www.gen-energija.si

Najem s podporo programske opreme SIEM - SPLUNK

TEHNIČNE SPECIFIKACIJE

Oznaka: SP-2025-029
Revizija: 0

Pripravil: Mitja Ribič

Podpisnik: Mitja Ribič
Specialist za kibernetsko varnost
Izdajatelj: SIGEN-CA G2
Številka certifikata: 09BC3FB200000000572D1FE5
Potek veljavnosti: 18. 07. 2030
Čas podpisa: 21. 10. 2025 12:58

Pregledal: Janez Kovačec

Podpisnik: Janez Kovačec
Specialist za kibernetsko varnost
Izdajatelj: GEN-E Enterprise CA01
Številka certifikata: 7100001F3FC12AD977839DC4DF000100001F3F
Potek veljavnosti: 22. 07. 2026
Čas podpisa: 21. 10. 2025 13:00

Odobril: dr. Bruno Glaser

Podpisnik: BRUNO GLASER
Poslovni direktor
Izdajatelj: SIGEN-CA G2
Številka certifikata: 00EAC8BC100000000057257600
Potek veljavnosti: 10. 12. 2025
Čas podpisa: 21. 10. 2025 13:05

Kazalo vsebine

1 UVOD 3
2 NAMEN 3
3 OKRAJŠAVE IN DEFINICIJE 3
3.1 OKRAJŠAVE 3
4 Funkcionalnosti orodja Splunk 4
5 Predmet naročila 5
6 VHODNI PODATKI PREDPOSTAVKE 6
7 UPORABA STANDARDOV IN PREDPISOV 6
8 ZAGOTOVITEV KVALITETE IN STROKOVNOSTI 6
9 PREGLED IN KONTROLA DELA 6
10 AKTIVNOSTI in ČASOVNI PLAN IZVEDBE 6
11 POROČANJE O NAPREDKU NALOGE IN ZAPISI 6
12 SPREMEMBE OBSEGA DELA 7
13 PREDAJA DOKUMENTACIJE IN NJENA OBLIKA 7
14 ORGANIZACIJSKI KONTAKT 7
15 DOSTOP DO INFORMACIJ 8
16 POGODBENO DELO 8
17 POSLOVNA SKRIVNOST 8

1 UVOD

V poslovnem informacijskem sistemu družbe GEN energija d.o.o. je vpeljano orodje Splunk za zajem, obdelavo in upravljanje varnostnih informacijskih dogodkov (SIEM – Security Information and Event Management). Orodje predstavlja ključen del sistema za zagotavljanje kibernetske varnosti, saj omogoča centralizirano zbiranje, analizo in obvladovanje varnostnih dogodkov.

2 NAMEN

Namen podaljšanja najema orodja Splunk je:

- zagotavljanje kontinuiranega delovanja obstoječe platforme za obdelavo varnostnih dogodkov,
- krepitev kibernetske varnosti in pravočasno odkrivanje potencialnih groženj,
- ohranitev skladnosti z zakonodajo in regulatornimi zahtevami (ZinfV-1),
- omogočanje centraliziranega nadzora in enotnega poročanja o varnostnih dogodkih,
- podpora notranjim in zunanjim revizijam ter forenzičnim preiskavam.

Z neprekinjeno uporabo orodja Splunk se GEN energiji omogoča učinkovito upravljanje varnostnih tveganj, zmanjševanje posledic incidentov in ohranjanje visoke stopnje zaupanja v stabilnost informacijskega sistema.

Obstoječa pogodba za najem programske opreme Splunk se izteče konec januarja 2026, zato je potrebno pravočasno zagotoviti podaljšanje, da ne pride do prekinitve delovanja sistema.

3 OKRAJŠAVE IN DEFINICIJE

3.1 OKRAJŠAVE

SIEM	Security Information and Event Management - upravljanje varnostnih informacij in dogodkov
SPLUNK	Platforma za zbiranje in analizo varnostnih podatkov, ki omogoča hitro odkrivanje, preiskovanje in odzivanje na kibernetske grožnje.

