TEHNIČKI PREDLOG

COTEE – Crnogorski operator tržišta električne energije

Predlog br. 2408-1/2026

Ponuda usluga SOC-a (Security Operations Center)



***Klijent*:**
Cotee
Podgorica

Datum: 24.08.2026

Cotee
81000 Podgorica, Crna gora

Poštovani,

U ime kompanije Čikom d.o.o., zadovoljstvo mi je da vam dostavim, ponudu za pružanje usluga Čikomovog SOC.

U skladu s našom posvećenošću pružanju vrhunskih sigurnosnih rješenja, obraćamo Vam se s ciljem da Vam predstavimo našu ponudu usluga Security Operations Center (SOC). Naša kompanija nudi sveobuhvatnu podršku u zaštiti informacionih sistema kroz kontinuirani nadzor, detekciju prijetnji i pravovremeno reagovanje na bezbjednosne incidente, u skladu s najvišim industrijskim standardima i regulatornim zahtjevima.

SOC usluga je posebno dizajnirana za organizacije koje zahtijevaju napredan nivo zaštite, uključujući sektore sa povećanim sigurnosnim rizicima i obavezama usklađenosti. Naš tim čine visoko kvalifikovani stručnjaci sa međunarodno priznatim sertifikatima kao što su CISSP, CISM, CEH, CompTIA Security+ i ISO/IEC 27001, NIS2 Lead implementator čime garantujemo stručnost, pouzdanost i profesionalan pristup u svakom segmentu pružanja usluge.

Bilo bi nam zadovoljstvo da u nastavku razgovaramo o Vašim specifičnim potrebama i mogućnostima saradnje.

Srdačno,

Ivan Stanković

Sales Manager – Cyber Security services and equipment

Čikom

Ivan.stankovic@cikom.com
+38267610110

Podgorica, 24.08.2026

Sadržaj

1. TAČAN NAZIV I ADRESA PONUĐAČA, PORESKI IDENTIFIKACIONI BROJ I KONTAKTI 4

2. PROFIL KOMPANIJE 5

3. GLAVNE REFERENCE 8

4. REFERENCE ZA MREŽNU I BEZBJEDNOSNU OPREMU 9

5. REFERENCE KLJUČNIH ČLANOVA PROJEKTNOG TIMA 10

6. ČIKOM SOC 14

6.1. Ključne funkcije SOC-a: 14

6.2. Komponente SOC: 15

6.3. Čikom SOC Tim – Struktura i Uloge 15

6.4. Onboarding process 16

6.5. Operativni SOC model – Operating Model 17

7. TEHNIČKA SPECIFIKACIJA 19

7.1. Cyber Security Platform 19

7.2. Qualys Vulnerability Management, Detection and Response 20

7.3. Privileged Access Management (PAM) 21

8. SERVICE LEVEL AGREEMENTS (SLA) 21

9. REPORTING, KPI, GOVERNANCE I PRAĆENJE KVALITETA USLUGE 21

9.1. Ključni KPI pokazatelji 22

9.2. Izvještavanje i transparentnost 22

9.3. Governance i upravljanje uslugom 22

9.4. Kontinuirano unapređenje 22

10. OBAVEZE I RESURSI KLIJENTA (CUSTOMER RESPONSIBILITIES) 22

10.1. Tehnički resursi klijenta 22

10.2. Organizacijski i kadrovski resursi 23

10.3. Operativna saradnja 23

10.4. RACI matrica i plan implementacije 23

11. FINANSIJSKA SPECIFIKACIJA 24

1. *Tačan naziv i adresa ponuđača, poreski identifikacioni broj i kontakti*

- ČIKOM d.o.o.
- Kontakt osoba za ovaj tender:
  - Nenad Vraneš, direktor prodaje
  - Adresa: Dalmatinska 78, 81000 Podgorica
- Tel/faks: 020-218181, 020-218182
- Broj telefona: 067-211-200
- E-mail: nenad@cikom.com
- WWW. cikom.com
- PIB : 02177579
- PDV: 30/31-00403-8
- 540-5089-10 (ERSTE)

2. *Profil kompanije*

O KOMPANIJI

Preduzeće za informatičko inženjerstvo i konsalting Čikom iz Podgorice osnovano je 1993. godine. Danas je Čikom vodeća kompanija na IT tržištu Crne Gore, razvijena od jednostavnog dobavljača računarske opreme u integratora i implementatora najsloženijih informatičkih rješenja, sposobna da svojim korisnicima pruži najširi spektar proizvoda i usluga u oblasti informatike, informacione bezbjednosti i komunikacionih tehnologija.

Najvažniji resurs ove kompanije su 80 kvalifikovanih zaposlenih i deset spoljnih saradnika, koji čine osnovu stabilnosti i pouzdanosti poslovnog sistema Čikoma – nesumnjivo najvećeg od svih informatičkih preduzeća Crne Gore.

MISIJA KOMPANIJE

Misija kompanije Čikom nije samo da prati informatičke inovacije na ovim prostorima, već da postane njen značajan kreator i moderator. Različiti informatički profili, naučni pristup, akumulirano znanje i iskustvo, prateći svetske standarde i veoma bliska saradnja sa korisnicima garancija su uspeha naše poslovne filozofije – INFORMATIKA SA LJUDSKIM PROFILOM. Čikom ne prodaje samo opremu i usluge; Činimo ih da služe vašim potrebama, kreativnosti i profesionalnoj afirmaciji. Sa našim velikodušnim prenosom znanja na korisnike, postižemo optimum upotrebljivosti i eksploatacije tehnologije koju primenjujemo.

VAŠ POUZDAN PARTNER

Ono što drugi smatraju veoma komplikovanim, shvatamo da je vrlo jednostavno i lako. Bavimo se konsaltingom, projektnim menadžmentom, razvojem različitih softverskih rešenja i implementacijom i integracijom svega toga u jedinstveni IT sistem. Konstantno povećanje kvaliteta ostvarujemo ulaganjem u obuke naših zaposlenih, čime dobijamo sva potrebna znanja iz oblasti komunikacionog inženjeringa i analize operativnih sistema.

Čikom svojim korisnicima obezbeđuje vrhunsku tehnologiju u hardverskim sistemima vodećih svetskih informatičkih kompanija, i stvara jedinstvene sisteme ovih jedinica, čineći ih efikasnijim za specifičnu softversku implementaciju. Nudimo 24x7 sistem održavanja, i uvek smo spremni da intervenišemo u slučaju kvarova.

