može izvršiti "izolaciju" krajnje tačke. Funkcionalni moduli moraju osigurati bezbjednost, usklađenost i operativnu higijenu za IT okruženja svih veličina. Modul mora biti visoko skalabilan i podržavati integraciju sa alatima trećih strana za naprednu vizualizaciju i automatizaciju najmanje putem webhooks i API-ja.</p> <p>Modul mora kombinovati nadzor zasnovan na agentima i bez agenata za prikupljanje, analizu i korelaciju sigurnosnih podataka iz različitih sistema kao što su krajnje tačke, mrežni uređaji i kontejneri. Ključne arhitektonske komponente moraju uključivati agenta i server za upravljanje, kao i integraciju sa drugim modulima.</p>	

1	Modul 1: Detekcija i Odgovor na Krajnjim Tačkama i Sistemima	<p>Ovaj modul će djelovati kao sloj za sigurnosni nadzor krajnjih tačkaka i servera. Koristi agente instalirane na krajnjim tačkama i serverima, koji prikupljaju logove, prate procese, provjeravaju konfiguracije i šalju događaje centralnom serveru za upravljanje. Server obrađuje događaje, primjenjuje pravila detekcije i može pokrenuti automatizovane odgovore kao što je izolacija računara. Takođe obrađene događaje šalje dalje u sistemu konkretno modulu 3 na dalju obradu. Zajedno sa indeksatorom i komandnom tablom, modul pruža vidljivost, otkrivanje ranjivosti, provjere usklađenosti i aktivan odgovor.</p> <p>Glavne Funkcionalnosti</p> <ul style="list-style-type: none"><li>- Detekcija Upada: Skenira malver, sumnjive anomalije, rootkit-e, skrivene fajlove, neovlašćene procese i mrežne aktivnosti.</li><li>- Analiza Log Podataka: Prikuplja i korelira logove iz sistema i aplikacija.</li><li>- Detekcija Ranjivosti: Identifikuje zastarjeli softver poređenjem sa CVE bazama.</li><li>- Procjena Konfiguracije: Nadgleda postavke sistema i aplikacija radi usklađenosti.</li><li>- Odgovor na Incidente: Podržava automatizovane kontramjere i alate za forenziku.</li><li>- Regulatorna i Usklađenost: Omogućava izvještaje i panele za standarde poput GDPR-a is sličnih bezbjedonosnih standarda.</li></ul>	1,00 komad
---	--	--	------------

2	Modul 2: Upravljanje Log Podacima sa Naprednom Detekcijom	<p>Otvoreno-kodna sigurnosna platforma koja obezbeđuje napredno upravljanje logovima, integrišući alate kao što su Sigma i JARA za unaprijeđenu detekciju. Njegova glavna funkcionalnost je prikupljanje, normalizacija, obogaćivanje i analiza mrežnih i krajnjih logova iz više izvora, omogućavajući duboku vidljivost i forenzičke kapacitete za sigurnosne operacije. Mora obezbijediti panele, alarme i upravljanje slučajevima, čineći ga pogodnim za implementaciju na nivou preduzeća.</p> <p>Ovaj modul funkcioniše kao sloj za nadzor i upravljanje logovima. Sigma pravila omogućavaju kreiranje detekcija koje izazivaju alarme pri sumnjivom ponašanju. Izvučeni fajlovi iz mrežnog saobraćaja mogu se skenirati pomoću JARA pravila radi identifikacije malvera. Modul obezbeđuje panele za lov na prijetnje, dugoročno skladištenje i forenzičku reprodukciju mrežnog saobraćaja. Takođe obrađene događaje šalje dalje u sistemu konkretno modulu 3 na dalju obradu</p> <p>Glavne Funkcionalnosti</p> <ul style="list-style-type: none"> <li>- Objedinjeno Prikupljanje Logova</li> <li>- Normalizacija i Obogaćivanje</li> <li>- Pravila Detekcije (Sigma i YARA)</li> <li>- Alarmiranje i Korelacija</li> <li>- Paneli i Pretraga</li> <li>- Forenzika i Istraga Incidenata</li> <li>- Usklađenost i Revizijski Tragovi</li> </ul>	1,00 komad
---	---	--	------------

