FINANCIJSKA AGENCIJA

OIB: 85821130368

Mažuranićevo šetalište 24b

(adresa nadležne jedinice)

FINANCIJSKA AGENCIJA
RC SPLIT 1
23 -10- 2026
PREDSTEČAJNE NAGODBE
PRIMANJE I OTPREMA POŠTE
KLASA 034-011/26-10/18
UR. BROJ 118-08-5012-26-510

Nadležni trgovački sud Trgovački sud u Splitu

Poslovni broj spisa **St-431/2026-20**

PRIJAVA TRAŽBINE VJEROVNIKA U PREDSTEČAJNOM POSTUPKU

PODACI O VJEROVNIKU:

Ime i prezime / tvrtka ili naziv
KONČAR - Digital d.o.o.

OIB **55191916939**

Adresa / sjedište
Fallerovo šetalište 22, Zagreb

PODACI O DUŽNIKU:

Ime i prezime / tvrtka ili naziv
STUDENAC d.o.o.

OIB **02023029348**

Adresa / sjedište
Četvrt Ribnjak 17, Omiš

PODACI O TRAŽBINI:

Pravna osnova tražbine (npr. ugovor, odluka suda ili drugog tijela, ako je u tijeku sudski postupak oznaku spisa i naznaku suda kod kojeg se postupak vodi)
Rješenje od 29.09.2026. St-431/2026 Trgovački sud u Splitu Ugovor o pružanju usluga sigurnosno operacijskog centra

Iznos dospjele tražbine **3750,00** (EUR)

Glavnica **3750,00** (EUR)

Kamate **0,00** (EUR)

Iznos tražbine koja dospijeva nakon otvaranja predstečajnog postupka
3625,00 (EUR)

Dokaz o postojanju tražbine (npr. račun, izvadak iz poslovnih knjiga)
Račun 2600529-41-1, 2600622-41-1, Ugovor br. 25-26-00044/850, kartica otv. stavki

Vjerovnik raspolaže ovršnom ispravom DA ☐ NE ☒ za iznos_____ (EUR)

Naziv ovršne isprave

_____

PODACI O RAZLUČNOM PRAVU:

Pravna osnova razlučnog prava

_____

_____

Dio imovine na koji se odnosi razlučno pravo

_____

_____

Iznos tražbine_____ (EUR)

Razlučni vjerovnik odriče se prava na odvojeno namirenje
ODRIČEM ☐ NE ODRIČEM ☐

Razlučni vjerovnik pristaje da se odgodi namirenje iz predmeta na koji se odnosi njegovo razlučno pravo radi provedbe plana restrukturiranja PRISTAJEM ☐ NE PRISTAJEM ☐

PODACI O IZLUČNOM PRAVU:

Pravna osnova izlučnog prava

_____

_____

Dio imovine na koji se odnosi izlučno pravo

_____

_____

Izlučni vjerovnik pristaje da se izdvoji predmet na koji se odnosi njegovo izlučno pravo radi provedbe plana restrukturiranja PRISTAJEM ☐ NE PRISTAJEM ☐

Mjesto i datum

ZAGREB, 21. 10. 2026.

Potpis vjerovnika

KONČAR
DIGITAL

KONČAR - Digital d.o.o.
Fallerovo šetalište 22, 10000 Zagreb 5

KONČAR
DIGITAL

ISO 9001 • 10002 • 14001 • 18295-1 • 20000-1 • 22301
27001 • 27701 • 37001 • 42001 • 45001 • 50001 • 55001

Končar – Digital d.o.o. za digitalne usluge
Hrvatska
10000 Zagreb
Fallerovo šetalište 22
OIB: 55191916939
Tel:
IBAN: HR4424840081135357397

STUDENAC d.o.o.
Četvrt Ribnjak 17
21310 Omiš
Hrvatska

OIB: 02023029348

RAČUN BROJ: 2600529-41-1

Oznaka: 2600529-41-1

Mjesto i datum računa: Zagreb, 31.8.2026.

Dospijeće: 30.9.2026.

ŠIFRA KUPCA: 0679
DATUM ISPORUKE / GOTOVOST: 31.8.2026.
BROJ UGOVORA: 25-26-00044/850
NAČIN PLAĆANJA: Transakcijski račun

Ugovor o pružanju usluga sigurnosnog operacijskog centra

R.B.	Opis	KOLIČINA	JMJ	JEDINIČNA CIJENA (EUR)	IZNOS (EUR) bez PDV-a
1	Mjesečna naknada za pružanje SOC usluga za kolovoz 2026.	1	KOM	3.000,00	3.000,00
			UKUPNO (EUR):		3.000,00
			POREZ 25% (EUR):		750,00
			SVEUKUPNO (EUR):		**3.750,00**

PRILIKOM PLAĆANJA NAVESTI POZIV NA BROJ: 0679-8501241-260529

PLATITI
u roku od 30 dana, do 30.09.2026
3.750,00 EUR

Izradio: KRISTINA BLAŽEVIĆ

Odobrio: STJEPAN SUČIĆ

VRIJEME IZDAVANJA RAČUNA: 31.8.2026. 13:00:38

KONČAR
DIGITAL

ISO 9001 • 10002 • 14001 • 18295-1 • 20000-1 • 22301
27001 • 27701 • 37001 • 42001 • 45001 • 50001 • 55001

Končar – Digital d.o.o. za digitalne usluge
Hrvatska
10000 Zagreb
Fallerovo šetalište 22
OIB: 55191916939
Tel:
IBAN: HR4424840081135357397

STUDENAC d.o.o.
Četvrt Ribnjak 17
21310 Omiš
Hrvatska

OIB: 02023029348

RAČUN BROJ: 2600622-41-1

Oznaka: 2600622-41-1

Mjesto i datum računa: Zagreb, 29.9.2026.

Dospijeće: 30.10.2026.

ŠIFRA KUPCA: 0679
DATUM ISPORUKE / GOTOVOST: 29.9.2026.
BROJ UGOVORA: 25-26-00044/850
NAČIN PLAĆANJA: Transakcijski račun

Ugovor o pružanju usluga sigurnosnog operacijskog centra

R.B.	Opis	KOLIČINA	JMJ	JEDINIČNA CIJENA (EUR)	IZNOS (EUR) bez PDV-a
1	Mjesečna naknada za pružanje SOC usluga za razdoblje od 01.09.2026. do 29.09.2026.	1	KOM	2.900,00	2.900,00

UKUPNO (EUR):	2.900,00
POREZ 25% (EUR):	725,00
SVEUKUPNO (EUR):	**3.625,00**

PRILIKOM PLAĆANJA NAVESTI POZIV NA BROJ: 0679-8501241-260622

PLATITI
u roku od 30 dana, do 30.10.2026
3.625,00 EUR

Izradio: KRISTINA BLAŽEVIĆ

Odobrio: STJEPAN SUČIĆ

VRIJEME IZDAVANJA RAČUNA: 8.10.2026. 8:42:45

Kartica kupca (otvorene stavke) (PO DATUMU DOKUMENTA)

Na dan: 30.9.2026.

Tip računa: SVI Valuta: EUR

Partner 0679 STUDENAC d.o.o. (OIB:02023029348)

Četvrt Ribnjak 17 21310 Omiš Hrvatska, Tel: , Fax: , Podr. komerc.: , , IBAN: HR9023600001502766885

Dokument	Dat. dok.	Duguje	Potražuje	Dat. dosp.	Eksterni br.	Konto	Opis	Saldo part.
41 2600529-41-1	31.08.26	3.750,00	0,00	30.09.26		1200		3.750,00
41 2600622-41-1	29.09.26	3.625,00	0,00	30.10.26		1200		7.375,00
41 2600623-41-1	30.09.26	125,00	0,00	30.10.26		1200		7.500,00
Ukupno za partnera:		**7.500,00**	**0,00**				**Saldo**	**7.500,00**

Končar - Digital d.o.o. za digitalne usluge i rješenja
Fallerovo šetalište 22, 10000 Zagreb
Tel: +381 1 3667 177
NKD: 7112
OIB: 55191916939
IBAN: HR6423600001102948970

Kupac:	STUDENAC d.o.o.	OIB:	02023029348
	STUDENAC d.o.o.	MBr:	
Adresa	Četvrt Ribnjak 17		
	21310 Omiš	Šifra:	0679
	Hrvatska	Fax:	
		Tel:	
		E-mail:	
		IBAN:	HR9023600001502766885

Predmet: Izvod otvorenih stavaka kupca

Poštovani,

Pregledavajući naše knjige na dan 30.9.2026. god. ustanovili smo da nam dugujete:

Rbr	Broj dokumenta	Dat. dok.	Dat. dosp.	Eksterni broj	Duguje	Potražuje	Saldo	Orig. Dug.	Orig. Pot.
1	41 2600529-41-1	31.08.26	30.09.26		3.750,00	0,00	3.750,00	3.750,00	0,00
2	41 2600622-41-1	29.09.26	30.10.26		3.625,00	0,00	7.375,00	3.625,00	0,00
3	41 2600623-41-1	30.09.26	30.10.26		125,00	0,00	7.500,00	125,00	0,00
		Ukupno za partnera:		EUR	7.500,00	0,00	7.500,00		

Prema našim poslovnim knjigama, dajemo vam specifikaciju i stanje otvorenih stavaka. Molimo da nam vratite jedan primjerak ovjerenog i usaglašenog izvoda u sljedećih 8 dana.
Ako u navedenom razdoblju ne dobijemo odgovor, smatramo da ste suglasni s našim stanjem.

M.P.

S poštovanjem,

KONČAR
KONČAR Digital d.o.o.
Fallerovo šetalište 22, 10000 Zagreb
12.10.2026

Potvrđujemo IOS

M.P.

Ovlaštena osoba

Osporavamo IOS iz sljedećih razloga:

Kristina Blažević

From: Kristina Blažević
Sent: 19. listopada 2026. 14:15
To: usklada.salda@studenac.hr; ivana.ilijas@studenac.hr
Subject: IOS
Attachments: 2098_261013091700_001.pdf

Poštovani,

Ljubazno molim da nam ovjerite IOS u prilogu.

Zahvaljujem!

From: Kristina Blažević
Sent: Tuesday, October 13, 2026 9:25 AM
To: 'usklada.salda@studenac.hr' <usklada.salda@studenac.hr>; ivana.ilijas@studenac.hr
Subject: IOS

Poštovani,

Ljubazno molim da nam ovjerite IOS u prilogu.

Zahvaljujem!

Kristina Blažević

KONČAR
DIGITAL

Financije i računovodstvo

KONČAR DIGITAL d.o.o. • Fallerovo šetalište 22, 10000 Zagreb, Hrvatska

• e-mail: kristina.blazevic@koncar.hr • mob: +385 95 356 5695 • www.koncar.hr

KONČAR - Digital d.o.o., Fallerovo šetalište 22, Zagreb, OIB: 55191916939, kojeg zastupa Stjepan Sučić, direktor (dalje u tekstu: Izvršitelj)

i

Studenac d.o.o., Četvrt Ribnjak 17, Omiš, OIB: 02023029348, kojeg zastupaju Michał Wojciech Seńczuk, predsjednik Uprave i Michał Andrzej Halwa, član uprave, (dalje u tekstu: Naručitelj)

sklapaju sljedeći:

UGOVOR O PRUŽANJU USLUGA SIGURNOSNOG OPERACIJSKOG CENTRA

Članak 1.