KORISNICI

Naša ponuda ispunjava zahtjeve korisnika u mnogim granama:

- Industrija
- Bankarstvo
- Telekomunikacija
- Vlada i institucije
- Biznis i turizam
- Obrazovanje

NUDIMO DODATNI KVALITET

Zato što smo:

- Cognyte
- Symantec Secure One Gold Partner

- Cynet Partner
- Stellar Cyber partner
- Splunk
- GOLD Microsoft sertifikovani partner, sa nadležnostima za:
    - Gold Datacenter
    - Silver Collaboration and Content
    - Silver Data Analytics
    - Silver Messaging
    - Silver Project and Portfolio Management
    - Silver Small and Midmarket Cloud Solutions
- HPE Platinum Partner Ready Solution Provider, Services Delivery partner,
- Software Defined Infrastructure - VMware & Hyper-V Virtualization Business
- Aruba Network Solution Provider and Silver Partner
- Dell-EMC Gold Solution Provider
- F5 Networks UNITY Authorized partner
- Cisco Premier Partner & Integrator
- CommScope Ruckus Networking CERTIFIED SOLUTION PROVIDER
- Check Point 3-Star Partner
- ASI - Accredited Systems Integrator of Allied Telesis and Gold Solution Partner
- ASP - Accredited Service Partner of Allied Telesis
- Avigilon Certified Solution Provider
- Rittal IT Channel Partner
- Reichle & De-Massari Authorized QPP-Partner
- VMware Partner Conect Advanced
- Veeam Silver Partner
- Menage Engine reseller
- Lexmark Accredited Service Partner

PONOSNI SMO NA PROJEKTE

U poslednjih nekoliko godina Cikom je završio najveće IT projekte u Crnoj Gori, pa ih ističemo:

- Usluge SOC – CGES
- Usluge SOC – Luka Bar
- Usluge SOC - Opstina Budva
- Usluge SOC - Monstat
- Usluge SOC - ZUNS
- e-DMS (Elektronski sistem za upravljanje dokumentima) za Vladu Crne Gore.
- eDMS sistem zasnovan na EMC Documentum platformi.
- On-line sastanci Vlade Crne Gore (elektronski sastanci).
- E-Gov. Rešenje za mrežnu bezbjednost, servere i skladišnu infrastrukturu za opštine u Crnoj Gori Podgorici, Baru, Pljevljima, Herceg Novom, Kotoru, Budvi...
- Infrastrukturne usluge Vlade Crne Gore zasnovane na Microsoft tehnologijama.
- Poreska uprava isporuka i instalacija HA Data centar, mrežna bezbednost, serveri i infrastruktura za skladištenje.
- Centralna banka Crne Gore - Serveri, skladišta i mrežna infrastruktura u primarnim i DR centrima podataka.
- Hipotekarna banka Crna Gora - Serveri, skladišta i mrežna infrastruktura u primarnim i DR centrima podataka.

- Ziraat Bank Montenegro - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u primarnim i DR centrima podataka.
- Iberostar Bellevue Montenegro - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u primarnom centru podataka.
- Elektroenergetski prenosni sistem Crne Gore - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u Primarnom datacentru.
- Agencija civilnog vazduhoplovstva Crne Gore - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u Primarnom datacentru.
- Glavni grad Podgorica - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u primarnom datacentru.
- Montenegro Telecom AD - Usluge podrške serverima, skladištima i infrastrukturnim uslugama.
- Sava Montenegro Assurance Company AD - City - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u primarnom datacentru.
- Hladni rudnik a.d. Pljevlja - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u primarnim i DR podatkovnim centrima.
- Opština Budva, Bar, Pljevlja - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u Primarnom datacentru.
- Luka Adria AD Bar - Serveri, skladišta, infrastrukturne usluge i mrežna infrastruktura u primarnim i DR podatkovnim centrima. Infrastruktura i oprema podatkovnog centra. MAN optička infrastruktura. Sistem video nadzora na otvorenom prostoru. Preduzeće Vi-Fi infrastruktura na otvorenom prostoru.
- Crnogorski elektrodistributivni sistem d.o., Primarna lokacija serverska soba sa isporukom i ugradnjom skladišne i serverske opreme i uslugama isporuke.
- Nacionalna javna služba - Radio i televizija Crne Gore, isporuka jednosmerne opreme i usluga u procesu modernizacije tehnoloških kapaciteta RTCG.
- One & Only Porto Novi resort – Kumbor Herceg Novi, isporuka i montaža HPE servera i skladišne opreme, Aruba mrežne opreme, Ruckus Wi-Fi opreme i usluga.
- Ministarstvo unutrašnjih poslova Crne Gore - Projekat Bezbedan grad - Video nadzor gradova Podgorica, Bar, Budva.
- Crnogorska agencija za nacionalnu bezbjednost - Isporuka i montaža opreme za mrežnu bezbednost, servere i skladišnu infrastrukturu, video nadzor, kontrolu pristupa, alarm, požar i monitoring.

Imamo sve potrebne sertifikate, znanje i iskustvo kako bismo zadovoljili nacionalne i međunarodne standarde. Članovi našeg tima imaju sertifikat ITIL v3 koji predstavlja skup praksi za upravljanje IT uslugama.

Takođe smo nosilac sertifikata:

- **Sistem menadžmenta kvalitetom ISO 9001:2015**
- **Sistem upravljanja bezbednošću informacija ISO/IEC 27001:2022**
- **Sistem za upravljanje informacijama o privatnosti ISO/IEC 27701:2019**
- **Sistem upravljanja uslugama ISO/IEC 20000-1:2018**

Kompanija Čikom d.o.o. ima:

- **Rešenje i dozvola za pristup tajnim podacima klasifikovanosti SECRET (broj 010) izdalo Direkcije za zaštitu tajnih podataka Crne Gore.**
- **Odluka i dozvola za pet (5) zaposlenih koji imaju dozvolu za pristup tajnim podacima klasifikovanosti SECRET**