4 Funkcionalnosti orodja Splunk

Orodje Splunk v informacijske okolju GEN energije d.o.o. zagotavlja naslednje ključne funkcionalnosti, ki pokrivajo celoten krog obvladovanja varnostnih dogodkov:

Zajem in konsolidacija podatkov:

- centraliziran zajem dogodkov iz vseh informacijskih sistemov družbe (strežniški sistemi, omrežna infrastruktura, aplikacije),
- integracija z oblačnimi storitvami (npr. Microsoft 365, Azure AD),
- standardizacija in normalizacija podatkov za nadaljnjo obdelavo.

Analiza in detekcija

- analiza dogodkov v realnem času za pravočasno zaznavanje nepravilnosti,
- korelacijska pravila in iskanja, ki povezujejo dogodke v kompleksne varnostne scenarije,
- uporaba strojnega učenja za zmanjšanje količine nerelevantnih dogodkov in izboljšanje natančnosti zaznavanja,
- odkrivanje napadov, notranjih zlorab in drugih varnostnih groženj.

Vizualizacija in nadzor

- oblikovanje nadzornih plošč (dashboards) za operativne in vodstvene potrebe,
- pregled ključnih varnostnih kazalnikov (KPI) in trendov skozi čas,
- grafični prikaz incidentov za hitro prepoznavanje anomalij.

Upravljanje incidentov in odziv

- registracija in upravljanje incidentov (dodeljevanje, spremljanje, zaključevanje),
- podpora pri forenzični preiskavi dogodkov,
- možnost uporabe avtomatiziranih odzivov (SOAR) na podlagi vnaprej definiranih pravil in playbookov.

Poročanje in skladnost

- generiranje samodejnih poročil za notranje in zunanje deležnike,
- revizijske sledi za dokazovanje skladnosti,
- podpora pri izpolnjevanju zahtev regulatorjev in zakonodaje (ZinfV-1).

5 Predmet naročila

Za potrebe zagotavljanja zanesljivega, neprekinjenega in skladnega delovanja sistema za upravljanje varnostnih dogodkov je potrebno podaljšati najem programske opreme Splunk z vključenimi licencami, podporo in spremljevalnimi storitvami, in sicer za obdobje treh (3) let od sklenitve pogodbe.

Obseg uporabe: **zajem do 20 GB podatkov na dan.**

Predmet naročila vključuje:

- **Podaljšanje osnovne licence Splunk Enterprise**
  - Programska oprema: Splunk Enterprise – Term License with Standard Success Plan
  - Obseg: do 20 GB/dan
  - Trajanje: 3 leta

- **Podaljšanje licence Splunk Enterprise Security (dodatek)**
  - Izdelek: Splunk Enterprise Security – Term License with Standard Success Plan
  - Obseg: do 20 GB/dan
  - Trajanje: 3 leta

- **Storitve strokovne podpore**
  - mesečno vključuje 6 ur strokovnih storitev, ki se obračunavajo po dejansko opravljenih urah,
  - storitve vključujejo svetovanje, konfiguracijo, nadgradnje, odpravo napak in podporo pri uporabi sistema Splunk,
  - zagotovljena je pripravljenost z odzivnim časom do 4 ur v primeru kritičnih incidentov.

6 VHODNI PODATKI PREDPOSTAVKE

Naročnik se zavezuje, da bo po potrebi za posamezne dele naloge izvajalcu zagotovil vse razpoložljive vhodne podatke, ki jih ima na razpolago in so potrebni za nemoteno opravljanje analiz oz. drugih aktivnosti povezanih z nalogo.

7 UPORABA STANDARDOV IN PREDPISOV

Pri vzpostavitvi in delovanju VOC je potrebno upoštevati zakonodajo, mednarodne standarde in dobre prakse, ki zagotavljajo celovit, usklajen in preverljiv pristop k obvladovanju kibernetske in informacijske varnosti. VOC mora slediti naslednjim standardom in priporočilom:

- **ZinfV-1** – Zakon o informacijski varnosti.
- **ISO/IEC 27001** – Sistemi upravljanja informacijske varnosti.

8 ZAGOTOVITEV KVALITETE IN STROKOVNOSTI

Vse storitve se bodo izvajale v skladu z določili programa zagotavljanja kakovosti izvajalca. Zaželeno je, da je le ta usklajen z določili EN ISO 9001.

9 PREGLED IN KONTROLA DELA

Izvajalec mora, v skladu s planom zagotavljanja kakovosti izvajati kontrolo produktov in nadzor del. Dodaten pregled rezultatov naloge lahko izvaja GEN ali njegov pogodbeni partner v skladu z dogovorjenim časovnim načrtom. Izvajalec je dolžan zagotoviti naročniku vse predpostavke, vhodne podatke, literaturo in druge reference, ki so bili uporabljeni pri izdelavi naloge.