Predmet Ugovora

Stavak 1.

Ovaj Ugovor o pružanju usluga Sigurnosnog Operativnog Centra dalje u tekstu: Ugovor) sklapa se na temelju prihvaćene Ponude Izvršitelja broj: 00002 od dana 24.9.2025. o Nabavi usluge Sigurnosnog Operativnog Centra, a koja Ponuda je sadržana u Prilogu 1 i čini sastavni dio ovog Ugovora.

Ugovorne strane sporazumno utvrđuju da je predmet ovog Ugovora nabava usluge uspostave Sigurnosnog Operativnog Centra (u daljnjem tekstu: SOC) informacijskog sustava za Naručitelja sukladno prihvaćenoj Ponudi Izvršitelja, a obuhvaća:

TEHNOLOGIJE:

SIEM - Security Information and Event Management (SIEM) rješenja za prikupljanje, normalizaciju i automatiziranu analizu sigurnosnih događaja i zapisa sa različitih uređaja u stvarnom vremenu.

SOAR - Security Orchestration, Automation and Response alata koji SOC timu omogućuje ručno ili automatizirano otvaranje sigurnosnog incidenta, automatsko ili ručno prikupljanje kontekstualnih informacija iz SIEM-a i ostalih kontrola. Sa SOAR-om je integriran sustav dojave o prijetnjama i dodatna programska podrška za automatizaciju odgovora na prijetnje.

Threat intelligence - proces koji predstavlja prikupljanje i analiziranje podataka i informacija o napadačkim aktivnostima kako bi se uz njihovu pomoć proaktivno unaprijedila zaštita sustava. Podaci koji se prikupljaju vezani su za potencijalne ili trenutne kibernetičke prijetnje, a obuhvaćaju: pokazatelje kompromitacije (engl. indicators of compromise – IOC), podatke o zlonamjernim IP adresama, domenama, URL-ovim, tehnikama, taktikama i procedurama napada i sl.

NDR - Network Detection and Response, rješenje koje omogućava organizacijama da identificiraju, analiziraju i odgovore na sofisticirane prijetnje unutar mrežnog okruženja. Platforma koristi napredne tehnologije poput umjetne inteligencije i strojnog učenja kako bi pružila potpunu vidljivost mrežnog prometa i automatski detektirala abnormalnosti, maliciozne aktivnosti i sigurnosne incidente.

EDR - Endpoint Detection and Response, rješenje pruža naprednu zaštitu krajnjih točaka kombiniranjem više slojeva sigurnosti za sprječavanje i otkrivanje prijetnji u stvarnom vremenu. Korištenjem automatizirane prevencije, analize ponašanja i detekcije anomalija, učinkovito zaustavlja ransomware, fileless napade, krađu vjerodajnica i zero-day eksploatacije. Omogućuje potpunu vidljivost aktivnosti na uređajima te brzu reakciju i izolaciju kompromitiranih sustava radi smanjenja rizika i zadržavanja poslovne kontinuiteta.

ZTNA - rješenje (Zero Trust Network Access) omogućuje siguran, kontroliran i precizno definiran pristup internim aplikacijama i resursima bez potrebe za tradicionalnim VPN-om. Temelji se na načelu "nikad ne vjeruj, uvijek provjeri", čime se autentikacija i autorizacija provode kontinuirano, neovisno o lokaciji korisnika ili uređaja. Sustav omogućuje granularnu kontrolu pristupa prema identitetu korisnika, stanju uređaja i kontekstu sesije, čime se značajno smanjuje rizik od neovlaštenog pristupa i lateralnog kretanja prijetnji unutar mreže. ZTNA rješenje time osigurava visoku razinu sigurnosti i pouzdanosti u hibridnim i distribuiranim IT okruženjima.

USLUGE:

Sigurnosni analitičari razine 1 - analiza najnovijih upozorenja kako bi se utvrdila relevantnost i hitnost, eskalaciju sigurnosnih upozorenja, procjena lažno pozitivnih dojava, prikupljanje kontekstualnih podataka, klasifikacija prijetnji, početna trijažu i određivanje prioriteta.

Sigurnosni analitičari razine 2 - izvršavanje duboke analize incidenata povezujući podatke iz različitih izvora, utvrđivanje da li je i koji kritični sustav ili skup podataka zahvaćen, savjetovanje o sanaciji te pružanje podrške za nove analitičke metode za otkrivanje prijetnji.

Sigurnosni analitičari razine 3 – koji djeluju kao lovci na prijetnje ne čekajući na eskalirane incidente, te su usko uključeni u razvoj, ugađanje i primjenu analize otkrivanja prijetnji.

Voditelj SOC-a - upravljanje resursima koji uključuju osoblje, proračun i strategiju tehnologije kako bi se zadovoljili taktički i strateški ciljevi, komunikacija s kontakt osobom klijenta. Pored toga, voditelj SOC-a je organizacijska kontakt osoba za poslovno-kritične incidente, te daje smjer za daljnju sigurnosnu strategiju.

Stavak 2.

Izvršitelj se obvezuje da će Uslugu iz Članka 1., Stavka 1. ovog Ugovora pružati Naručitelju u skladu s odredbama ovog Ugovora, a osobito u rokovima i količinama specificiranim u Ponudi, osim ako nije drugačije uređeno posebnim odredbama ovog Ugovora ili eventualnim pisanim aneksima i izmjenama dogovorenim između ugovornih strana.

Članak 2.

Odgovorna osoba od strane Naručitelja

Ugovorne strane su suglasne da će odgovorna osoba Naručitelja biti Direktor IT-a, čiji će direktni kontakt biti naveden u operativnim procedurama i eskalacijskim mehanizmima koji će biti uspostavljeni između Naručitelja i Izvršitelja.

Članak 3.

Vrijednost Ugovora i Način Plaćanja

Jedinične cijene Usluga specificirane su u Troškovniku sadržanom u Prilogu 2 ovog Ugovora koji čini njegov sastavni dio i nepromjenjive su za cijelo vrijeme trajanja ovog Ugovora. Jedinične cijene Usluga uključuju sve troškove pružanja usluga i popuste, te ne sadrže PDV. Sve cijene iskazane su u EUR, a plaćanje će biti izvršeno također u EUR na račun Raiffeisen banke d.d.:

IBAN: HR4424840081135357397

Naručitelj će plaćanja obavljati na temelju ispostavljenih računa, koje će Izvršitelj izdavati sukladno pruženim uslugama, a prema jediničnim cijenama iz ugovornog Troškovnika. Naručitelj je dužan ispravan račun platiti u roku od 30 (trideset) dana od dana primitka računa. Uz račun, Izvršitelj je obvezan priložiti specifikaciju izvršenih usluga, ovjerenu od strane predstavnika Naručitelja.

Račun mora biti dostavljen Naručitelju u roku od 3 (tri) dana od dana izdavanja. U slučaju da račun nije ispravan, Naručitelj će vratiti izvornik Izvršitelju na ispravak, a Izvršitelj je obvezan ispravan račun dostaviti Naručitelju u roku od 3 (tri) dana.

Ugovorne strane suglasno utvrđuju da će Izvršitelj, po dovršetku uspostave sustava i svih aktivnosti obuhvaćenih ponudom koje se naplaćuju jednokratno (uključujući uspostavu i inicijalizaciju sustava, Symantec licence za ZTNA i EDR rješenje), a što će biti potvrđeno potpisanim primopredajnim zapisnikom, ispostaviti Naručitelju račun na ukupni iznos od **48.490,00 EUR bez PDV-a** (slovima: četrdeset osam tisuća četiristo devedeset eura).

Izvršitelj će s naplatom mjesečnih naknada za pružanje SOC usluga započeti tek nakon potpisivanja primopredajnog zapisnika, kojim se potvrđuje uspostava i ispravno funkcioniranje inicijalnog sustava. Mjesečna naknada za pružanje SOC usluga iznosi **3.000,00 EUR bez PDV-a** (slovima: **tri tisuće eura**) mjesečno za maksimalni broj nadziranih uređaja, te će se obračunavati i naplaćivati sukladno stvarnom broju nadziranih radnih stanica i poslužitelja, a u skladu s cijenama, količinama i ostalim uvjetima navedenim u ponudi.

Ugovorne strane nadalje suglasno potvrđuju da će se kontinuirano pratiti stvarni broj radnih stanica i poslužitelja (servera) u uporabi kod Naručitelja, pri čemu maksimalni broj nadziranih uređaja može iznositi **1.000 (tisuću)** komada mjesečno za spomenutu cijenu od 3000 EUR bez PDV-a iz prethodnog paragrafa.

Članak 4.

Obveze Naručitelja

Naručitelj je obvezan surađivati s Pružateljem usluga u obavljanju njegovih obveza u opsegu i na način prilagođen svakoj konkretnoj aktivnosti, putem odgovarajućih uputa te omogućavanjem pristupa dostupnim podacima, osim u dijelu koji je u potpunosti pod nadležnošću Pružatelja usluga.

Naručitelj se obvezuje staviti na raspolaganje svoje resurse i informacije potrebne Izvršitelju za ispunjavanje ugovornih obveza te dostaviti točnu, jasnu, specificiranu i vjerodostojnu dokumentaciju (uključujući podatke, opise procesa, pravila i naputke) nužnu za izvršavanje Ugovora. Također, Naručitelj se obvezuje da neće dopustiti trećoj strani obavljanje aktivnosti iz Ugovora bez prethodnog dogovora. U slučaju uključivanja trećih osoba u izvršenje

ugovornih aktivnosti, Izvršitelj neće biti odgovoran za moguće kašnjenja i nepravilnosti u pružanju usluga.

Naručitelj se posebno obvezuje obavijestiti Izvršitelja o svakoj promjeni u njegovim IT sustavima koja može utjecati na izvršenje ugovorenih poslova. U slučaju nepravovremene obavijesti, Izvršitelj se neće smatrati odgovornim za bilo kakvu štetu koja bi mogla nastati kao posljedica takvog propusta Naručitelja.

Članak 5.

Obveze Izvršitelja

Izvršitelj je obvezan, prilikom izvršavanja Ugovora, u cijelosti uvažavati stajališta odgovorne osobe Naručitelja te bez njezine prethodne suglasnosti ne smije uvoditi nikakve promjene u vezi s razinom kvalitete, načinom pružanja ili količinom Usluga, niti odstupati od standarda, normi i pravila struke.

Izvršitelj je obvezan izvršavati sve svoje obveze u skladu s Tehničkim specifikacijama i rokovima odaziva, kako je navedeno i precizirano u prihvaćenoj Ponudi Izvršitelja:

Prioritet	Utjecaj na raspoloživost, integritet ili povjerljivost informacijskog sustava i poslovnih procesa	Odziv u satima	Rok za rješavanje
P1	ozbiljno narušeno	2 h	8 h
P2	bitno smanjeno	4 h	12 h
P3	otežano	8 h	16 h
P4	odstupa od specifikacije	16 h	32 h

U slučaju bilo kakvih nedostataka u vezi s pruženim Uslugama koje su predmet ovog Ugovora, Izvršitelj je dužan, o svom trošku, odmah, a najkasnije u roku određenom u pisanom nalogu Naručitelja, pristupiti otklanjanju istih prema primjedbama i uputama Naručitelja. Ukoliko Izvršitelj ne pristupi otklanjanju nedostataka u zadanom roku, Naručitelj zadržava pravo raskinuti Ugovor.