3. *Glavne reference*

	Kupca	Kontakt osoba	Period realizacije projekta	Rešenje isporučeno	Opis projektne aktivnosti
1.	Luka Bar	Hasan Ćuturić hasan.cuturic@lukabar.me	2025-	SOC operativni centar - Cynet, Stellar Cyber i Perception Point	Implementacija Cynet, Stellar Cyber i Perception Point sa uključenom podrškom i održavanjem i pružanjem usluge upravljanja i detekcije odgovora (MDR)
2.	Opstina Budva	Željko Racanović zeljko.racanovic@budva.me	2025-	SOC operativni centar - Stellar Cyber	Implementacija Stellar Cyber sa uključenom podrškom i održavanjem i pružanjem usluge upravljanja i detekcije odgovora (MDR)
3.	ZUNS	Lazo Leković lazo.lekovic@zuns.me	2025-	SOC Operations Center - Symantec Endpoint Security Complete, SMG, Stellar Cyber	Implementacija Symantec Endpoint Security Complete, SMG, Stellar Cyber sa uključenom podrškom, održavanjem i pružanjem usluge upravljanja i detekcije odgovora (MDR)
4.	Monstat	Boro Durković Boro.Durkovic@monstat.org	2025-	Symantec Endpoint Security Complete	Instalacija i implementacija Symantec endpoint zaštite, Symantec Messaging gatevay i Symantec Mail Security for Exchange, godišnja podrška
	Crnogorski Elektropreno sni sistem AD	Ivan Asanović Ivan.asanovic@cges.me	2025-	SOC operativni centar - Stellar Cyber	Implementacija Stellar Cyber sa uključenom podrškom i održavanjem i pružanjem usluge upravljanja i detekcije odgovora (MDR)
5.	Crnogorski Elektropreno sni sistem AD	Ivan Asanović Ivan.asanovic@cges.me	2009-2025	Symantec Endpoint Security Complete, Splunk Enterprise	Impplementacija I konfiguracija Splunk Enterprise, Nadogradnja Symantec endpoint zaštite, Symantec Messaging gatevay i Symantec Mail Securiti for Exchange, godišnja podrška
6.	Centralna banka Crne Gore	Igor Ivanović Igor.ivanovic@cbcg.me	2022-2025	Splunk Enterprise	Implementacija i konfiguracija Splunk Enterprise
7.	Uprava prihoda i carina	Veselin Jovićević veselin.jovicevic@tax.gov.me	2006-2025	Symantec Endpoint Security Complete	Nadogradnja Symantec Endpoint zaštite licenci i godišnja podrška
8.	Ziraat banka	Dževad Djecević dzevad.djecevic@ziraatbank.me	2017-2025	Symantec Endpoint Security Complete	Nadogradnja Symantec Endpoint zaštite licenci i godišnja podrška

9.	Prva banka	Bojan Šljivić Bojbojan.sljivic@pravabankacg.com	2016-2025	Symantec Endpoint Security Complete I Splunk Enterprise	Nadogradnja Symantec Endpoint zaštite licenci i godišnja podrška Implementacija i konfiguracija Splunk Enterprise
10.	Opstina Budva	Željko Račanović zeljko.racanovic@budva.me	2009-2025	Symantec Endpoint Security Complete	Nadogradnja Symantec Endpoint zaštite licenci i godišnja podrška
11.	Opstina Pljevlja	Jasmin Kulugija Jasmin.kulugija@pljevlja.co.me	2008-2025	Symantec Endpoint Security Complete	Nadogradnja Symantec Endpoint zaštite licenci i godišnja podrška
12.	Ministarstvo Odbrane	Luka Simonović luka.simonovic@mod.gov.me	2007-2025	Symantec Endpoint Security Complete	Nadogradnja Symantec Endpoint zaštite licenci i godišnja podrška

4. Reference za mrežnu i bezbjednosnu opremu

Vrsta mrežne opreme	Proizvođača	Lista projekata u kojima je isporuka i montaža mrežne i bezbjednosne opreme
LB i WAF	F5	- Crnogorski Telekom - Lovćen banka
DAM	Imperva	- Prva Banka
PAM	Wallix	- Skupština - Hipotekarna Banka - CGES
Mrežna oprema L2 i L3 prekidači	Arubu	- Porto Novi Novi-Vinodolski - Ministarstvo prosvete - AZMONT (Jedan i jedini Porto Novi) - SAVSKI VENAC
	Cisco	- Porto Novi (OSCAD) - NSA - Pivara Trebjesa Nikšić - Prva banka Crne Gore - Lovćen banka - Ziraat banka
	Allied Telesis	- Opština Herceg Novi - Crnogorski elektroprenosni sistem - Privredna komora Crne Gore - NSA - Klinički centar Crne Gore - Studentski dom
	Check Point	- Crnogorski elektroprenosni sistem - Ministarstvo spoljnih poslova

Oprema za bezbjednosnu mrežu		- Ministarstvo odbrane Crne Gore - Prva banka Crne Gore - Elektroprivreda Crne Gore - Crnogorski elektrodistributivni sistem - Rudnik uglja Pljevlja - Glavni grad Podgorica
	Palo Alto	- Porto Novi Novi-Vinodolski - d.o.o. - Opština Pljevlja
	Sophos	- Luka Bar - Agencija za civilno vazduhoplovstvo - Finansije Plus - Državna revizorska institucija - Opština Herceg Novi - Glavni grad Podgorica - Uprava za ugljovodonike - Centralno klirinško depozitno društvo AD - Opština Budva - Opština Herceg Novi

5. *Reference ključnih članova projektnog tima*

	Ime i koliko dugo radi za kompaniju	Polje rada	Referentni sertifikati	Nota
1.	Dragoslav Kenjić 20 godina	Projektovanje informacionih sistema	Ekspert Core Infrastructure	Dugogodišnje iskustvo u projektovanju, implementaciji hardverskih i softverskih rješenja za data centre, opremu i rješenja za informacionu bezbjednost
2.	Almir Karastanović 16 godina	Implementacija bezbednosti	Ekspert Symantec Endpoint Securiti rešenje Symantec sertifikovani specijalista Microsoft sertifikovani specijalista	Dugogodišnje iskustvo u projektovanju, implementaciji Microsoft i Symantec Endpoint Security rješenja
3.	Mladen Bukilić 16 godina	Implementacija bezbednosno-informacionih usluga	CISO NIS2 lead implementer CompTIA Cysa+ CompTIA Security Analytics Professional Comptia Security+ Lead external Auditor for 27001. 22301 Splunk Enterprise Security Certified Administrator Symantec sertifikovani specijalista	Dugogodišnje iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.

4.	Mišo Vraneš, 25 godina	IT infrastructure expert	Dell PowerMax and VMAX Family Solutions Operate 2023 certificate, HP Accredited Platform Specialist HP StorageWorks MSA1000 and MSA 1500 2005, HP Accredited Solutions Expert Advanced Server Administrator V8, HP Accredited Technical Proffesional BladeSystem Solutions Integrator V8.1, HP Master Accredited Storage Solutions Acrhitect V1, Microsoft Certified Professional, Specialist - Implementation Engineer, Dell EMC Unity Solutions Version 1.0, Specialist - Implementation Engineer, NetWorker Version 7.0, Specialist - Implementation Engineer, PowerMax and VMAX Family Solutions Version 1.0, Specialist - Platform Engineer, PowerMax and VMAX All Flash Version 2.0, VEEAM CErtified Engineer	Ekspert u segmentu IT infrastrukture: Servers, Storage, Backup, Linux, Vmware, HyperV
5.	Mladen Joknić 14 godina	Implementacija bezbednosti	Ekspert Symantec Endpoint Security rješenje Symantec sertifikovani specijalista	Dugogodišnje iskustvo u projektovanju, implementaciji Symantec Endpoint Security rješenja
6.	Slobodan Bulatović, 25 godina	IT infrastructure expert	Dell PowerMax and VMAX Family Solutions Operate 2023 certificate, HP Accredited Platform Specialist HP StorageWorks MSA1000 and MSA 1500 2005, HP Accredited Solutions Expert Advanced Server Administrator V8, HP Accredited Technical Proffesional BladeSystem Solutions Integrator V8.1,	Ekspert u segmentu IT infrastrukture: Servers, Storage, Backup, Linux, Vmware, HyperV