10 AKTIVNOSTI in ČASOVNI PLAN IZVEDBE

	Aktivnost	**Trajanje aktivnosti [teden]**	**Zaključek aktivnosti po podpisu pogodbe [teden]**
1	Podpis pogodbe	0	T_0
2	Namestitev novih licenc in posodobitev na zadnjo verzijo	1	$T_0 + 1$

11 POROČANJE O NAPREDKU NALOGE IN ZAPISI

Izvajalec je dolžan nemudoma obvestiti naročnika v primeru nejasnosti ali drugih odprtih vprašanj, ki bi zahtevali naročnikove vhodne podatke ali navodila za uspešen zaključek in samo vsebino naloge.

Izvajalec je dolžan pripraviti in posredovati zapisnik vsakega sestanka najkasneje v 2 delovnih dneh po sestanku.

Izvajalec je dolžan pripravljati in posredovati mesečno poročilo o izvajanju aktivnosti odgovornemu vodji projekta.

12 SPREMEMBE OBSEGA DELA

Spremembe obsega dela so možne na osnovi pisnega aneksa k osnovni pogodbi, s katerim se morata strinjati obe pogodbeni stranki.

13 PREDAJA DOKUMENTACIJE IN NJENA OBLIKA

Izvajalec bo predal dokumentacijo na osnovi obsega dela določenega v poglavju 3. Tekstualni del mora biti v MS Word formatu in Acrobat Reader formatu. Tabele, grafi in sheme morajo biti v izvorni obliki (ne kot slika). Skenirana besedila, slike in tabele referenčne dokumentacije so lahko v MS Office formatu ali drugem formatu, ki je splošno znan in razpoložljiv ter ne popači podatkov. Izvajalec bo vso elektronsko dokumentacijo predal preko FTP strežnika ali podobnega strežnika, na USB mediju ali preko e-pošte.

Projektna naloga je lahko shranjena v ločenih datotekah, po glavnih poglavjih projektne naloge. Ne glede na to pa mora izvajalec celotno projektno nalogo shraniti tudi v enotno datoteko.

Predani dokumenti	**Vrsta**	**Kopije**
Vmesno poročila/dokumenti/predstavitve	elektronsko	.pdf, .docx, .dwg, .jpg, .ppt
Končno poročilo/dokumenti/predstavitve	elektronsko	.pdf, .docx, .dwg, .jpg, .ppt

Poročila morajo biti predana (napisana) v urejevalniku v okviru naslednjih kriterijev:

Urejevalnik: Microsoft Word, MS Excel, MS Office PowerPoint

Velikost papirja: A4

Jezik: Slovenščina

14 ORGANIZACIJSKI KONTAKT

Izvajalec koordinira nalogo z odgovornim vodjem projekta.

Odgovorni vodja projekta	**Janez Kovačec**
	Specialist za kibernetsko varnost
	janez.kovacec@gen-energija.si
	040616590
Namestnik vodja projekta	Mitja Ribič
	Specialist za kibernetsko varnost
	mitja.ribic@gen-energija.si
	031414495

15 DOSTOP DO INFORMACIJ

Izvajalec mora zagotoviti neomejen dostop do informacij, ki jih bo le-ta uporabil pri izdelavi naloge. Naročniku mora zagotoviti vpogled in kontrolo nad vsemi referencami in merodajnimi informacijami.

16 POGODBENO DELO

Izvajalec sme izvajati dela po pogodbah s svojimi pod-pogodbenimi partnerji, vendar le s tistimi, ki jih navede v ponudbi. Za vse pod-pogodbene izvajalce se zahteva enaka usposobljenost kot za pogodbenega izvajalca na specifičnem področju za katerega je pogodba določena.

17 POSLOVNA SKRIVNOST

Za poslovno skrivnost naročnika štejejo vsi podatki, ki jih bo naročnik dostavil izvajalcu (vhodni podatki) oz. podatki, do katerih bo izvajalec prišel v zvezi z izvajanjem del. Naročnik in izvajalec se zavežeta, da bosta vse podatke, označene kot poslovna skrivnost, hranila na način, ki bo določen s pogodbo.