Izvršitelj je odgovoran za pružanje usluga sukladno uvjetima iz ponude, primjenjujući profesionalne standarde i najbolje prakse. Odgovornost Izvršitelja ograničena je na tehnologije i usluge pod njegovom izravnom kontrolom te je isključen od odgovornosti za štete koje proizlaze iz postupanja ili propusta Naručitelja, uključujući:

- **Neimplementacija preporuka:** Ako Naručitelj ne postupi prema preporukama i upozorenjima Izvršitelja vezanim uz detektirane incidente ili rizike, Izvršitelj ne odgovara za nastale štete.

- **Incidenti povezani s tehnologijama trećih strana:** Izvršitelj ne snosi odgovornost za incidente ili kvarove koji su rezultat problema u sustavima, softverima, mrežama ili alatima drugih proizvođača, koji nisu pod kontrolom Izvršitelja.

- **Nedostupnost Korisnika:** Ako Naručitelj ne odgovori pravovremeno na prijavu incidenta ili ne osigura pristup sustavima, Izvršitelj nije odgovoran za kašnjenja u rješavanju problema i posljedice koje iz toga proizlaze. Rješavanje takvih problema odgađa se do trenutka kada je osigurana odgovarajuća koordinacija.

Odgovornost Izvršitelja za štetu, bilo izravnu ili neizravnu, ograničena je na štete proizašle iz njegovog izravnog propusta, uz isključenje odgovornosti za štete uzrokovane nemarom ili nepažnjom Naručitelja, ili ne postupanjem prema preporukama iz dostavljenih izvještaja. Izvršitelj nije odgovoran za posljedice, neizravne i posredne štete, osim ako su one nastale zbog namjernog ili grubo nepažljivog postupanja Izvršitelja (nemar/krivnja).

Članak 6.

Rokovi Pružanja Usluga i Sankcije za Kašnjenje

Ugovorne strane suglasne su da će, u slučaju odstupanja od rokova pružanja Usluga iz ovog Ugovora zbog razloga na strani Izvršitelja, Naručitelj pozvati Izvršitelja da obvezu ispuni u primjerenom roku koji ne može biti dulji od 15 (petnaest) kalendarskih dana. Ukoliko Izvršitelj ni u tom roku ne ispuni obvezu, Naručitelj zadržava pravo odbiti prihvaćanje izvršenih Usluga te neće biti u obvezi izvršiti bilo kakvo plaćanje prema Izvršitelju.

Članak 7.

Trajanje i raskid Ugovora

Ugovor se sklapa na neodređeno vrijeme, i stupa na snagu danom potpisivanja. Svaka ugovorna strana ovlaštena je redovno bez ikakvog razloga, otkazati Ugovor pisanim putem uz otkazni rok od 60 (šezdeset) dana. Ukoliko Izvršitelj propusti ispuniti obveze iz ovog Ugovora, predstavnik Naručitelja može putem pisane obavijesti zatražiti od Izvršitelja da ispuni obvezu u odgovarajućem roku.

Naručitelj ima pravo raskinuti Ugovor u sljedećim slučajevima:

- ako Izvršitelj ne postupi prema obavijesti za ispunjenje obveze sukladno prethodnom stavku,
- ako Izvršitelj prepusti podizvršitelju pružanje pojedinih usluga bez prethodne suglasnosti Naručitelja,
- ako Izvršitelj postane nesolventan, ode u stečaj ili,
- ako Izvršitelj ne ispuni druge obveze iz ovog Ugovora, a za koje je kao sankcija predviđen raskid Ugovora prema ovom Ugovoru ili zakonu.

Naručitelj može raskinuti Ugovor putem pisane obavijesti Izvršitelju. U slučaju raskida Ugovora zbog štete koju je uzrokovao Izvršitelj, Naručitelj će platiti Izvršitelju samo za usluge koje su pružene do datuma raskida, umanjeno za troškove i štetu koju je Naručitelj pretrpio zbog raskida Ugovora.

Izvršitelj ima pravo raskinuti ovaj Ugovor prije isteka roka na koji je Ugovor sklopljen u slučaju da Naručitelj ne ispunjava svoje ugovorne obveze te ne otkloni posljedice povrede u roku od 30 (trideset) kalendarskih dana od primitka pisanog upozorenja Izvršitelja. U slučaju neispunjenja, neurednog ispunjenja ili kršenja ugovornih obveza od strane Izvršitelja, Naručitelj zadržava i pravo na naknadu stvarno pretrpljene štete.

Posebno opravdani razlozi za raskid od strane Izvršitelja uključuju:

- kašnjenje plaćanja od strane Naručitelja,
- izmjene koje Naručitelj izvrši na svojim IT sustavima bez prethodnog obavještavanja Izvršitelja, a koje utječu na pružanje ugovorenih usluga.

Članak 8.

Profesionalnost i Etičnost Izvršitelja

Izvršitelj se obvezuje da će tijekom izvršenja ugovornih obveza djelovati profesionalno, neovisno, etički i s pažnjom dobrog stručnjaka. Izvršitelj jamči korektnost u postupku te izostanak bilo kakve zabranjene prakse. Također, Izvršitelj izražava suglasnost s provedbom revizije cijelog predmeta Ugovora od strane neovisnih stručnjaka te prihvaća punu odgovornost i sankcije, uključujući bezuvjetan otkaz Ugovora, u slučaju kršenja bilo koje odredbe Ugovora.

Članak 9.

Viša Sila

„Viša sila" podrazumijeva događaj ili okolnost koja nastaje nakon sklapanja Ugovora, a koju ugovorna strana nije mogla predvidjeti niti otkloniti, niti na nju utjecati, te koja nije posljedica pogreške i/ili nemara strane pogođene „višom silom".

Naručitelj nema pravo naplatiti kaznu niti raskinuti Ugovor zbog neizvršavanja i/ili neurednog izvršavanja ugovornih obveza od strane Izvršitelja, ako je i u onoj mjeri u kojoj je neizvršavanje i/ili neuredno izvršavanje obveza posljedica djelovanja „više sile".

U slučaju nastupa „više sile", pogođena ugovorna strana obvezna je odmah pisanim putem obavijestiti drugu stranu o nastupanju „više sile", inače se pravo na pozivanje na „višu silu" neće priznati.

Nastup „više sile" ne oslobađa ugovornu stranu obveze, već odgađa njezino ispunjenje za vrijeme trajanja tih okolnosti.

Nakon što okolnosti „više sile" prestanu, ugovorna strana mora ispuniti svoju obvezu, ukoliko je to i dalje moguće.

Članak 10.

Povjerljivost Podataka

Izvršitelj se obvezuje čuvati kao poslovnu tajnu sve podatke koje dobije od Naručitelja ili trećih osoba po nalogu Naručitelja u vezi s ovim Ugovorom. Poslovnu tajnu predstavljaju i svi podaci koje pripremi Pružatelj usluga u svrhu ispunjenja ovog Ugovora.

Svi podaci i dokumenti koje dostavi Naručitelj vlasništvo su Naručitelja, te ih Izvršitelj ne smije koristiti, objaviti niti proslijediti na bilo koji način izvan okvira ovog Ugovora bez prethodnog pisanog odobrenja Naručitelja.

Osim osobama koje su angažirane na realizaciji Ugovora, Izvršitelju nije dozvoljeno obznaniti Ugovor, njegove odredbe, tehničke uvjete ili bilo koji njegov dio trećim osobama bez prethodnog pisanog pristanka Naručitelja.

U slučaju nepridržavanja obveza čuvanja tajnosti podataka od strane Izvršitelja ili njegovih zaposlenika, Naručitelj ima pravo na naknadu štete koju je pretrpio, kao i na sve koristi koje je Izvršitelj ostvario za sebe ili treću stranu.

U slučaju kršenja obveza čuvanja tajnosti podataka od strane Izvršitelja, Naručitelj zadržava pravo raskinuti Ugovor, neovisno o tome je li pretrpio štetu.

Obveza čuvanja povjerljivih podataka traje i nakon prestanka Ugovora, najmanje tri (3) godine.

Izvršitelj se obvezuje postupati u skladu s GDPR-om (EU 2016/679) i Zakonom o zaštiti osobnih podataka u dijelu u kojem obrađuje osobne podatke Naručitelja.

Članak 11.

Mirno Rješavanje Sporova

Sve eventualne sporove nastale na temelju ili u vezi s ovim Ugovorom, Naručitelj i Izvršitelj će nastojati riješiti mirnim putem, u dobroj vjeri i kroz međusobne pregovore.

Ukoliko nije moguće postići mirno rješenje spora, ugovara se nadležnost stvarno nadležnog suda prema sjedištu Naručitelja.

Članak 12.

Odgovorne Osobe za Realizaciju Ugovora

Odgovorna osoba Naručitelja za realizaciju Ugovora je:

Kontakt osoba: Marko Kralj

e-mail adresa: marko.kralj@studenac.hr

Mob: +385 91 639 4279

Odgovorna osoba Izvršitelja za realizaciju Ugovora je:

Kontakt osoba: Sanja Carević Višnjić

e-mail adresa: sanja.carevic@koncar.hr

Mob: +385 99 6041730

Za prijavu sigurnosnih evenata od strane Naručitelja, kao i probleme u radu sa IT sustavima koji su predmet ovog ugovora, koristiti će se IT Service Management sustav Naručitelja (Jira SM) te slati notifikacije prema Izvršitelju. Detalji će biti opisani u operativnoj proceduri.

Članak 13.

Suradnja i Dobra Vjera

Ugovorne strane će u izvršavanju ovog Ugovora međusobno surađivati u dobroj vjeri te se obvezuju potpisati sve potrebne isprave, dati sva očitovanja i poduzeti sve druge radnje potrebne za izvršavanje Ugovora.

Ako bi pojedine odredbe Ugovora iz bilo kojeg razloga bile ili postale ništetne, pobojne ili na bilo koji način nevaljane, to neće utjecati na valjanost ostalih odredbi Ugovora niti na valjanost Ugovora u cjelini. U tom slučaju, nedopuštena ili nevaljana odredba automatski će se smatrati zamijenjenom dopuštenom odredbom koja po svojoj svrsi i sadržaju najviše odgovara poslovnoj svrsi nedopuštene ili nevaljane odredbe.

Članak 14.

Primjena Zakona

Ugovorne strane suglasne su da će se na sva pitanja koja nisu posebno uređena odredbama ovog Ugovora primjenjivati važeći Zakon o javnoj nabavi, Zakon o obveznim odnosima Republike Hrvatske te ostali relevantni propisi koji uređuju predmetno područje.

Ovaj Ugovor stupa na snagu nakon što ga potpišu obje ugovorne strane, s datumom posljednjeg potpisa.

Ugovor je sastavljen u 2 (dva) istovjetna primjerka, od kojih svaka strana zadržava 1 (jedan) primjerak.