			HP Master Accredited Storage Solutions Acrhitect V1, Microsoft Certified Professional, Specialist - Implementation Engineer, Dell EMC Unity Solutions Version 1.0, Specialist - Implementation Engineer, NetWorker Version 7.0, Specialist - Implementation Engineer, PowerMax and VMAX Family Solutions Version 1.0, Specialist - Platform Engineer, PowerMax and VMAX All Flash Version 2.0, VEEAM CErtified Engineer, Vmware Certified Professional 5 - Data Center Virtualization, Vmware Certified Professional - Data Center Virtualization 2022	
7.	Marko Čarapić 9 godina	Implementacija mrežne bezbjednosti	Checkpoint Administrator CP Expert CP CCFE CP CCTE Palo alto Network security administrator Aruba Switching and routing Aruba mobile Associate Cisco CCNA Sophos Central engineer, XG firewall F5 BIGIP Administrator	Dugogodišnje iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
8.	Tijana Radulović 6 godine	Implementacija mrežne bezbjednosti	Checkpoint Administrator CP Expert CP CCFE CP CCTE Palo alto Network security administrator Aruba Switching and routing Aruba mobile Associate	Dugogodišnje iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.

			Cisco CCNA F5 BIGIP Administrator	
9.	Bogdan Šćekić 3 godine	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner CompTIA CySA+ ce (Cybersecurity Analyst) CompTIA Security+ CompTIA Advanced Security Practitioner – SecurityX INE Security eJPT Junior Penetration Tester CompTIA PenTest+	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
10.	Balša Božović 4 godine	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner Stellar Cyber SOC Analyst Associate CompTIA CySA+ ce (Cybersecurity Analyst) CompTIA Secure Infrastructure Specialist – CSIS CompTIA Security Analytics Expert – CSAE CompTIA Security Analytics Professional – CSAP CompTIA Security+ ce CompTIA Advanced Security Practitioner – SecurityX ce Symantec 250-580 Endpoint Security Complete R2	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
11.	Nikola Radaković 5 godine	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner CompTIA CySA+ ce (Cybersecurity Analyst) CompTIA Security+ ce CompTIA Advanced Security Practitioner – SecurityX ce	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
12.	Sava Tomović 2 godine	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner Stellar Cyber SOC Analyst Associate Fortinet Certified Professional Network Security Comptia Security+	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.

13.	Zvonko Popović 3 godine	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner Stellar Cyber SOC Analyst Associate Symantec 250-580 Endpoint Security Complete R2	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
14.	Ognjen Šćekić 1 godinu	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner Stellar Cyber SOC Analyst Associate CompTIA Security+ CompTIA PenTest+	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
15.	Danko Krstonijević 3 godinu	Implementacija mrežne bezbednosti	Stellar Cyber SOC Analyst Associate CompTIA Security+	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
16.	Miljan Golubović 1 godinu	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner Stellar Cyber SOC Analyst Associate	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.
17.	Bojana Beljkaš 2 godine	Implementacija mrežne bezbednosti	Cynet Certified Technical Partner Stellar Cyber SOC Analyst Associate	Iskustvo u implementaciji i održavanju bezbjednosnog informacionog sistema.

6. Čikom SOC

Čikomov bezbjednosni operativni centar (SOC) predstavlja centralnu operativnu funkciju koja integriše ljude, procese i tehnologije u cilju efikasnog otkrivanja, analize i odgovora na bezbjednosne prijetnje i incidente. SOC se sastoji od definisanih operativnih procesa, naprednih bezbjednosnih tehnologija i tima iskusnih i sertifikovanih bezbjednosnih analitičara iz različitih IT i bezbjednosnih domena. Čikom SOC pruža usluge u režimu 24x7x365, djelujući kao produžetak interne IT i bezbjednosne funkcije.

SOC aktivnosti se realizuju u skladu sa relevantnim regulatornim i industrijskim okvirima (uključujući ISO/IEC 27001, DORA, NIS2 i GDPR), u mjeri u kojoj se odnose na obim pružene SOC usluge, uz puno poštovanje internih politika i procedura.

6.1. Ključne funkcije SOC-a:

- **Praćenje i otkrivanje -** Kontinuirano praćenje bezbjednosnih događaja i analiza sumnjivih aktivnosti na osnovu log zapisa, mrežnog saobraćaja i bezbjednosnih upozorenja.
- **Incident Response -** Pravovremena trijaža, istraga i podrška u odgovoru na bezbjednosne incidente, uključujući preporuke za zadržavanje, sanaciju i oporavak.
- **Threat Intelligence -** Prikupljanje, analiza i primjena informacija o aktuelnim i novim prijetnjama, uključujući prijetnje izvan informacionog sistema klijenta.
- **Usklađenost** - Regulatorna i proceduralna podrška klijentu u ispunjavanju regulatornih i internih zahtjeva kroz SOC procese, evidenciju incidenata i izvještavanje.
- **Izvještavanje**: Operativni, tehnički i menadžerski izvještaji o bezbjednosnim događajima, incidentima, SLA metrima i trendovima rizika, uključujući ad hoc i izvršne izvještaje.

