Zahtjev za ponudom

Upravljana usluga SOC sa integriranim SIEM-om za potrebe Poslovna grupa Auto Hrvatska

Verzija, 1.1

Zagreb, 15.05.2026.

1. Uvod

Poslovna grupa Auto Hrvatska (u daljnjem tekstu: **PGAH**) pokreće postupak odabira partnera za isporuku upravljane usluge Sigurnosnog operativnog centra (Security Operations Center – **SOC**) s integriranim Sustavom za upravljanje sigurnosnim informacijama i događajima (Security Information and Event Management – **SIEM**).

Poslovna grupa obuhvaća 12 trgovačkih društava te obavlja trgovačku i servisnu djelatnost u gospodarskom i osobnom programu za nova i rabljena vozila s pripadajućim dijelovima, gumama, servisnom opremom, alatima i servisnim uslugama, posluje na 33 lokacije u 4 države (Hrvatska, Slovenija, Bosna i Hercegovina, Sjeverna Makedonija) i zapošljava više od 800 djelatnika. IT okruženje obuhvaća oko 650 radnih stanica i 36 poslužitelja.

PGAH nije klasificiran kao subjekt od posebnog javnog interesa prema NIS2 direktivi, no strategijskim prioritetom smatra kontinuirano unaprjeđenje kibernetičke sigurnosti u skladu s rastućim rizicima u sektoru maloprodaje vozila.

---

2. Poslovna pozadina i kontekst

2.1 O poslovnoj grupi

PGAH obuhvaća maloprodaju novih i rabljenih vozila (osobnih automobila i kamiona), prodaju rezervnih dijelova, servisnu djelatnost i prodaju prateće opreme. Poslovanje je geografski distribuirano s centralnom informatičkom infrastrukturom i regionalnim lokacijama.

Ključni poslovni procesi koji zahtijevaju kontinuiranu zaštitu:

- Sustavi za upravljanje prodajom i servisom vozila (DMS – Dealer Management System)
- Financijsko-računovodstveni sustavi
- Active Directory i identiteti korisnika
- Microsoft 365 / Exchange Online (O365 Hybrid)
- Interna web infrastruktura i IIS poslužitelji

2.2 Trenutno stanje IT sigurnosti

Na temelju interne analize, PGAH trenutno raspolaže sljedećim sigurnosnim mehanizmima u operativnoj nadležnosti partnera. Kompletno serversko okruženje je outsourcano kod partnera kao i aktivna mrežna infrastruktura.

Kategorija	Rješenje / Status
Firewall / UTM / IPS	Fortigate (1 uređaj, centralni)

Endpoint zaštita (EDR/AV)	Bitdefender Endpoint Security
Autentifikacija	Active Directory (Kerberos on-prem) + O365 MFA
E-mail / SaaS zaštita	Microsoft 365 (O365 Hybrid Exchange)
Cloud	Microsoft Azure (1 hub)
Upravljanje uređajima	ManageEngine Endpoint Central SE (Software Distribution, Patch Mgmt, Inventory)
Helpdesk / ITSM	SysAid, Hesk
SIEM	Nije implementiran
NAC / DLP / WAF / CASB	Nisu implementirani
Vulnerability scanning	ManageEngine Endpoint Central Security Edition

3. Predmet zahtjeva za ponudom

3.1 Opseg tražene usluge

PGAH traži isporuku **upravljane SOC usluge kao managed service**, koja obuhvaća:

1. **Implementaciju i upravljanje SIEM platformom** – dobavljač implementira, konfigurira i operativno održava SIEM sustav. PGAH zahtijeva i vlastiti (self-service) pristup SIEM platformi u svrhu internog nadzora.
2. **Operativni nadzor 24/7/365** – preaktivan monitoring sigurnosnih događaja u realnom vremenu.
3. **Trijaža i analiza incidenata** – klasifikacija, prioritizacija i eskalacija sigurnosnih upozorenja.
4. **Odgovor na incidente (Incident Response)** – SOC reagira na detektirane prijetnje te dostavlja konkretne preporuke za sanaciju.
5. **Threat Intelligence** – kontinuirano praćenje aktualnih prijetnji i primjena relevantnih detekcijskih pravila (use cases).

3.2 Željene razine usluge (SOC Tier model)

Ponuda mora uključivati sljedeće razine usluge (SOC tier):

- **Tier 1** – Kontinuirani monitoring sigurnosnih događaja putem SIEM-a; klasifikacija i prioritizacija incidenata; odgovor na poznate, jednostavne napade prema predefiniranim procedurama.
- **Tier 2** – Dublja analiza kompleksnijih, ali poznatih vrsta napada; definiranje mjera za suzbijanje, eliminaciju i oporavak od sigurnosnih incidenata.