Datum: 01.12.2025

Za Izvršitelja:

Stjepan Sučić, direktor

Potpis: _____

KONČAR
DIGITAL
KONČAR - Digital d.o.o.
Fallerovo šetalište 22, 10000 Zagreb

Za Naručitelja:

Michał Wojciech Seńczuk,
predsjednik uprave

Potpis: _____

STUDENAC
Studenac d.o.o.
Cerovi Ribnjak 27
21310 Omiš

Michał Andrzej Halwa, član uprave

Potpis: _____

Dokument: Opis SOC usluge

Napredni sigurnosno operativni centar
Ponuda br. 00002

Rujan, 2025.

SADRŽAJ

Podaci o dokumentu	***3***
Uvod	***4***
Zaposlenici	***5***
procesi i faze upravljanja incidentima	***6***
Tehnologije i Funkcionalnosti	***8***
Specifikacija ponuđenog rješenja	***12***
Usluga nadzora i odgovora na incidente	*12*
Opseg nadzora	*12*
Primjeri detekcijskih pravila	*13*
Arhitektura sustava	*20*
Plan implementacije i početka pružanja usluge	*20*
Uloge i odgovornosti	*20*
Preduvjeti	*21*
SLA	*22*
Izvještavanje	*22*
Cijene i komercijalni uvjeti	***24***
Isporuka usluga	*26*
Valjanost ponude	*26*
Trajanje Ugovorne obaveze	*26*
Dodatne informacije	*26*

PODACI O DOKUMENTU

Ponuda ili pojedini dijelovi ponude sadrže povjerljive podatke ponuđača Končar - Digital d.o.o. Opis usluge i sadržaj ovog dokumenta namijenjeni su isključivo ovlaštenim zaposlenima klijenta Studenca ili njegovim stručnim savjetnicima, ali samo u svrhu ocjene ove ponude te pod uvjetom da su upoznati i vezani povjerljivošću ponude i njenog sadržaja. Podaci sadržani u ovom dokumentu, prilozi i sve poruke povezane s njom, ne smiju se otkrivati, kopirati, koristiti u cijelosti ili djelomično, u bilo koju drugu svrhu osim za procjenu i realizaciju usluge.
Ova ponuda u vlasništvu je ponuđača. Zaštita poslovne tajne biti će preciznije definirana ugovorom. U slučaju da klijent ne odluči realizirati ponudu, i dalje je dužan čuvati povjerljivost podataka sadržanih u ovom dokumentu.
Ponuda podliježe standardnim uvjetima pružatelja usluga.
Zbog važnosti procesa koji se obrađuju i informacija koje ti procesi stvaraju i obrađuju, posebno je važna zaštita osobnih podataka, što će biti ugovorom definirano prije početka projekta.

Rev.br.	Datum izrade	Autor	Opis izmjene
1.0	26.05.2025.	Mario Jurčević	Osnovni tekst

Pregledao i odobrio dokument

Pregledano	Funkcija
Stjepan Sučić	Direktor, Končar - Digital d.o.o.

Distribucija dokumenta

Osoba	Funkcija
Marko Kralj	IT Direktor
Ivica Benutić	Voditelj odjela IT Infrastruktura
Matko Novaković	Viši specijalist opće nabave

UVOD

Sigurnost informacija i zaštita podataka ključni su aspekti poslovanja svake organizacije. Porastom sofisticiranosti kibernetičkih napada, organizacije se suočavaju s izazovima u održavanju sigurnosti IT okruženja. Upravo zbog toga, učinkovita zaštita zahtijeva neprestano praćenje, analizu i reakciju na sigurnosne incidente. Security Operation Center (SOC) usluge predstavljaju srž tih napora, pružajući centralizirano mjesto za nadzor i upravljanje sigurnosnim prijetnjama u stvarnom vremenu.

Naša ponuda SOC usluga osmišljena je kako bi vašoj organizaciji omogućila robustan i sveobuhvatan pristup sigurnosnom upravljanju. Kroz implementaciju naprednih tehnologija, stručnost naših timova i proaktivni pristup, osiguravamo kontinuiranu zaštitu vaših digitalnih resursa. U ovom dokumentu predstavljamo detalje naših SOC usluga, uključujući ključne funkcionalnosti, prednosti te način implementacije i podrške.

Končar - Digital SOC:

24x7 Praćenje i nadzor: Naš SOC tim neprestano prati sigurnosne događaje kako bi osigurao brzu identifikaciju i odgovor na potencijalne prijetnje.

Proaktivna zaštita: Naš proaktivni pristup omogućuje prepoznavanje prijetnji prije nego što mogu prouzročiti štetu.

Napredna analitika i detekcija prijetnji: Korištenjem najmodernijih alata i tehnologija, omogućujemo prepoznavanje i analizu kompleksnih napada.

Odgovor na incidente: Brzo i učinkovito reagiramo na sigurnosne incidente, minimizirajući potencijalne štete i osiguravajući kontinuitet poslovanja.

Izvještavanje i Usklađenost: Pripremamo detaljne izvještaje koji pomažu vašoj organizaciji u održavanju usklađenosti s relevantnim standardima i propisima.

Ekspertni pristup: Naši stručnjaci posjeduju bogato iskustvo i znanje u području kibernetičke sigurnosti, osiguravajući najbolju moguću zaštitu za vašu organizaciju.

Skalabilnost: Naše usluge mogu se prilagoditi potrebama vaše organizacije, bez obzira na njezinu veličinu i kompleksnost IT okruženja.

Smanjenje troškova: Ulaganjem u SOC usluge smanjujete potrebu za velikim internim resursima i specijaliziranim alatima.

Proces implementacije SOC usluga uključuje temeljitu procjenu trenutnog stanja IT sigurnosti, definiranje specifičnih potreba i ciljeva te prilagodbu naših rješenja kako bi najbolje odgovarala poslovnim zahtjevima. Uz kontinuiranu podršku i redovite procjene sigurnosnog stanja, osiguravamo da organizacija ostane zaštićena od svih vrsta kibernetičkih prijetnji.

U nastavku ovog dokumenta detaljnije ćemo opisati svaki aspekt naših SOC usluga, uključujući tehničke specifikacije, korake koje poduzimamo kako bismo osigurali najvišu razinu zaštite. Nadamo se da ćete prepoznati vrijednost i važnost SOC usluga te da ćemo imati priliku surađivati na poboljšanju sigurnosnog okruženja vaše organizacije.

ZAPOSLENICI

Uloga	Opis	Vještine	Odgovornosti
 **Razina 1** Sigurnosni analitičari	Specijalisti za trijažu	Vještine analize sigurnosno relevantnih događanja. Poznavanje rada operacijskih sustava i računalnih mreža, poznavanje sigurnosnih koncepata	Analiza najnovijih upozorenja kako bi se utvrdila relevantnost i hitnost, eskalaciju sigurnosnih upozorenja, procjena lažno pozitivnih dojava, prikupljanje kontekstualnih podataka, klasifikacija prijetnji, početna trijažu i određivanje prioriteta. Sigurnosni analitičari prve razine aktivno prate i doprinose svojim prijedlozima poboljšavanju studija slučajeva na SIEM alatu, postupaka odgovora i finom podešavanju automatizacije odgovora, rješavanjem incidenata ili eskalacijom na analitičare druge razine.
 **Razina 2** Sigurnosni analitičari	Specijalisti za odgovore na incidente	Sve vještine analitičara prve razine te naprednije vještine analize sigurnosnih događaja. Vještine forenzičke istrage i odgovora na sigurnosne incident	Upravljanje sigurnosnim upozorenjima zaprimljenih eskalacijom od analitičara prve razine te provođenje analize temeljnog uzroka sigurnosnog incidenta. Prikupljanje dodatnih kontekstualnih informacija za tehničku analizu sa ciljem utvrđivanja osnovnog uzroka sigurnosnog upozorenja. Utvrđivanje metoda napada, identifikacija napadača, cilja i svrhe napada. Ažuriranje klasifikacije događaja, važnosti, pomoć pri forenzičkoj analizi i određivanje sljedećih koraka.
 **Razina 3** Sigurnosni eksperti – analitičari	Specijalisti za pronalazak prijetnji	Sve vještine analitičara druge razine te napredne vještine forenzičke istrage i pronalaska prijetnji.	Sigurnosni eksperti zaprimaju eskalirane sigurnosne incidente i analiziraju njihov utjecaj na poslovanje. Analitičari ove razine dodavaju kontekstualne informacije, provode dodatnu analizu i na temelju poslovnog učinka preporučuju odgovore i druge razine eskalacije. Ova funkcija također provodi akciju odgovora na incident, uključujući eskalaciju sigurnosnog incidenta na CSIRT (tim za odgovor na računalne sigurnosne incidente). Sigurnosni eksperti obavljaju ulogu pronalaska prijetnji (engl. Threat Hunt) i dodatno provjeravaju učinkovitost sigurnosnih kontrola i moguće tragove kompromitacije štićenog sustava.
 **Razina 4** Voditelj SOC-a	Vodstvo i upravljanje	Sve vještine analitičara treće razine te napredne komunikacijske i upravljačke vještine.	Voditelj SOC-a provodi nadzor rada i stalno poboljšavanje kvalitete usluge, brine o zaposlenicima i njihovom stalnom usavršavanju. Voditelj SOC-a je u stalnoj komunikaciji sa svim klijentima te zaposlenicima SOC-a prenosi sve relevantne poslovne zahtjeve.

PROCESI I FAZE UPRAVLJANJA INCIDENTIMA

Faza	Opis
Detekcija i procjena	**Zašto je ova faza važna?** Prva faza u obradi sigurnosnih incidenata gdje se na temelju prikupljenih informacija iz IT sustava korištenjem prethodno definiranih detekcijskih pravila analizira sigurnosna prijetnja. Ključni pokazatelji pronalaze se u zapisima dobivenim na temelju aktivnosti korisnika, procesa, sustava, prihvaćanja/odbijanja prometa na vatrozidima itd. Specifični nizovi i kombinacije događaja u određenim obrascima mogu signalizirati događaj koji kojeg je potrebno obraditi. Uspješnosti u ovoj fazi pridonosi brza klasifikacija događaja, kako bi se mogli odrediti prioriteti, a kritični događaji koji zahtijevaju dodatnu istragu eskalirati. **Što SOC analitičari rade u ovoj fazi?** • Definiranje i kontinuirano ažuriranje indikatora napada • Identifikacija vektora napada, alata i iskorištavanja ranjivosti • Identifikacija opsega indikatora napada • Procjena o potrebi pokretanja procesa i procedura za odgovor na incidente temeljem izvršene analize
Klasifikacija i izvještavanje	**Zašto je ova faza važna?** Cilj ove faze je evidentirati sve činjenice povezane sa incidentom te iste u jasnom obliku komunicirati prema svim potrebnim stranama **Što SOC analitičari rade u ovoj fazi?** • Analiza indikatora kako bi se utvrdila točnost upozorenja ili izvještaja • Dokumentiranje relevantnih vremena i ostalih činjenica vezanih uz poduzete aktivnosti • Dodjela prioriteta incidenta na osnovu procjene utjecaja incidenta • Izvještavanje svih potrebnih strana kako bi se poduzele potrebne radnje
Suzbijanje	**Zašto je ova faza važna?** Cilj ove faze je zaustavljanje napadača, izoliranje kompromitiranih dijelova sustava te, ukoliko je moguće, otkrivanje uzroka incidenta. Tehničke mjere u ovoj fazi provode osobe/timovi zaduženi za održavanje pojedinih sustava (najčešće timovi klijenta SOC usluge) uz prethodne konzultacije sa SOC analitičarima. **Što SOC analitičari rade u ovoj fazi?** • Definiranje opsega incidenta • Izolacija kompromitiranih dijelova sustava (npr. izolacija računala, zaključavanje korisničkih računa i sl.) • Otkrivanje uzroka incidenta • Savjetovanje klijenta SOC-a prilikom izvještavanja o incidentu nadležnom tijelu