6.2. Komponente SOC:

Komponenta	Opis
SIEM (Security Information and Event Management)	Centralizovano prikupljanje, analiza i korelacija sigurnosnih događaja. Integracija sa postojećim SIEM sistemom.
EDR/XDR (Endpoint & Extended Detection and Response)	Integracija sa EDR/XDR rješenjima radi detekcije i odgovora na prijetnje na krajnjim tačkama i širem okruženju.
Threat Intelligence Platform	Korišćenje TI izvora i platformi za identifikaciju prijetnji i kampanja.
Network Traffic Analysis (NTA)	Analiza mrežnog saobraćaja za otkrivanje anomalija i zlonamjernih aktivnosti.
Incident Response & Forensics	Podrška u reagovanju na incidente i sprovođenje digitalne forenzičke analize
SOAR	Orkestracija i automatizacija bezbjednosnih procesa i odgovora na incidente.
Vulnerability awareness (savjetodavno)	Identifikacija i korelacija informacija o ranjivostima sa detektovanim prijetnjama (bez aktivnog skeniranja)

6.3. Čikom SOC Tim – Struktura i Uloge

Ime i Prezime	SOC Tier	Pozicija	Opis uloge
Mladen Bukilić	Manager	SOC Manager	Vođenje tima, strateško planiranje i nadzor
Balša Božović	Tier 3	SOC Tim lider	Forenzika, eskalacija i mentorstvo, Incident response koordinacija, napredna analiza prijetnji, forenzika, proaktivni lov prijetnji
Bogdan Šćekić	Tier 3	Senior Analyst	Incident response, napredna analiza prijetnji, forenzika, proaktivni lov prijetnji,
Nikola Radaković	Tier 2	Senior Analyst	Praćenje alarma, analiza događaja, koordinacija sa Tier 1 i 3
Sava Tomović	Tier 2	Senior Analyst	Praćenje alarma, analiza događaja, koordinacija sa Tier 1 i 3
Zvonko Popović	Tier 1	Analyst	Prva linija detekcije, monitoring sistema, prijava sumnjivih aktivnosti, evidencija i osnovna analiza incidenata
Ognjen Šćekić	Tier 1	Analyst	Prva linija detekcije, trijaža i monitoring sistema, prijava sumnjivih aktivnosti, evidencija i osnovna analiza incidenata
Danko Krstonijević	Tier 1	Analyst	Prva linija detekcije, monitoring sistema, prijava sumnjivih aktivnosti, evidencija i osnovna analiza incidenata

Miljan Golubović	Tier 1	Analyst	Prva linija detekcije, monitoring sistema, prijava sumnjivih aktivnosti, evidencija i osnovna analiza incidenata
Bojana Beljkaš	Tier 1	Analyst	Prva linija detekcije, monitoring sistema, prijava sumnjivih aktivnosti, evidencija i osnovna analiza incidenata
Almir Karastanović	Tier 2	Senior Analyst	Praćenje alarma, analiza događaja, koordinacija sa Tier 1 i 3
Mladen Joknić	Tier 2	Senior Analyst	Praćenje alarma, analiza događaja, koordinacija sa Tier 1 i 3
Slobodan Bulatović	Tier 3	Senior Analyst	Forenzika, Incident response, napredna analiza prijetnji, forenzika, proaktivni lov prijetnji.
Mišo Vraneš	Tier 3	Senior Analyst	Forenyika, Incident response, napredna analiza prijetnji, forenzika, proaktivni lov prijetnji.
Ostali timovi (20 inžinjera)	Tler 2 i 3	Expert analysts in different segments	U slučaju da je neophodno angažman ostalih stručnih timova Čikoma (Infrastruktura, Microsoft, Network Security,...)

6.4. Onboarding process

Proces uvođenja SOC usluge osmišljen je tako da obezbijedi sigurnu, kontrolisanu i regulatorno usklađenu integraciju klijenta u SOC operativni model.

SOC onboarding predstavlja sveobuhvatan proces koji podrazumijeva tehničku analizu, pravno-regulatornu usklađenost, edukaciju korisnika i kontinuiranu komunikaciju, sa ciljem da klijent od samog početka ima potpunu vidljivost svoje bezbjednosne pozicije i maksimalnu korist od SOC usluge.

Onboarding i implementacioni proces obuhvata korake koji podržavaju pristup validaciji sistema kroz DQ, IQ, OQ i PQ aktivnosti, uključujući procjenu zahtjeva, tehničku integraciju, funkcionalno testiranje, validaciju alarmiranja i operativnu verifikaciju sistema.

Faze procesa uvođenja:

1. Inicijalni kontakt i priprema:
   - Uvodni sastanak sa predstavnicima kompanije
   - Potpisivanje NDA i razmjena osnovnih informacija
   - Definisanje inicijalnih ciljeva, očekivanja i opsega SOC usluge

2. Procjena potreba i postojećeg stanja:
   - Prikupljanje informacija o poslovnim ciljevima i IT infrastrukturi
   - Analiza postojećih sistema, aplikacija, korisničkih naloga i log izvora
   - Identifikacija regulatornih, sigurnosnih i internih zahtjeva
   - Izrada preporuka za optimizaciju i integraciju u SOC uslugu

3. Ugovaranje i definisanje operativnog modela
   - Formalizacija saradnje kroz ugovor i SLA
   - Definisanje kontakt osoba (SPOC), eskalacionih procedura i komunikacionih kanala

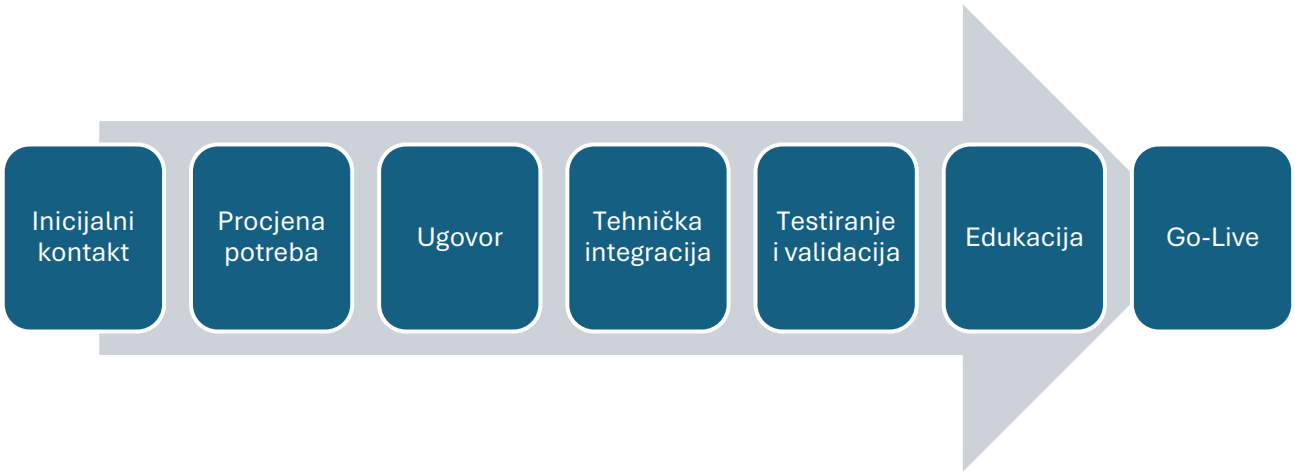
- Usaglašavanje vremena odziva i odgovornosti

4. Tehnička integracija
   - Integracija sistema klijenta sa SOC rješenjem putem sigurnih konekcija
   - Konfiguracija prikupljanja log zapisa i senzora
   - Integracija sa postojećim SIEM sistemom klijenta, ukoliko klijent ima implementirano SIEM rješenje