- **Tier 3** – Napredna analiza i digitalna forenzika za sofisticirane i nepoznate napade; analiza prethodnih incidenata radi prevencije i optimizacije procedura; praćenje threat intelligence izvora i ažuriranje detekcijskih pravila.

3.3 SIEM platforma – zahtjevi

- SIEM mora biti sposoban za ingestion logova iz svih izvora navedenih u sekciji 4
- PGAH zahtijeva vlastiti pristup SIEM platformi (portal/dashboard) za:
  - Pregled aktivnih upozorenja i incidenata
  - Pregled i pretraživanje logova (ad-hoc upiti)
  - Uvid u stanje monitoriranih entiteta
  - Izvještaje i dashboarde
- Ponuđač mora navesti koja SIEM platforma se koristi (vendor i licenčni model)
- Ponuđač mora jasno opisati model pohrane logova (on-premise, cloud, hybrid) i lokaciju pohrane podataka (bitno zbog GDPR-a – podaci moraju ostati u EU)
- Retencija logova: minimalno **3 mjeseci online** + mogućnost dugoročne arhive

3.4 Izvori logova – opseg monitoringa

Na temelju IT infrastrukture PGAH-a, sljedeći izvori logova ulaze u opseg SOC/SIEM monitoringa:

Izvor	Detalji	Količina
Firewall / IPS	Fortigate	1
Endpoint EDR	Bitdefender Endpoint Security	~650 endpointa
Windows radne stanice	Windows 11 (određeni eventi)	~650
Windows poslužitelji	Windows Server (general purpose)	35
Active Directory	On-premise AD	1
DNS	Microsoft DNS	1
DHCP	Microsoft DHCP	1
Microsoft 365 / Exchange	O365 Hybrid, Exchange Online	1 (O365 tenant)
Azure	Azure IaaS (procjena ukoliko je potrebno)	1 hub
IIS Web serveri	IIS 7	2
AV / Anti-malware	Bitdefender Endpoint Security	1 konzola

Projektirana veličina okruženja za 3 godine: ~700 radnih stanica, ~40 poslužitelja.

Ponuđač je dužan navesti kako tretira rast broja izvora i koristi li model temeljen na broju izvora (assets), EPS-u (events per second), volumenu (GB/dan) ili nekom drugom modelu licenciranja. Svakako očekujemo od ponuđača prijedloge best practice u okviru našeg okruženja a temeljem njihovih dosadašnjih iskustava.

---

4. Tehničke i operativne specifikacije

4.1 Implementacija i onboarding

- Ponuđač je odgovoran za cjelovitu implementaciju i konfiguraciju SIEM-a
- Onboarding svih navedenih izvora logova mora biti završen unutar **90 dana** od potpisa ugovora
- Ponuđač treba navesti potrebe za pristupom internoj mreži PGAH-a (agenti, konektori, VPN, API integracije) i pristupna prava potrebna za provedbu projekta
- Ponuđač treba opisati vlastiti onboarding proces i projektni plan

4.2 Upravljanje upozorenjima i incidentima

- Sva upozorenja moraju biti dokumentirana u sustavu za praćenje incidenata
- Definirati SLA za:
    - Vrijeme odgovora na kritične incidente (P1)
    - Vrijeme odgovora na visoke incidente (P2)
    - Eskalacijski postupak i kontaktni model
- SOC mora biti dostupan **24/7/365**

4.3 Detekcijska pravila (Use Cases)

- Ponuđač mora dostaviti popis inicijalnih detekcijskih pravila relevantnih za okruženje PGAH-a (Windows AD, Fortigate, Bitdefender, O365 po potrebi i Azure)
- Pravila trebaju biti usklađena s MITRE ATT&CK frameworkom
- Ponuđač mora opisati proces kontinuiranog razvoja i ažuriranja use caseova
- PGAH je zainteresiran za detekciju specifičnih scenarija: lateral movement, credential abuse, ransomware indicatori, phishing kampanje, anomalije u AD-u

4.4 Izvještavanje

- **Tjedni izvještaj**: pregled upozorenja i incidenata za protekli tjedan
- **Mjesečni izvještaj**: sažetak sigurnosnog stanja, trendovi, statistike, preporuke
- **Adhoc izvještaji** na zahtjev PGAH-a
- Izvještaji trebaju biti dostupni u SIEM portalu s mogućnošću preuzimanja u Excel ili PDF formatu.