Oporavak	**Zašto je ova faza važna?** Cilj ove faze je vratiti sustav u prvobitno stanje te podesiti dodatne sigurnosne kontrole kako se incident ne bi ponovio. **Što SOC analitičari rade u ovoj fazi?** • Onemogućavanje pristupa sustavima napadaču • Povratak sustava u pred-incidentno stanje (npr. povratak datoteka iz pričuvnih kopija, promjena lozinki, ponovna instalacija radnih stanica/poslužitelja i sl.) zajedno sa timom klijenta SOC-a • Pružanje savjetodavnih usluga za implementaciju mjera za umanjivanje rizika (koje sprječavaju ponavljanje istog ili sličnog incidenta)
Aktivnosti nakon incidenta	**Zašto je ovaj proces važan?** Cilj ove faze je na temelju novih saznanja dobivenih u prethodnim fazama razmotriti sve aspekte (organizacijske, proceduralne, tehničke itd.) koji mogu rezultirati povećanjem razine sigurnosti. **Što SOC analitičari rade u ovoj fazi?** • Pružanje savjetodavnih usluga za implementaciju organizacijskih mjera (promjena politika i operativnih procedura vezanih na korištenje ICT sustava) • Pružanje savjetodavnih usluga za analizu i izradu plana povećanja otpornosti na kibernetičke napade • Pružanje savjetodavnih usluga za implementaciju tehničkih mjera (podešavanje i/ili integracija novih tehničkih elemenata zaštite)

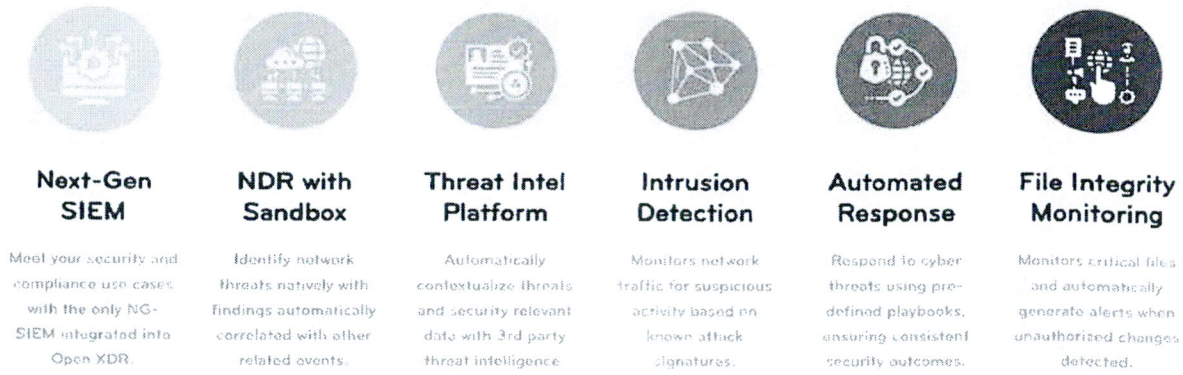
TEHNOLOGIJE I FUNKCIONALNOSTI

Tehnološko rješenje može biti ponuđeno kao SaaS platforma, virualna platforma na postojećoj virtualizacijskoj okolini (npr. VMWare) ili hardversko rješenje postavljeno u data centar (engl. appliance).

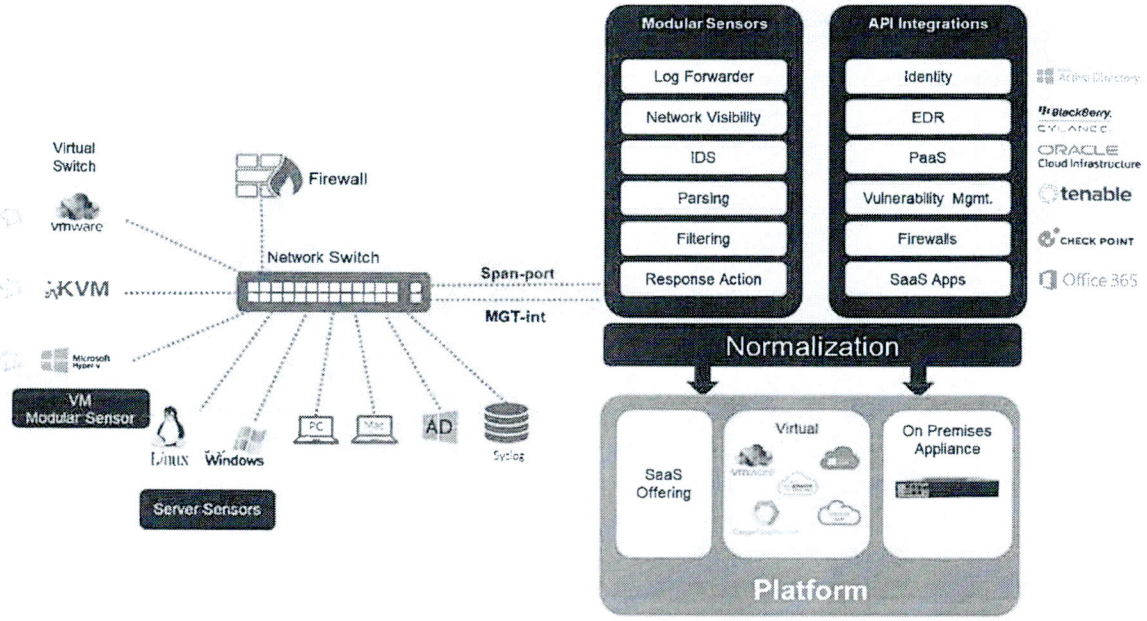
Alat	Opis
Endpoint Protection	Symantec Endpoint Detection and Response (EDR) omogućuje naprednu detekciju, analizu i odgovor na sigurnosne incidente koji nadilaze mogućnosti klasične antivirusne zaštite. Rješenje objedinjuje detaljnu endpoint telemetriju, analizu ponašanja i globalni threat intelligence kako bi se osigurala pravovremena identifikacija, učinkovita istraga i brza sanacija prijetnji poput ransomwarea, fileless napada, lateralnog kretanja i krađe vjerodajnica. **Advanced Threat Detection & Response** Rješenje kontinuirano prikuplja i analizira podatke s krajnjih uređaja, uključujući procese, mrežnu komunikaciju, registry i memoriju. Na temelju korelacije tih podataka identificira sumnjive obrasce ponašanja te omogućuje detekciju i odgovor na poznate i nepoznate prijetnje koje prolaze ispod razine klasične preventivne zaštite.. **Behavioral Analysis & Machine Learning** Analiza aktivnosti sustava u kombinaciji s modelima strojnog učenja omogućuje prepoznavanje odstupanja od uobičajenog rada aplikacija i operativnog sustava. Time se učinkovito otkrivaju napredne tehnike napada, uključujući eskalaciju privilegija, lateralno kretanje unutar mreže te komunikaciju s command-and-control infrastrukturom. **Anti-Ransomware Detection** Ransomware aktivnosti identificiraju se kroz prepoznatljive ponašajne indikatore, uključujući neuobičajene promjene i šifriranje datoteka. U slučaju detekcije, omogućeno je brzo ograničavanje incidenta kroz izolaciju endpointa i pokretanje odgovarajućih response aktivnosti. **Global Threat Intelligence** Symantec EDR koristi podatke iz Symantec Global Intelligence Network (GIN), globalnog sustava za prikupljanje i analizu prijetnji temeljenog na velikom broju endpoint, web i email senzora. Sigurnosni događaji automatski se obogaćuju reputacijskim podacima o IP adresama, domenama, URL-ovima i datotekama. **Incident Investigation & Root Cause Analysis** Rješenje omogućuje detaljnu istragu sigurnosnih incidenata kroz vremensku liniju događaja. Sigurnosni timovi dobivaju jasan uvid u početni vektor napada, korištene tehnike i opseg kompromitacije unutar okruženja. **Fileless Attack Detection** Posebna pažnja posvećena je detekciji napada bez upotrebe datoteka, uključujući zloupotrebu PowerShella, WMI-ja, legitimnih sistemskih alata (LOLBins) i napade u memoriji. Detekcija se temelji prvenstveno na analizi ponašanja i konteksta aktivnosti. **Endpoint Isolation & Remote Response**

	U slučaju sigurnosnog incidenta, administrator može udaljeno izolirati kompromitirani uređaj od mreže kako bi se spriječilo daljnje širenje prijetnje, uz zadržavanje potrebnog pristupa za forenzičku analizu i sanaciju. **Threat Hunting** Napredne threat hunting funkcionalnosti omogućuju proaktivno pretraživanje endpoint telemetrije koristeći indikatore kompromitacije i ponašajne obrasce, čime se povećava vjerojatnost ranog otkrivanja skrivenih ili dugotrajnih prijetnji. **Integration with Symantec Endpoint Security** Symantec EDR je u potpunosti integriran sa Symantec Endpoint Security platformom, što omogućuje centralizirano upravljanje, korelaciju podataka i jedinstven pogled na prevenciju, detekciju i odgovor na prijetnje. **MITRE ATT&CK Mapping** Svi relevantni sigurnosni događaji i detektirane aktivnosti mapiraju se na MITRE ATT&CK framework, što olakšava razumijevanje korištenih tehnika napada, standardizira analizu incidenata i ubrzava donošenje odluka tijekom incident response procesa.
Endpoint Detection and Response	**Automatic Remediation** Omogućuje provođenje automatskih i ručno pokrenutih mjera sanacije s ciljem brzog ograničavanja i uklanjanja prijetnji. Dostupne radnje uključuju zaustavljanje zlonamjernih procesa, uklanjanje datoteka, izolaciju kompromitiranih uređaja s mreže te onemogućavanje korisničkih aktivnosti. Sve sanacijske aktivnosti mogu se provoditi lokalno na endpointu ili centralizirano putem upravljačke konzole. **Automatic Forensic** Svaki sigurnosni incident automatski se analizira u stvarnom vremenu. Generira se forenzički pregled napada koji prikazuje tijek incidenta od početne kompromitacije do završnih aktivnosti, uz ključne informacije o procesima, korisniku i mrežnoj komunikaciji. **File & Process Events Monitoring & Logging** Kontinuirano bilježenje događaja vezanih uz procese i datoteke omogućuje detaljnu forenzičku analizu i pouzdanu rekonstrukciju sigurnosnih incidenata. **Endpoint Inventory & Status** Centralizirani pregled endpointa, instaliranih aplikacija i sigurnosnog statusa omogućuje brzo prepoznavanje rizičnih uređaja i zastarjelih aplikacija. **Network Threat Visibility** Vidljivost mrežne komunikacije endpointa omogućuje detekciju sumnjivih konekcija, lateralnog kretanja i neautoriziranih mrežnih aktivnosti. **Browser Security & Zero-Phishing** Kontinuirani nadzor i analiza web aktivnosti korisnika omogućuju prepoznavanje i blokiranje phishing napada te pokušaja krađe osjetljivih podataka, uključujući nove i prethodno nepoznate zlonamjerne web lokacije, u stvarnom vremenu.
SIEM	