5. Testiranje i validacija:
   - Verifikacija tehničke funkcionalnosti i korelacije događaja
   - Testiranje alertinga i eskalacija
   - Simulacija sigurnosnih incidenata radi provjere SLA i procedura

6. Edukacija i priprema za produkciju:
   - Edukacija odgovornih osoba o SOC operativnom modelu
   - Upoznavanje sa procedurama incident response-a, komunikacije i eskalacije
   - Obuka za korišćenje SOC portala i izvještaja

7. Operativno puštanje u rad (Go-Live):
   - Aktivacija kontinuiranog 24x7x365 nadzora
   - Operativno upravljanje sigurnosnim događajima i incidentima
   - Redovno izvještavanje u skladu sa ugovorenim SLA parametrima



6.5. Operativni SOC model – Operating Model

Čikomov SOC tim radi u modelu:

- Tier 1
- Tier 2
- Tier 3

Čikom SOC ima definisane interne BCP i DR procedure koje obezbjeđuju kontinuitet SOC usluge i dostupnost ključnih funkcija u slučaju incidenta ili prekida rada, u skladu sa ugovorenim SLA parametrima.

Pristup SOC platformi i podacima klijenta je striktno kontrolisan po principu najmanjih privilegija (least privilege). Administrativni i analitički pristup imaju isključivo ovlašćeni članovi Čikom SOC tima, uz višefaktorsku autentifikaciju i evidenciju pristupa. SOC operacije se izvode iz kancelarija Čikom d.o.o. u Crnoj Gori. Svi pristupi i aktivnosti su logovani i dostupni za reviziju na zahtjev klijenta. SOC platforma podržava audit logging, kontrolu

pristupa, evidenciju aktivnosti korisnika i sigurnosne mehanizme koji podržavaju zahtjeve 21 CFR Part 11, uključujući sljedivost aktivnosti, autentifikaciju korisnika i reviziju bezbjednosnih događaja.

- **Tier 1 – Monitoring i trijaža (24x7x365)**

Opseg aktivnosti:

- Kontinuirano i proaktivno praćenje sigurnosnih događaja u režimu **24x7x365**
- Trijaža upozorenja, uključujući obogaćivanje događaja informacijama o prijetnjama, dodavanje konteksta i rangiranje nivoa kritičnosti (severity)
- Identifikacija i eliminacija lažno pozitivnih i benignih upozorenja
- Dokumentovanje početnih nalaza i kreiranje sigurnosnih incidenata u ticketing sistemu

Koordinacija sa SPOC-om klijenta:

Za sve sigurnosne događaje srednjeg, visokog ili kritičnog prioriteta, Tier 1:

- Obavještava definisani SPOC na strani klijenta
- Dostavlja rezime incidenta koji uključuje pogođene sisteme, preliminarni kontekst i inicijalnu procjenu uticaja
- Eskalacija na Tier 2 se vrši automatski u skladu sa definisanim SLA vremenima, bez potrebe za eksplicitnim odobrenjem, dok se SPOC kontinuirano informiše o toku istrage i preduzetim aktivnostima

- **Tier 2 – Incident Investigation & Deep Analysis**

Opseg aktivnosti:

- Aktivira se automatski u skladu sa SLA pravilima ili po detekciji incidenta koji zahtijeva detaljniju analizu
- Detaljna analiza log zapisa, mrežnog saobraćaja (flow data) i obrazaca napada
- Analiza ponašanja sistema i korisnika korišćenjem napredne analitike
- Mapiranje prijetnji i tehnika napada korišćenjem MITRE ATT&CK okvira
- Identifikacija uzroka incidenta, njegovog obima i potencijalnog uticaja
- Definisanje i preporuka mjera za zadržavanje incidenta (containment) i narednih koraka za sanaciju

- **Tier 3 – Threat Hunting, Threat Intelligence, Remediation Support**

Opseg aktivnosti:

- Aktivira se u slučaju potvrđenih, naprednih ili perzistentnih prijetnji, kao i u okviru planiranih threat hunting aktivnosti
- Proaktivni lov na prijetnje kroz analizu postojećih logova, mrežnog saobraćaja i ponašanja sistema
- Razvoj prilagođenih detekcionih pravila, logike napada i analitičkih dashboarda
- Koordinacija sa timovima klijenta u cilju sanacije i zadržavanja incidenta
- Izrada post-incident izvještaja i definisanje preventivnih mjera za unapređenje bezbjednosti
- Sprovođenje digitalne forenzike, uključujući analizu memorije, diskova i mrežnog saobraćaja
- Koordinacija incident response aktivnosti i davanje smjernica Tier 1 i Tier 2 timovima
- Aktivno otkrivanje prijetnji koje nisu identifikovane automatizovanim alatima, uz korišćenje više izvora informacija radi formiranja potpune slike incidenta
- Penetration testing

7. Tehnička specifikacija

7.1. Cyber Security Platform

Implementacija platforme za sajber bezbjednost dizajnirana da unaprijedi bezbjednosne operacije kroz automatizaciju i vještačku inteligenciju. Integriše različite bezbjednosne alate i mogućnosti kako bi obezbijedio jedinstven pristup otkrivanju i reagovanju na prijetnje. Ovo rješenje je licencirano na end-to-end osnovi (server, laptop / PC, Firewall).

Ovo rješenje može biti implementirano:

- Cloud based
- On prem
- Hibridno – za vas smo ponudu pripremili u skladu sa ovim modelom

Model primene	Opis	Gde je implementiran	Osnovne komponente	Postavljanje senzora	Protok podataka
Cloud	Sve komponente hostovane u Cloudu (npr. AWS, Azure, Google)	Cloud	Korisnički interfejs za upravljanje, Data Lake, Analitics Engine u Cloudu	Cloud VPC-ovi, on-prem mreže, krajnje tačke	Senzori prosleđuju podatke na platformu u cloudu putem sigurnih kanala
On-Prem	Sve komponente raspoređene u klijentovom data centru ili privatnom cloud-u	Infrastruktura u vlasništvu klijenta	Korisnički interfejs za upravljanje, Data Lake, Analitics Engine on-prem	Korporativne mreže, krajnje tačke, perimetar data centra	Senzori prosleđuju podatke na on-prem platformu preko interne mreže
Hibridno	Kombinacija analitike u Cloud-u i lokalnog prikupljanja podataka	Cloud + klijentska infrastruktura	Korisnički interfejs za upravljanje i analitika u oblaku; Senzori i opcioni Data Lake on-prem	Cloud VPC-ovi, on-prem mreže i krajnje tačke	Senzori prosleđuju informacije u Cloud analitiku ili lokalno u zavisnosti od politike

