



Ur.br. 01-951-3-2026  
Zagreb, 08.05.2026.

**Predmet nabave: Pružanje usluge informacijske sigurnosti vezane uz ulogu sigurnosno operativnog centra (SOC) + SIEM**

**Ev.broj nabave: 18/2026 JN**

### **Opis usluge:**

1. **Neprekidni nadzor (24/7/365)** – SOC koristi aplikacije za kontinuirano prikupljanje i analizu sigurnosnih događaja u stvarnom vremenu. Usklađenost sa normom ISO 22301. Ovaj nadzor omogućuje brzo otkrivanje i reagiranje na sumnjive aktivnosti, smanjujući vrijeme potrebno za odgovor na prijetnjekontrolu, revidiranje i usklađivanje postojećih predložaka svih vrsta ugovora u graditeljstvu na hrvatskom i engleskom jeziku te razvoj pojedinih projekata ili transakcija vezanih uz poslovanje Naručitelja,
2. **Otkrivanje i analiza prijetnji** – koriste napredne algoritme i pravila korelacije kako bi prepoznao anomalije, maliciozne aktivnosti i potencijalne napade na infrastrukturu. SOC tim vrši detaljnu analizu svakog sumnjivog događaja kako bi odredio njegovu ozbiljnost i potreban odgovor,
3. **Odgovor na incidente** – SOC implementira automatizirane sigurnosne mehanizme koji, putem integracije sa SOAR rješenjima, mogu izolirati kompromitirane sustave, blokirati IP adrese i spriječiti širenje prijetnje,
4. **Generiranje sigurnosnih izvještaja i preporuka** – Redoviti sigurnosni izvještaji pružaju pregled ključnih incidenata, prepoznatih ranjivosti i preporučenih mjera za poboljšanje sigurnosti,
5. **Praćenje usklađenosti sa sigurnosnim standardima** – aplikacija omogućuje provjeru usklađenosti s normama kao što su ISO 27001, GDPR, NIST i CIS benchmarki, analizirajući konfiguraciju sustava i identificirajući odstupanja od preporučenih sigurnosnih postavki,

### **KOMPONENTE SOC-a**

SOC usluga temelji se na sljedećim komponentama:

- **Aplikacija** – Centralna platforma za prikupljanje, analizu i korelaciju sigurnosnih događaja. Omogućuje uvid u potencijalne prijetnje kroz napredne dashboarde i prilagođena pravila detekcije.
- **IDS/IPS sustavi** – Omogućuju detekciju i prevenciju mrežnih napada analizom mrežnog prometa u stvarnom vremenu. SOC koristi pravila prilagođena specifičnim potrebama klijenta.
- **EDR rješenja** – Endpoint Detection and Response rješenja pružaju detaljan uvid u aktivnosti na krajnjim točkama, uključujući otkrivanje malicioznog koda, neovlaštenih promjena u datotekama i sumnjivih korisničkih aktivnosti.



- **SOC Analitički Tim** – Tim stručnjaka koji neprekidno nadzire, analizira i reagira na sigurnosne incidente. Koristi alate za brzo donošenje odluka i smanjenje vremena detekcije prijetnji.
- **Incident Response Team** – Specijalizirani stručnjaci zaduženi za hitnu intervenciju i sanaciju posljedica kibernetičkih napada. Tim primjenjuje forenzičke metode kako bi identificirao izvor napada i spriječio slične incidente u budućnosti.

## OPSEG MONITORINGA

SOC s aAplikacijom će nadzirati sljedeće komponente:

- **Mrežnu infrastrukturu** – Firewalli, routere, VPN sustave i druge mrežne uređaje. Analiziraju se logovi prometa, pokušaji neovlaštenog pristupa i anomalije u mrežnom ponašanju.
- **Servere i aplikacije** – Kontinuirano praćenje Windows/Linux servera, baza podataka i poslovnih aplikacija kako bi se detektirale ranjivosti, neovlaštene promjene u konfiguraciji i potencijalne prijetnje.
- **Korisničke uređaje** – Radne stanice, mobilne uređaje i IoT uređaje. SOC analizira ponašanje uređaja, pristup osjetljivim podacima i moguće indikacije kompromitacije.
- **Logove i zapisnike aktivnosti** – Centralizirano prikupljanje i analiza logova sustava, aplikacija i mrežnih uređaja kako bi se identificirali sigurnosni incidenti.

## SIGURNOSNI ALATI I TEHNOLOGIJE

Za realizaciju SOC usluge koriste se aplikacije u kombinaciji s drugim alatima:

- **Ap1** – Prikupljanje, analiza i korelacija podataka iz različitih izvora.
- **Ap2** – IDS/IPS rješenja za mrežnu detekciju napada.
- **Ap3** – Pohrana i vizualizacija logova.
- **Ap4** – Host-based Intrusion Detection System.
- **Ap5** – Skener ranjivosti.

## PROCES ODGOVORA NA INCIDENTE

Proces odgovora na incidente temelji se na funkcionalnostima Ap1 i uključuje:

1. **Detekciju prijetnje** – Identifikacija sumnjivih aktivnosti analizom logova i anomalija u Ap1
2. **Analizu događaja** – Korelacija podataka iz više izvora kako bi se identificirale stvarne prijetnje.
3. **Klasifikaciju i procjenu rizika** – Procjena potencijalne štete i prioritizacija odgovora.
4. **Automatiziran odgovor** – Ap1 omogućuje automatsko blokiranje IP adresa, izolaciju zaraženih sustava i primjenu pravila za zaštitu podataka.
5. **Forenzičku istragu i izvještavanje** – Dubinska analiza incidenata i preporuke za poboljšanje sigurnosne strategije.
6. **Preventivne mjere** – Primjena sigurnosnih politika i kontinuirana edukacija zaposlenika kako bi se smanjio rizik ljudskih pogrešaka.