	Security Information and Event Management (SIEM) je rješenje za prikupljanje, normalizaciju i automatiziranu analizu sigurnosnih događaja i zapisa sa različitih uređaja u stvarnom vremenu. Neke od funkcionalnosti SIEM-a su: • Prikupljanje podataka sa različitih izvora • Korelacija, ispitivanje i analiza poveznica i ovisnosti među događajima i incidentima • Brzo pretraživanje i analiza logova s naprednim upitima i filtriranjem • Upozoravanje, slanje automatskih upozorenja za potencijalno opasne događaje odmah nakon analize prikupljenih incidenata • Provjera usklađenosti sa definiram standardima upravljanja sigurnošću i zaštite informacija • Dugoročna pohrana sigurnosnih logova • Vizualizacija podataka i izvješća za lakše razumijevanje sigurnosnog stanja
SOAR	SOAR (engl. Security Orchestration, Automation and Response) je alat koji SOC timu omogućuje ručno ili automatizirano otvaranje sigurnosnog incidenta, automatsko ili ručno prikupljanje kontekstualnih informacija iz SIEM-a i ostalih kontrola. Sa SOAR-om je integriran sustav dojave o prijetnjama i dodatna programska podrška za automatizaciju odgovora na prijetnje. SOAR pruža podršku procesima za odgovor na pojedine vrste incidenta koja analitičarima olakšava sve korake obrade incidenta. Ovisno o podršci krajnjih uređaja SOC tim kroz SOAR može automatizirati ili ručno pokrenuti odgovor koji može zadržati i blokirati incident promjenama postavki krajnjih sustava kao što su vatrozidi i drugi sigurnosni sustavi.
Threat intelligence	Threat intelligence proces predstavlja prikupljanje i analiziranje podataka i informacija o napadačkim aktivnostima kako bi se uz njihovu pomoć proaktivno unaprijedila zaštita sustava. Podaci koji se prikupljaju vezani su za potencijalne ili trenutne kibernetičke prijetnje, a obuhvaćaju: pokazatelje kompromitacije (engl. indicators of compromise – IOC), podatke o zlonamjernim IP adresama, domenama, URL-ovim, tehnikama, taktikama i procedurama napada i sl.
Network Detection and Reponse	Network Detection and Reponse je tehnologija koja koristi napredne analitičke tehnike kako bi se sumnjive aktivnosti na mreži detektirale i spriječile.
Sandbox	Sandbox je izolirano i kontrolirano okruženje koje služi za sigurno testiranje potencijalno štetnog softvera ili koda. Sandbox omogućuje analizu sumnjivih datoteka bez rizika od zaraze ili oštećenja produkcijskih sustava.



Slika 1. Prikaz funkcionalnosti rješenja



Slika 2. Prikaz platforme i opcija za instalaciju

SPECIFIKACIJA PONUĐENOG RJEŠENJA

Končar – Digital SOC kao uslugu isporučuje upravljanu uslugu sigurnosnog operativnog centra (engl. Managed Security Operation Centre) i to uz oslanjanje na postojeće tehničke sustave klijenta, kao i koristeći vlastite dodatne tehničke sustave koje će instalirati kod klijenta i integrirati ih sa sustavima klijenta.

Končar – Digital SOC tim će navedene tehničke sustave instalirati na lokaciji klijenta, a upravljanje će obavljati obavljati na svojoj lokaciji VPN pristupom ili drugim pristupnim načinom koji će mu klijent otvoriti za tu namjenu.

Pružena usluga obuhvaća integraciju i korištenje EDR, NDR, SIEM i SOAR rješenja te procese proaktivnog provođenja sigurnosti opisane u prethodnim poglavljima ovog dokumenta. Detaljniji opis usluge i integracije nalazi se u nastavku ovog dokumenta.

Usluga nadzora i odgovora na incidente

Končar – Digital SOC za ponuđenu uslugu osigurava odgovarajuće tehničko osoblje koje će pružati tehničku podršku i postupanje sa sigurnosnim incidentima u slučaju incidenta ili sumnje u incident. Končar – Digital SOC za potrebe provođenja usluge osigurava odgovarajući broj tehničkog osoblja koje će biti na raspolaganju klijentu, i to:

- Sigurnosni analitičari razine 1 - analiza najnovijih upozorenja kako bi se utvrdila relevantnost i hitnost, eskalaciju sigurnosnih upozorenja, procjena lažno pozitivnih dojava, prikupljanje kontekstualnih podataka, klasifikacija prijetnji, početna trijažu i određivanje prioriteta.

- Sigurnosni analitičari razine 2 - izvršavanje duboke analize incidenata povezujući podatke iz različitih izvora, utvrđivanje da li je i koji kritični sustav ili skup podataka zahvaćen, savjetovanje o sanaciji te pružanje podrške za nove analitičke metode za otkrivanje prijetnji.

- Voditelj SOC-a - upravljanje resursima koji uključuju osoblje, proračun i strategiju tehnologije kako bi se zadovoljili taktički i strateški ciljevi, komunikacija s kontakt osobom klijenta. Pored toga, voditelj SOC-a je organizacijska kontakt osoba za poslovno-kritične incidente, te daje smjer za daljnju sigurnosnu strategiju.

- Sigurnosni analitičari razine 3 – koji djeluju kao lovci na prijetnje ne čekajući na eskalirane incidente, te su usko uključeni u razvoj, ugađanje i primjenu analize otkrivanja prijetnji.

Klijent SOC-a osigurava tehničko osoblje koje će koordinirati timovima klijenta i izvršavati zadatke prema matrici odgovornosti definiranoj u sljedećim poglavljima ovog dokumenta.

Opseg nadzora

Sigurnosni nadzor se provodi nad imovinom klijenta SOC-a integracijom prethodno opisanog rješenja, a najčešći izvori zapisa su:

1. Windows poslužitelji
2. Linux poslužitelji
3. Mrežni uređaji
   - Vatrozidi
   - Mrežni usmjeritelji
   - Kontroleri za bežične mreže

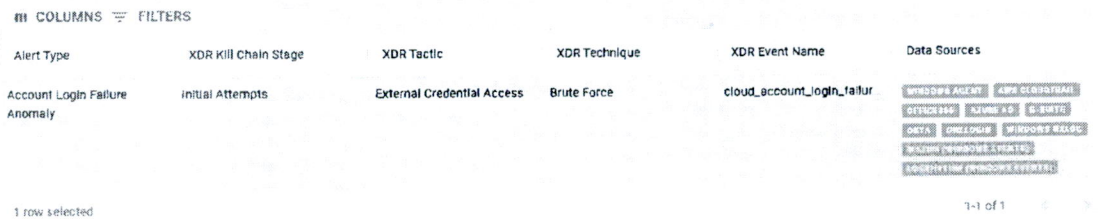
4. SaaS servisi kao što je Microsoft O365
5. Baze podataka
6. Web poslužitelji
7. Sigurnosni uređaji
   - Antivirus i EDR sustavi
   - IPS uređaji
   - Mail i web gateway uređaji
8. Sustavi za upravljanje servisima u oblaku
9. Aplikacije za podršku poslovnim procesima
10. IaaS, PaaS, SaaS sustavi

Primjeri detekcijskih pravila

Omogućavanje novih detekcijskih pravila kontinuirani je posao koji zahtjeva specifična znanja, a ovisi o identificiranim potencijalnim prijetnjama. U nastavku se nalaze primjeri često korištenih detekcijskih pravila. Napomena: kako bi dolje navedena detekcijska pravila bila funkcionalna klijent SOC-a mora osigurati da izvorišni sustavi šalju sve potrebne zapise.

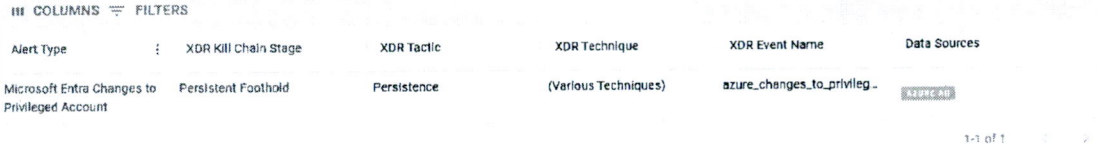
Neovlašteni pokušaji pristupa: pravila otkrivaju neuspjele pokušaje prijave, posebno kada dolazi do višestrukih uzastopnih neuspjeha. Ovo je često znak brute-force napada, gdje napadači koriste automatizirane metode za pogađanje lozinki. Pravila prate i zapise o neuspjelim prijavama kako bi se brzo identificirale potencijalne prijetnje.

Primjer:



Pokušaji eskalacije privilegija: otkriva pokušaje promjene privilegija korisnika, kao što su dodavanje korisnika u administrativne grupe ili promjene u korisničkim ulogama u cloud sustavima poput Active Directory-a, Azurea ili AWS-a. Eskalacija privilegija je čest korak u kibernetičkim napadima gdje napadači pokušavaju dobiti šire ovlasti na sustavu.

Primjer:



Zaključavanje računa: Detekcija zaključanih računa zbog ponavljanih neuspjelih prijava. Pravila automatski upozoravaju sigurnosne timove kada dođe do ovakvih incidenata, kako bi mogli odmah reagirati na potencijalne brute-force napade ili pokušaje neovlaštenih prijava.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Office 365 Blocked User	Initial Attempts	External XDR UBA	XDR Suspicious User	office365_blocked_user	

1-1 of 1

Modifikacija sigurnosnih grupa: Ova pravila prate promjene u članstvima sigurnosnih grupa, što može uključivati dodavanje ili uklanjanje korisnika iz privilegiranih grupa. Ovakve promjene mogu biti znakovi kompromitirane mreže ili unutarnjih prijetnji.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Sensitive Windows Active Directory Attribute Modification	Persistent Foothold	Defense Evasion	Domain Policy Modification	windows_security_ad_sens..	

1-1 of 1

Neobične lokacije prijave: Detekcija prijava s neuobičajenih geografskih lokacija pomaže identificirati moguće napade na korisničke račune, poput pokušaja kompromitiranja s udaljenih ili nepoznatih IP adresa

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
User Login Location Anomaly	Initial Attempts	External XDR NBA	XDR Location Anomaly	user_login_region	

1-1 of 1

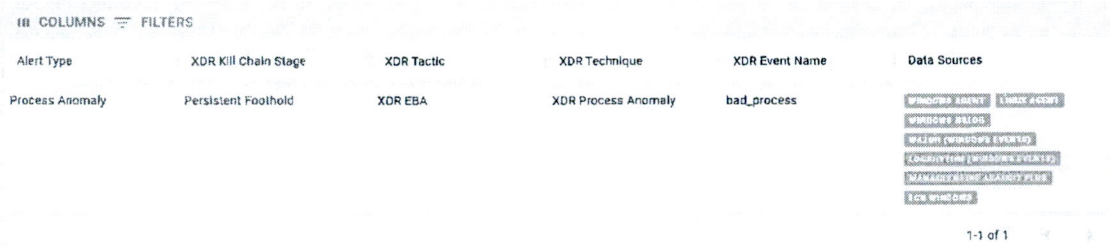
Otkrivanje zlonamjernog softvera: Pravila koja otkrivaju poznate potpise zlonamjernog softvera, kao što su procesi povezani s ransomwareom, virusima ili trojancima. Ova pravila omogućuju ranu detekciju zlonamjernih aktivnosti i sprječavaju širenje malware-a unutar mreže.