- U svakom scenariju potrebno je implementirati/instalirati agente i NDR sensor/e. NDR senzori mogu biti implementirani/instalirani kao virtuelne mašine ili fizički uređaji.
- Broj licenci se izračunava na osnovu broja krajnjih tačaka (endpoint), firewall, servera i usera M365. Broj usera se moze korigovati bez problema (finansijski dio za broj licenci se može korigovati kroz definisanje uslova u ugovoru i na kraju isteka)
- Podrzani Windows i Linux sistemi
- Sistem je dostupan 99,9%

Komponente Cyber Security uključene u našu ponudu:

- SOAR sledeće generacije (bezbjednosna orkestracija, automatizacija, odgovor),
- Mrežna detekcija i odgovor (NDR)
  - Vidljivost: Obezbjeđuje praćenje mreže i otkrivanje prijetnji, eliminišući slijepe tačke u bezbjednosti mreže.
  - Automatizovani odgovor: Automatizuje lov na prijetnje i odgovor, smanjujući potrebu za ručnom intervencijom.
  - Mrežni senzori mogu biti VM ili fizički uređaj
- Open Extended Detection and Response (Open XDR)
  - Integracija: Kombinuje podatke iz različitih bezbjednosnih alata, uključujući detekciju krajnjih tačaka, detekciju mreže i Cloud security, kako bi pružio jedinstven pogled na prijetnje.
  - Multi-layer AI: Koristi naprednu AI za analizu podataka na cijeloj površini napada (attack surface), poboljšavajući tačnost i brzinu otkrivanja prijetnji.
- Next Gen SIEM (NG-SIEM):

  - Prikupljanje podataka i normalizacija: Prikuplja i normalizuje bezbjednosna upozorenja, logove i telemetriju iz bilo kog izvora, pretvarajući različite podatke u konzistentan format za analizu.
  - User-friendly interfejs: Dizajniran da bude jednostavan za korišćenje i primjenu, što ga čini dostupnim bezbjednosnim timovima svih veličina.
- TIP (Threat inteligenced platform - platforma za obavještavanje o prijetnjama):
  - Integracija: Prikuplja i integriše obavještajne podatke o prijetnjama iz više izvora kako bi poboljšao otkrivanje i odgovor na prijetnje.
  - Obogaćivanje: Obogaćuje bezbjednosne podatke kontekstualnim obavještavanjem o prijetnjama, poboljšavajući tačnost detekcija.
  - Korelacija: Povezuje obavještavanje o prijetnjama sa bezbjednosnim događajima kako bi pružio dublji uvid u potencijalne prijetnje.
- UEBA (Analitika ponašanja korisnika i entiteta):
  - Analiza ponašanja: Prati i analizira ponašanje korisnika i entiteta kako bi otkrio anomalije koje mogu ukazivati na insajderske prijetnje ili kompromitovane račune.
  - Fuzija podataka: Prikuplja podatke iz različitih izvora, kao što su SIEM alati, mrežni saobraćaj i logovi sa Active Directory, kako bi pružili sveobuhvatan pregled aktivnosti korisnika.
  - Otkrivanje anomalija: Koristi mašinsko učenje za identifikaciju neobičnih obrazaca ponašanja koji odstupaju od norme.

7.2. Qualys Vulnerability Management, Detection and Response

Qualys Vulnerability Management, Detection and Response (VMDR) je napredno cloud rješenje za upravljanje ranjivostima i sajber prijetnjama u IT okruženju. Platforma omogućava organizacijama da u realnom vremenu otkrivaju, analiziraju, prioritizuju i otklanjaju sigurnosne propuste na serverima, računarima, cloud sistemima, aplikacijama, IoT i OT uređajima — sve kroz jednu centralizovanu platformu.

- Broj licenci se izračunava na osnovu broja asseta. Broj asseta se moze korigovati bez problema (finansijski dio za broj licenci se može korigovati kroz definisanje uslova u ugovoru i na kraju isteka)
- Podrzani Windows i Linux sistemi

Glavne funkcionalnosti

- Detekcija ranjivosti
  - Kontinuirano skeniranje sistema pomoću: Cloud Agent-a, mrežnih skenera, pasivnih senzora
  - Otkrivanje poznatih sigurnosnih propusta i CVE ranjivosti
- Prioritizacija rizika (TruRisk)
  - Procjena rizika na osnovu: kritičnosti Sistema, dostupnih exploit alata, aktivnih prijetnji u svijetu, poslovnog uticaja
  - Fokus na ranjivosti koje predstavljaju najveći stvarni rizik
- Praćenje u realnom vremenu
  - Neprekidno praćenje promjena i novih prijetnji
  - Automatska upozorenja za kritične ranjivosti

7.3. Privileged Access Management (PAM)

WALLIX PAM (Privileged Access Management) je sigurnosno rješenje namijenjeno zaštiti, kontroli i nadzoru privilegovanih pristupa kritičnim IT sistemima i resursima organizacije.

Omogućava centralizovano upravljanje administratorskim i drugim privilegovanim nalozima, kao i preciznu kontrolu ko može pristupiti određenom sistemu, kada i pod kojim uslovima. Pristup se može omogućiti bez direktnog otkrivanja administratorskih lozinki korisnicima, čime se dodatno smanjuje mogućnost njihove zloupotrebe.

WALLIX PAM takođe omogućava praćenje i snimanje privilegovanih sesija, pa organizacija može imati detaljan zapis aktivnosti administratora, eksternih saradnika i drugih korisnika sa visokim nivoom ovlašćenja. Ovo je posebno značajno za sigurnosne provjere, istrage incidenata i audit.

8. Service Level Agreements (SLA)

Severity	Tier 1 – Monitoring i trijaža	Tier 2 – Istraga	Tier 3 – Napredna analiza	Ciljno vrijeme rješavanja
Critical	≤ 30 minuta	Immediate	≤ 2 sata	≤ 6 sati
High	≤ 60 minuta	≤ 2 sata	≤ 4 sata	≤ 18 sati
Medium	≤ 3 sata	≤ 4 sata	≤ 24 sata	≤ 48 sati
Low	≤ 24 sata	≤ 24 sata	Po potrebi	≤ 30 dana*
Info	≤ 48 sati	Best effort	N/A	≤ 30 dana*

* Incidenti niskog i informativnog prioriteta se formalno obrađuju i izvještavaju u skladu sa zahtjevima tendera kroz redovne mjesečne izvještaje.