4.5 GDPR i lokacija podataka

- Svi logovi i podaci moraju biti pohranjeni na infrastrukturi unutar **EU** (Europska unija)
- Ponuđač mora navesti točnu lokaciju podatkovnih centara i procesnih sustava
- Ponuđač mora opisati mjere zaštite podataka relevantne za GDPR

---

5. Zahtjevi prema ponuđaču

Ponuđač mora ispuniti sljedeće minimalne uvjete prihvatljivosti:

- Minimalno **3 godine iskustva** u isporuci upravljanih SOC/SIEM usluga
- Referentne instalacije u okruženjima s distribuiranim lokacijama
- ISO 27001 certifikacija ili ekvivalentni standard za vlastite operacije
- SOC analitičari s relevantnim certifikatima (GIAC, CISSP, CEH, CompTIA Security+, ili ekvivalentni) – uključiti životopise ključnih ljudi
- Sposobnost komunikacije i dokumentacije na **hrvatskom jeziku** (ili engleskom, uz prijevod ključnih dokumenata)
- Lokalni ili regionalni tim za podršku (PGAH preferira dobavljača s prisutnošću u RH ili regiji)

6. Komercijalni uvjeti i model usluge

Ponuđač treba jasno strukturirati ponudu po sljedećim elementima:

6.1 Jednokratni troškovi (CAPEX / Setup)

- Implementacija i konfiguracija SIEM-a
- Onboarding izvora logova
- Inicijalna konfiguracija detekcijskih pravila
- Edukacija PGAH-ovog ICT tima za rad u SIEM portalu
- Sve druge jednokratne stavke nužne za stavljanje rješenja u funkciju

6.2 Redovni godišnji troškovi (OPEX / Subscription)

- Licenca/pretplata za SIEM platformu
- SOC upravljana usluga (Tier 1 + Tier 2 + Tier 3)
- Infrastruktura za potrebe on-prem servera
- Infrastruktura za potrebe pohrane logova (navesti kapacitet)
- Threat Intelligence pretplata (ako se naplaćuje zasebno)

- Sve druge višekratne stavke nužne za stavljanje rješenja u funkciju i redovno funkcioniranje

6.3 Varijabilni troškovi

- Troškovi vezani uz rast okruženja (novi endpointi, novi log izvori)
- Troškovi dodatnih ad-hoc aktivnosti (forenzike, posebne analize)

6.4 Opcije i dodaci

- Vulnerability Assessment / Scanning usluga
- Penetration testing
- Phishing simulacije
- PGAH SIEM licenca za samostalni rad (ako se licencira zasebno od SOC usluge)

8. Detalji podnošenja ponude

- **Datum objave RFP-a:** 18.05.2026.
- **Krajnji rok za dostavu ponuda:** 03.06.2026.
- **Planirani datum donošenja odluke:** 17.06.2026.
- **Planirani početak usluge:** Q3 2026.

Ponuda se dostavlja **isključivo putem portala** za koji ćete primiti link u emailu poziva. Tekstualni dio ponude u **PDF formatu**. Komercijalni dio ponude u **priloženom Excel TCO obrascu**.

Sva pitanja i komunikacija vezana uz ovaj RFP moraju biti upućena isključivo niže navedenim RFP kontaktima. PGAH zadržava pravo odbiti svaku ponudu ili ne odabrati niti jednog ponuđača bez obrazloženja.

- **Hrvoje Vid** – hrvoje.vid@autohrvatska.hr
- **Tomislav Marenić** – tomislav.marenic@autohrvatska.hr

---

9. Obvezni sadržaj ponude

Svaka ponuda mora sadržavati sljedeće elemente:

1. **Opis ponuđene usluge** – detaljan opis SOC i SIEM usluge, SOC tier modela, dostupnosti, procesa eskalacije
2. **Opis SIEM platforme** – vendor, verzija, arhitektura (cloud/on-prem/hybrid), licencni model, pristupne mogućnosti za korisnika
3. **Onboarding plan** – projektni plan s vremenskim okvirom i ključnim obvezama

4. **Use case katalog** – popis inicijalnih detekcijskih pravila (minimalno 20 use caseova relevantnih za PGAH okruženje)
5. **SLA pravila** – definicije razina prioriteta, vremena odgovora i eskalacijskih procedura
6. **Sigurnosna i GDPR dokumentacija** – lokacija podataka, ISO 27001 ili ekvivalent, DPA (Data Processing Agreement) nacrt
7. **Reference** – minimalno 2 referentne implementacije sličnog ili većeg opsega
8. **Komercijalna ponuda** – popunjen Excel TCO obrazac s jasnom razradom svih troškova
9. **Kvalifikacije tima** – životopisi, opisi uloga i relevantnih certifikata SOC analitičara

---

Auto Hrvatska d.d. zadržava pravo prihvatiti samo određene elemente ponude ili zatražiti dodatne informacije od pojedinog ponuđača.