Primjer:



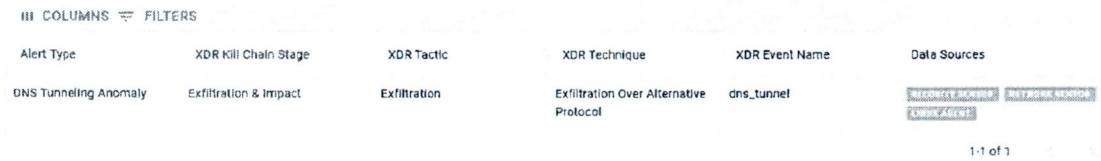
Sumnjiva aktivnost procesa: Otkrivanje neobičnih ili sumnjivih procesa, poput pokretanja neovlaštenih aplikacija ili skripti koje se obično koriste u napadima. Ova pravila pomažu identificirati alate za eksploataciju i druge maliciozne procese.

Primjer:



DNS anomalije: Pravila za praćenje neobičnih obrazaca DNS upita, koji mogu ukazivati na pokušaje DNS tuneliranja ili komunikacije s Command and Control (C2) poslužiteljima. Ove aktivnosti često prethode ili prate napade.

Primjer:



Anomalije e-pošte: Pravila koja otkrivaju sumnjive aktivnosti e-pošte, poput pokušaja phishinga, masovne distribucije zlonamjernih privitaka ili neuobičajenih poruka od legitimnih korisnika. Praćenje ovih aktivnosti ključno je za zaštitu korisnika od krađe identiteta.

Primjer:



Neobičan mrežni promet: Pravila za otkrivanje anomalija u mrežnom prometu, uključujući neuobičajeno velike količine podataka ili komunikaciju s nepoznatim ili sumnjivim IP adresama. Ovo može biti znak ransomware napada ili curenja podataka.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Suspicious Windows Network Connection	Persistent Foothold	Defense Evasion	(Various Techniques)	suspicious_windows_netw...	WINDOWS AGENT WINDOWS XDLOG

1-1 of 1

Skeniranje portova: Detekcija unutarnjih i vanjskih pokušaja skeniranja portova. Napadači često koriste skeniranje portova kako bi identificirali otvorene ili ranjive servise unutar mreže, što je često prvi korak u napadu.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Internal IP / Port Scan Anomaly	Exploration	Discovery	Network Service Scanning	internal_port_scan	NETWORK SENSOR LINUX AGENT WINDOWS AGENT NETFLOW CISCO ASA CISCO FIREPOWER CISCO VPN HILLSTONE JUNIPER SRX JUNIPER SRX SONICWALL FG SILVERLINE SANSFOR NGAF MERAKI

1-1 of 1

Neovlašteni pristup mreži: Praćenje pokušaja pristupa neovlaštenim mrežnim segmentima ili uređajima. Pravila upozoravaju na pokušaje povezivanja na osjetljive dijelove mreže ili segmente zaštićene višim razinama sigurnosti.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Sensitive Windows Network Share File or Folder Access	Propagation	Lateral Movement	Remote Services	windows_security_sensitiv	WINDOWS AGENT WINDOWS XDLOG

1-1 of 1

Promjene konfiguracije: Detekcija nenajavljenih ili sumnjivih promjena u konfiguracijama sustava ili aplikacija. Ove promjene mogu ukazivati na pokušaje kompromitiranja sustava ili unutarnje prijetnje.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Sensitive Windows Active Directory Attribute Modification	Persistent Foothold	Defense Evasion	Domain Policy Modification	windows_security_ad_sens...	WINDOWS AGENT WINDOWS XDLOG

1-1 of 1

Brute force napadi: Pravila koja otkrivaju brute-force napade na mehanizme autentifikacije, gdje napadači koriste automatizirane metode za pokušaj prijave s različitim lozinkama sve dok ne uspiju dobiti pristup.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
External Brute-Forced Successful User Login	Initial Attempts	External Credential Access	Brute Force	external_user_success_bru...	

1-1 of 1

Skeniranje ranjivosti: Detekcija iskorištenih ranjivosti od strane napadača uz pomoć integracije s alatima za upravljanje ranjivostima.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Internal Exploited Vulnerability	Exploration	Internal XDR NBA	XDR Exploitated Vulnerability	internal_vuln_exploit_correl...	SECURITY SENSOR FIREWALL LOGS

1-1 of 1

Sumnjivo lateralno kretanje: Pravila koja prate pokušaje lateralnog kretanja unutar mreže, kao što su nenajavljene prijave na nove uređaje ili korištenje alata kao što su PsExec ili PowerShell za daljinsku kontrolu.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Private to Private Exploit Anomaly	Propagation	Lateral Movement	Exploitation of Remote Services	exploit_attempt_priv_priv	

1-1 of 1

PowerShell aktivnost: Otkrivanje sumnjivih PowerShell naredbi ili skripti koje se često koriste u napadima za postizanje trajnog pristupa ili izvršavanje zlonamjernih naredbi.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
PowerShell Remote Access	Persistent Foothold	Execution	Command and Scripting Interpreter	powershell_cnc	WINDOWS AGENT WINDOWS XDLOG

1-1 of 1

Odlaganje vjerodajnica (credential dumping): Detekcija alata ili tehnika povezanih s odlaganjem vjerodajnica, poput Mimikatz alata, koji napadačima omogućuju pristup lozinkama i autentifikacijskim tokenima.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Mimikatz Credential Dump	Propagation	Internal Credential Access	OS Credential Dumping	mimikatz_mem_scan	

1-1 of 1

Komunikacija s Command and Control (C2) poslužiteljima: Pravila za otkrivanje mrežnih aktivnosti koje su povezane s C2 poslužiteljima, gdje napadači održavaju kontrolu nad zaraženim sustavima.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Command & Control Reputation Anomaly	Persistent Foothold	XDR Intel	XDR Command and Control Reputation	cnc_reputation	

1-1 of 1

Sumnjive promjene registra: Detekcija promjena u ključnim postavkama Windows registra, što je čest znak napada gdje se postavke mijenjaju kako bi napadači dobili trajni pristup sustavu ili sakrili svoju aktivnost.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Suspicious Windows Registry Event Impact	Exfiltration & Impact	Impact	(Various Techniques)	suspicious_windows_regist...	

1-1 of 1

Neovlašteni pristup bazi podataka: Praćenje nenajavljenih pokušaja pristupa bazama podataka ili pokušaja izvođenja neuobičajenih upita koji mogu ukazivati na kompromitiranje baza podataka.

Primjer:

COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Internal SQL Anomaly	Propagation	Lateral Movement	Exploitation of Remote Services	Internal_mysql_anomaly	

1-1 of 1

Sumnjiv odlazni promet: Otkrivanje odlaznih mrežnih veza prema visokorizičnim zemljama ili neuobičajenim IP adresama koje mogu biti povezane s krađom podataka, što može biti indikator zlonamjerne aktivnosti ili krađe podataka.

Primjer:

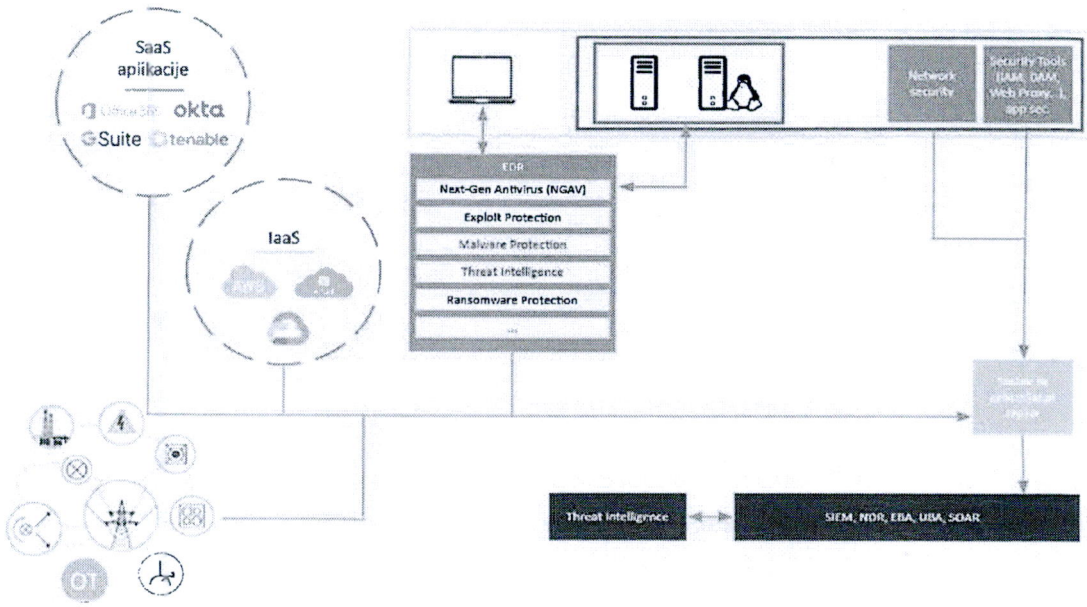
COLUMNS FILTERS

Alert Type	XDR Kill Chain Stage	XDR Tactic	XDR Technique	XDR Event Name	Data Sources
Public to Private Export Anomaly	Initial Attempts	Initial Access	Exploit Public-Facing Application	exploit_attempt_pub_priv	[redacted]

1-1 of 1

Arhitektura sustava

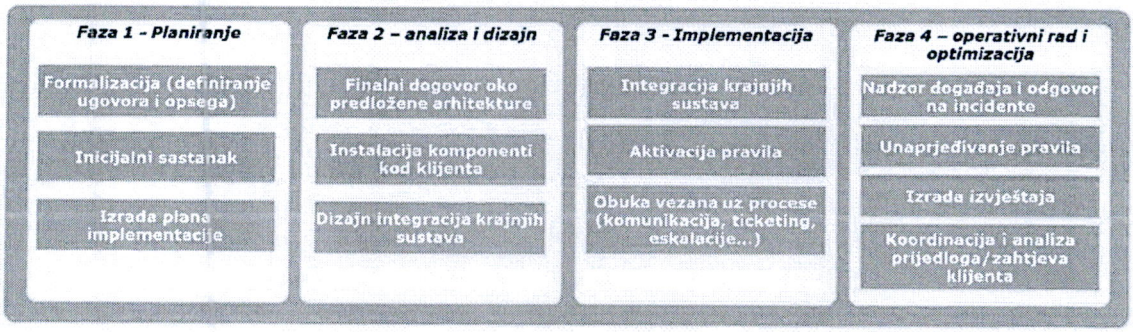
Primjer arhitektura sustava prikazan je donjom slikom, a može se razlikovati u odnosu na sustave i zahtjeve klijenta.



Temeljem inicijalne analize očekivanog broja događaja klijent morati osigurati određene hardverske resurse koji će biti iskorišteni za instalaciju SIEM komponenti za prikupljanje zapisa (ukoliko se ide na virtualiziranu platformu).