3	Modul 3: Platforma za Orkestraciju i Automatizaciju	<p>Otvoreno-kodna platforma sa “drag-and-drop” dizajnerom za automatizaciju, koja omogućava integraciju i sopstvenog koda za složene scenarije.</p> <p>Platforma nudi veliki broj unaprijed definisanih integracija i podržava “self-hosted” modele implementacije, obezbjeđujući potpunu kontrolu nad podacima i fleksibilno skaliranje.</p> <p>Omogućava bogat set integracija i podršku za rad sa API-jima, što omogućava i tehničkim i netehničkim korisnicima da grade i održavaju sigurnosnu automatizaciju.</p> <p>Ovaj modul služi kao “mozak” za orkestraciju i automatizaciju SOAR sistema. On izvršava “playbook”-e koji povezuju detekciju, log menadžment i obavještajne podatke o prijetnjama. Upozorenja se šalju ovom modulu, obogaćuju obavještajnim podacima i automatski prosljeđuju u akcije odgovora (blokiranje IP-a, onemogućavanje naloga, izolacija krajnjih tačaka). Analitičari mogu vizuelno dizajnirati radne tokove, dok programeri mogu proširiti mogućnosti sopstvenim skriptama.</p> <p>Glavne Funkcionalnosti</p> <ul style="list-style-type: none"> <li>- Automatizovani “Playbook”-i</li> <li>- Integracioni Hub</li> <li>- Vizuelni Dizajner Radnih Tokova</li> <li>- Predefinisana Pravila</li> <li>- Automatizovani Okidači</li> <li>- Upravljanje Slučajevima</li> <li>- Proširiva Tržnica Integracija</li> <li>- Višekorisničke Operacije</li> <li>- Hibrid No-Code/Pro-Code</li> <li>- Orkestracija Infrastrukture</li> </ul>	1,00 komad
---	---	---	------------

4	Modul 4: Platforma za Obavještajne Podatke o Prijetnjama	<p>Otvoreno-kodna platforma za obavještajne podatke koja transformiše sirove prijetnje u upotrebljive uvide centralizovanjem podataka iz više izvora. Mora koristiti STIX2 kompatibilan graf znanja za organizovanje i vizualizaciju složenih odnosa između aktera prijetnji, kampanja, indikatora kompromitacije, ranjivosti i žrtava. Platforma mora podržavati automatizovane radne tokove, omogućavajući dinamičku detekciju prijetnji, odgovor i lov na prijetnje. Takođe obrađene događaje šalje dalje u sistemu konkretno modulu 3 na dalju obradu</p> <p>Ovaj modul funkcioniše kao sloj za obavještajne podatke o prijetnjama. On prikuplja strukturisane i nestrukturisane izvore i kreira relacijski graf infrastrukture protivnika, tehnika i indikatora. Orkestracioni modul koristi ovaj sistem tokom izvršavanja "playbook"-a za obogaćivanje alarma kontekstom (npr. identifikacija da IP adresa pripada poznatom akteru). Novi nalazi se mogu vratiti u graf, obezbjeđujući povratnu spregu između detekcije i obavještajnih podataka.</p> <p>Glavne Funkcionalnosti</p> <ul style="list-style-type: none"> <li>- Centralizovano Upravljanje Podacima o Prijetnjama</li> <li>- STIX2 Graf Znanja</li> <li>- Automatizovana Detekcija i Upravljanje IOC-ima</li> <li>- Napredna Vizualizacija i Analitika</li> <li>- Upravljanje Slučajevima i Odgovor na Incidente</li> <li>- Real-Time Tokovi Podataka i Generisanje Feed-ova</li> <li>- Ekosistem Konektora</li> <li>- Skalabilnost i Visoka Dostupnost</li> </ul>	1,00 komad
---	--	---	------------

5	Integracija	<p>Svi gore navedeni moduli od 1 do 4 moraju raditi kao jedinstven SOAR sistem.</p> <ul style="list-style-type: none"><li>- Modul 1 obezbjeđuje vidljivost krajnjih tačaka i sistema.</li><li>- Modul 2 obezbjeđuje log detekciju.</li><li>- Modul 3 orkestrira automatizovane radne tokove koji povezuju Module 1, 2 i 4.</li><li>- Modul 4 obogaćuje sve alarme kontekstom i snabdijeva detekciju eksternim obavještajnim podacima.</li><li>- Implementacija modula 1 ne smije uticati na postojeće performanse endpoint uređaja</li><li>- Sva pravila i akcije u okviru SOAR sistema bice naknadno definisani u skladu sa trenutnim zahtjevima potrebama UIKS-a.</li></ul>	1,00 komad
---	-------------	---	------------