Severity (SOC)	Kritičnost	Opis uticaja
Critical	Kritičan incident	Ozbiljan uticaj na povjerljivost, integritet ili dostupnost; značajan uticaj na poslovanje
High	Incident visokog prioriteta	Značajan uticaj na dio poslovanja ili ključne sisteme
Medium	Incident srednjeg prioriteta	Ograničen uticaj na manji dio poslovanja
Low	Incident niskog prioriteta	Zanemarljiv uticaj na poslovanje
Info	Informativni događaj	Nema direktnog uticaja; informativnog karaktera

9. Reporting, KPI, Governance i praćenje kvaliteta usluge

Izvjestaj	Frequency	Opis
Dnevni SOC izvještaj	Dnevno	Operativni pregled bezbjednosnih događaja, obim detektovanih prijetnji, status trijaže i otvoreni incidenti
Sedmični SOC izvještaj	Nedeljno	Rezime detektovanih incidenata, ključne metrike odziva, status eskalacija i otvorena operativna pitanja
Mjesečni SOC izvještaj	Mjesečno	Izvještaj o operativnom radu SOC usluge, analiza trendova rizika, pregled incidenata, praćenje SLA parametara i preporuke za unapređenje bezbjednosti
Izvještaj o threat hunting aktivnostima	Kvartalno	Dokumentovani rezultati ciljanih istraga, korišćeni scenariji i podaci, identifikovane prijetnje i preporučene mjere
Executive Briefing	Kvartalno	Pregled strateških prijetnji, trendova u napadima, procjena rizika i preporuke za menadžment

9.1. Ključni KPI pokazatelji

Kvalitet SOC usluge prati se kroz skup mjerljivih pokazatelja koji se redovno izvještavaju:

- MTTD (Mean Time To Detect) – prosječno vrijeme detekcije bezbjednosnog događaja
- MTTR (Mean Time To Respond) – prosječno vrijeme reakcije na incident
- SLA usklađenost – procenat incidenata obrađenih u skladu sa definisanim SLA vremenima
- Broj i kritičnost incidenata – raspodjela po Critical / High / Medium / Low
- Stopa lažno pozitivnih alerta
- Trendovi i ponavljajući uzroci incidenata

9.2. Izvještavanje i transparentnost

- Operativni izvještaji se dostavljaju u skladu sa ugovorenom dinamikom (dnevni, sedmični, mjesečni i kvartalni).
- Svi bezbjednosni incidenti se evidentiraju i dostupni su za reviziju.
- Klijent ima uvid u status otvorenih incidenata i mjere koje su preduzete ili preporučene.

9.3. Governance i upravljanje uslugom

- Definisana je jasna podjela odgovornosti između Klijenta i Čikom SOC tima (RACI model).
- Održavaju se **periodični servisni sastanci** (najmanje kvartalno) radi:
  - pregleda performansi SOC usluge
  - analize trendova prijetnji
  - razmatranja preporuka za unapređenje bezbjednosti
- Po potrebi se organizuju ad-hoc sastanci u slučaju značajnih bezbjednosnih događaja.

9.4. Kontinuirano unapređenje

SOC usluga se kontinuirano unapređuje kroz:

- prilagođavanje detekcionih pravila i use-case scenarija
- unapređenje incident playbook-ova
- integraciju novih izvora prijetnji i obavještajnih podataka
- preporuke za tehničke i organizacione mjere unapređenja bezbjednosti klijenta

10. Obaveze i resursi klijenta (Customer Responsibilities)

10.1. Tehnički resursi klijenta

Klijent obezbjeđuje sljedeće resurse neophodne za uspješnu implementaciju i operativni rad SOC usluge:

- Pristup relevantnim log izvorima (serveri, mrežna oprema, endpointi, aplikacije)
- Infrastrukturu za on-premise instalaciju (virtuelne ili fizičke resurse za senzore)
- Mrežnu povezanost i firewall pravila potrebna za SOC integraciju
- Svi endpoint-i moraju imati EDR-XDR rješenje instalirano

10.2. Organizacijski i kadrovski resursi

Klijent imenuje:

- SPOC (Single Point of Contact) za operativnu komunikaciju sa SOC timom
- Odgovorne osobe za:
  - Odobravanje eskalacija i remediation aktivnosti
  - Koordinaciju sa internim IT i bezbjednosnim timovima
  - Kontakt osobe dostupne u skladu sa ugovorenim SLA vremenima

10.3. Operativna saradnja

Klijent je odgovoran za:

- Sprovođenje preporučenih remediation mjera na svojim sistemima
- Obezbjeđivanje pravovremenih povratnih informacija tokom istraga
- Učešće u periodičnim sastancima, revizijama i edukacijama
- Čikom SOC ne sprovodi destruktivne ili poslovno-kritične remediation aktivnosti (npr. izolacija sistema, blokade servisa, izmjene konfiguracije) bez saglasnosti klijenta, osim ako nije drugačije ugovoreno. Klijent zadržava krajnju odgovornost i odluku o sprovođenju mjera sanacije.

10.4. RACI matrica i plan implementacije

Aktivnost	Čikom SOC	Klijent
Monitoring i detekcija	R	I
Trijaža i klasifikacija	R	I
Incident investigation	R	I
Threat hunting	R	I
Preporuka remediation mjera	R	C
Odobravanje remediation mjera	I	A
Implementacija - remediation	C	R
Izvještavanje	R	I

Legenda: **R** – Responsible, **A** – Accountable, **C** – Consulted, **I** – Informed

Plan implementacije

Faza	Opis	Rok
Inicijalna priprema	NDA, SPOC, plan implementacije	do 10 dana
Tehnička integracija	Log izvori, SIEM, senzori	do 10 dana
Testiranje i validacija	Alarm, SLA, eskalacija	do 5 dana
Edukacija	Operativna i proceduralna	do 5 dana
SOC Go-Live	24x7x365 monitoring	**≤ 30 dana**

11. Finansijska specifikacija

- ***2027 godina***

Naziv usluge	Cijena za 12 mjeseci
SOC usluge sa uključenim Stellar Cyber licencama	25.200,00 €
Qualys Vulnerability Management – 40 licenci	7.500,00 €
PAM minimalno 50 licenci	7.000,00 €
Total bez PDV-a	39.700,00 €

- ***2028 godina***

Naziv usluge	Cijena za 12 mjeseci
SOC usluge sa uključenim Stellar Cyber licencama	28.980,00 €
Qualys Vulnerability Management – 40 licenci	8.625,00 €
PAM minimalno 50 licenci	8.050,00 €
Total bez PDV-a	45.655,00 €

- ***2029 godina***

Naziv usluge	Cijena za 12 mjeseci
SOC usluge sa uključenim Stellar Cyber licencama	33.300,00 €
Qualys Vulnerability Management – 40 licenci	9.900,00 €
PAM minimalno 50 licenci	9.260,00 €
Total bez PDV-a	52.460,00 €

Ivan Stanković,
Cyber security menadžer prodaje

Podgorica, 24.08.2026