Plan implementacije i početka pružanja usluge

Prijedlog plana implementacije prikazan je donjom slikom, a detalji i izmjene se mogu usuglasiti prema potrebama klijenta.



Uloge i odgovornosti

Opisana usluga (nadzor sigurnosnih događaja i upozorenja) osigurava kontinuirani nadzor sigurnosnih događaja, otkrivanje i analizu sigurnosnih incidenata/događaja te reakciju na incident radi sprječavanja širenja incidenta, uklanjanja uzorka i oporavak od incidenta.

U definiranim vremenskim intervalima za pružanje usluga SOC-a istovremeno su dostupni analitičari prve i druge razine za područja ICT tehnologija iz definiranog opsega usluge (npr. mrežnih tehnologija, serverskih tehnologija, radnih stanica itd.).

Klijent SOC-a odgovoran je za identifikaciju imovine koja će se nadzirati te uz popis imovine mora dostaviti najmanje:

1. Mrežnu topologiju (*engl.* Subnets)
2. Listu privilegiranih korisnički računa koji se koriste za administraciju IT okruženja

Odgovornosti prilikom integracije sustava

Aktivnost	Končar – Digital	Klijent SOC-a
Priprema virtualne okoline za instalaciju potrebnih komponenti u klijentovoj okolini	C/I	R/A
Instalacija i održavanje sustava korištenih za Končar – Digital SOC u klijentovoj okolini	R/A	C/I
Komunikacija i uključivanje / isključivanje sustava u i iz SOC usluge	C/I	R/A
Inicijalna i redovna isporuka podataka o imovini (kritičnost imovine, informacije o okolini, verzije softvera, IP adrese itd.)	C/I	R/A
Održavanje i sigurnosno ažuriranje sustava povezanih na Končar - Digital SOC	C/I	R/A

Odgovornosti prilikom nadzora događaja i upravljanja incidentima

Aktivnost	Končar – Digital	Klijent SOC-a
Nadzor događaja	R/A	I
Detekcija i analiza događaja	R/A	I
Generiranje prijave slučaja uz određivanje vjerojatnog redoslijeda prioriteta	R/A	I
Odgovaranje na sigurnosne događaje: • Neutralizacija • Iskorjenjivanje • Oporavak	C/I	R/A
Ublažavanje učinaka sigurnosnih događaja	C/I	R/A

Odgovornosti i zaduženja za platforme korištene u SOC-u

Aktivnost	Končar – Digital	Klijent SOC-a
Nadzor dostupnosti alata (XDR, SIEM, SOAR...)	R/A	I
Popravak kvarova konfiguracije alata korištenih za SC	R/A	I

Preduvjeti

Prije implementacije sustava klijent bi trebao osigurati sljedeće:

- Popis ključnih ljudi u organizaciji (npr. članovi Uprave, odgovorne osobe za financije i informatiku i slično)
- Popis kontakt osoba iz IT odjela kao i osoba odgovornih za sigurnost
- Proces notifikacije i eskalacije za slučaj incidenta
- IP adrese za sustave koji se implementiraju

Kako bi se cijeli sustav mogao adekvatno implementirati potrebno je osigurati podršku osoba zaduženih za:

- Poslužitelje

- klijentska računala
- Active Directory domenu
- Mrežne i sigurnosne uređaje (preklopnike, vatrozide, proxyje, sandbox, itd.)

SLA

Nakon otkrivanja sigurnosnog incidenta SOC pruža kontinuiranu podršku u otkrivanju izvora incidenta, otklanjanja i minimiziranja štete, te prikupljanja dokaza i informacija o tijeku incidenta, sve do zatvaranja incidenta.

Rješavanje sigurnosnih incidenata s obzirom na ozbiljnost incidenata i njihov utjecaj na informacijski sustav i poslovne procese provode se prema sljedećoj tablici:

Prioritet	Utjecaj na raspoloživost, integritet ili povjerljivost informacijskog sustava i poslovnih procesa	Odziv u satima	Rok za rješavanje
P1	ozbiljno narušeno	2 h	8 h
P2	bitno smanjeno	4 h	12 h
P3	otežano	8 h	16 h
P4	odstupa od specifikacije	12 h	32 h

Izvještavanje

Sastavni dio usluge je i izvještavanje o poduzetim intervencijama/zahvatima.
Izvještavanje se sastoji od:
1. Izvještaja o incidentu
2. Mjesečnog izvještaja
3. Izvještaja definiranog od strane klijenta SOC-a (1-2 izvještaja)

Izvještaj o incidentu podrazumijevaju izvještavanje o statusu pojedinog incidenta, a sastoje se od sljedećih informacija:
1. Opis incidenta
2. Kontakt podaci prijavitelja
3. Detalji prijave incidenta:
   - vrijeme kada se incident dogodio
   - vrijeme kada je incident otkriven
   - vrijeme kada je incident prijavljen
   - vrijeme kada je incident riješen
4. Fizička lokacija/adresa incidenta
5. Status
6. Popis i opis sustava na koje je incident utjecao sa poznatim detaljima
7. Kategorija incidenta sukladno taksonomiji incidenata
8. Prioritet incidenta i faktori koji su utjecali na prioritizaciju
9. Mjere sprječavanja ili umanjenja utjecaja
10. Prijedlog akcija za rješavanje incidenta

Mjesečni izvještaj sastoji se od sljedećih poglavlja:
1. Izvještaj za upravu – razina sigurnosti, broj detektiranih prijetnji, zadovoljavanje ugovorenih SLA parametara i povijesni trendovi detekcija
2. Ugovori o razini usluge – raspis definiranih razina usluge
3. Upravljanje uslugama SOC-a:
   - Vremena pružanja usluga

- Broj zaprimljenih/izvršenih zahtjeva za promjenom
- Broj aktivnih detekcijskih pravila
- Broj sustava koji su bili nedostupni za slanje zapisa zajedno s trajanjem nedostupnosti
- Broj sustava koji su dodani/uklonjeni iz sustava/usluge nadzora

4. Nadzor događaja i upozorenja
   - Analiza incidenata (uključujući i tablicu sa detaljima svih incidenata)
   - Trajanje obrade incidenata
   - Analiza sigurnosnih incidenata po kritičnosti
   - Analiza sigurnosnih upozorenja po kategorijama
   - Analiza upozorenja prema tipu
5. Prijedlozi za unapređenje – popis i kratki opis prijedloga koji su proizašli iz zapažanja prilikom pružanja usluge

g

Troškovnik za uspostavu / inicijalizaciju sustava i edukaciju (jednokratno):

R.br	Opis	Ukupna cijena za korisnika EUR
1	Implementacija i dokumentacija ponuđenog sustava (jednokratno)	3.000,00
2	Edukacija administratora (uključeno u cijenu)	0,00
	Ukupni iznos bez PDV-a:	**3.000,00**
	PDV (25%):	**750,00**
	Ukupni iznos s PDV-om	**3.750,00**

Troškovnik za alate i uslugu Security Operations Centra (mjesečno):

R.br	Opis	Količina	Jedinična cijena	Ukupna cijena za korisnika EUR
1	SOC Centar 24/7 licence i upravljana usluga uključuje: SIEM, XDR, NDR i SOC 24/7 uslugu za potrebe Studenca (mjesečno po end-pointu)	1000	3,00	3.000,00
	Ukupni iznos bez PDV-a:			**3.000,00**
	PDV (25%):			**750,00**
	Ukupni iznos s PDV-om			**3.750,00**

Troškovnik za Symantec EDR licence za godinu dana (jednokratno):

R.br	Opis	Količina	Jedinična cijena	Ukupna cijena za korisnika EUR
1	SESC-SES-SUB - Endpoint Security Complete (Includes New SES/SEP Subscription), Hybrid Subscription License with Support, Per Device, 1Y	2400	13,85	33.240,00
	Ukupni iznos bez PDV-a:			**33.240,00**
	PDV (25%):			**8.310,00**
	Ukupni iznos s PDV-om			**41.550,00**

***Napomena za Symantec licence:**

Za korištenje licenci Naručitelj plaća pretplatu na godišnjoj bazi, a svake godine je potrebno obnoviti pretplatu, odnosno kupiti nove licence (subscription model).

*Za Symantec proizvode predviđeno je godišnje povećanje cijena od približno 10%. Međutim, vaša ugovorena fiksna cijena ostaje zagarantirana sve **do 30.12.2026.** Pravovremenim obnavljanjem ponude u idućoj godini, osiguravate iste jedinične cijene kao u 2025. godini, bez dodatnih povećanja.*

Troškovnik za Symantec Web Security licence za godinu dana (jednokratno):

R.br	Opis	Količina	Jedinična cijena	Ukupna cijena za korisnika EUR
1	**SAC-SUB - Symantec ZTNA formerly Secure Access Cloud, Cloud Service Subscription with Support, User 1 YR**	500	24,50	12.250,00
	Ukupni iznos bez PDV-a:			**12.250,00**
	PDV (25%):			**3.062,50**
	Ukupni iznos s PDV-om			**15.312,50**

***Napomena za Symantec licence:**

Za korištenje licenci Naručitelj plaća pretplatu na godišnjoj bazi, a svake godine je potrebno obnoviti pretplatu, odnosno kupiti nove licence (subscription model).

*Za Symantec proizvode predviđeno je godišnje povećanje cijena od približno 10%. Međutim, vaša ugovorena fiksna cijena ostaje zagarantirana sve **do 30.12.2026.** Pravovremenim obnavljanjem ponude u idućoj godini, osiguravate iste jedinične cijene kao u 2025. godini, bez dodatnih povećanja.*

Plaćanje

Rok za plaćanje je do 30 dana po primitku mjesečnog računa za obavljenu uslugu.
Rok za plaćanje je do 30 dana po primitku primopredajnog zapisnika o isporuci opreme.
Sve cijene iskazane su u EUR i plaćanje je također u EUR na račun Raiffeisen banke d.d.:
IBAN: HR2124840081135280987

Isporuka usluga

Rok isporuke za usluge je prema dogovoru s korisnikom.

Valjanost ponude

Ponuda vrijedi do 30.09.2025. godine od datuma primitka ponude.
Za sva dodatna pojašnjenja, eventualne izmjene i dopune stojimo Vam na raspolaganju.

Trajanje Ugovorne obaveze

Ugovor se sklapa na razdoblje od tri (3) godine, računajući od dana potpisivanja ugovora od strane obiju ugovornih strana.

Ugovorne obve razdoblje.

Po isteku ugovo sporazumom ugovornih strana putem pi

13:20

DPD

Dodatne inf

Ovlaštena konta

Za sva pojašnje u stojimo Vam na raspolaganju.

Kontakt osoba:
Sanja Carević Vi
+385 99 6041 7
sanja.carevic@k

S poštovanjem,

Sanja Carević Višnjić, voditeljica ključnih kupaca

KONČAR - Digital d.o.o.
Fallerovo šetalište 22
10000 Zagreb, Hrvatska



FINANCIJSKA AGENCIJA
MAŽURANIĆEVO ŠETALIŠTE 24 B
21 000 SPLIT

„ ~~ZA~~ PREDSTEČAJNI POSTUPAK "

KONČAR

DIGITAL