

Naša št.: 285-41/4-202025
Datum: 20. 3. 2025

TEHNIČNE SPECIFIKACIJE IN ZAHTEV NAROČNIKA

Licence in najem opreme za kibernetško obrambo, št. 285-41

KAZALO

1	PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA	3
2	TEHNIČNE SPECIFIKACIJE IN ZAHTEVE.....	3
2.1	Splošno.....	3
2.1.1	Splošno.....	3
2.1.2	Specifikacija in tehnične zahteve predmeta javnega naročila.....	3
2.1.3	Tehnična podpora	5
2.1.4	Ostale zahteve	6

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA

Predmet tega javnega naročila je najem opreme in licenc za sistem za kibernetško obrambo Darktrace.

Najem in licenčna oprema – licence se nabavlja za obdobje 4 let oziroma 48 mesecev, šteto od dneva aktivacije posamezne licence

Natančne tehnične specifikacije zahteve so opisane v nadaljevanju tega dokumenta.

2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE

2.1 Splošno

2.1.1 Splošno o sistemu Darktrace

Sistem naročnika je sestavljen iz heterogenih sistemov različnih proizvajalcev (HP, IBM, DellEMC, Cisco, Fortinet, PaloAlto, Juniper in podobno).

Jedro omrežje predstavlja Cisco Nexus 9000 serije, naprava za agregacijo in zajem omrežnih pretokov (TAP/SPAN) pa je proizvajalca Garland Networks. Ponudnik lahko pričakuje normaliziran pretok podatkov, ki bo injiciran v strojno opremo sistema za avtomatizirano kibernetško obrambo preko agregacijske naprave.

Naročnik ima v svojem informacijskem okolju implementirano rešitev za centralno upravljanje kibernetške obrambe proizvajalca Darktrace. Sistem sestoji iz treh modulov in sicer; Darktrace Prevent, Darktrace Antigena Email in Darktrace ASM.

2.1.2 Specifikacija in tehnične zahteve predmeta javnega naročila

Specifikacija in tehnične zahteve so podane spodaj.

Postavka	Predmet	Zahteva	Kosov
2.1.2.1	Darktrace Prevent	Najem naprave Darktrace (size M) in licence Darktrace Prevent za najmanj 1500 IP naslovov in možnostjo Ask the Expert. za obdobje 48 mesecev.	1 KPL
2.1.2.2	Darktrace Antigena Email	Najem naprave Darktrace Email in licence Darktrace Antigena Email, za najmanj 350 mailboxov.	1 KPL
2.1.2.3	Darktrace ASM	Licenca za sistem za upravljanje napadalne površine Darktrace ASM – attack surface management.	1 KPL

Licenčna oprema se nabavlja za obdobje 4 let (48 mesecev). V času veljavnosti licenc morajo biti za naročnika zagotovljene vse nadgradnje in morebitni popravki programske opreme, ki je predmet tega naročila.

Opis

Darktrace Prevent mora omogočati integracijo z naročnikovim NGFW (PaloAlto, Fortinet). Sistem mora omogočati podporo za dodatne protokole CNS/ IoT - radarski protokol ASTERIX in nuditi podporo oz. analizo za posameznih dogodkov (2nd level support za posamezne dogodke – t.i. Ask the Expert).

Sistem mora biti namenska fizična naprava z nameščeno programsko opremo za zaznavanje in preprečevanje naprednih kibernetičnih varnostnih groženj, ki se priključi v informacijsko okolje naročnika na način, da lahko ne invazivno in v realnem času analizira promet v celotnem komunikacijskem omrežju oziroma izbranih VLAN-ih (prek zrcaljenja vrat ("TAP" oz. "SPAN") oz. na ustrezen drug način).

Omogočati stalen nadzor aktivnosti in prometa v komunikacijskem omrežju, identificiranje znanih in neznanih potencialnih varnostnih groženj, razvrščanje groženj v skupine in pripravo opozoril v realnem času, takoj ob zaznavi groženj oz. anomalij.

Omogočati enoten pregled nad celotnim omrežjem z vsemi VLAN-i in vsemi v omrežje priključenimi napravami, vključno s fizičnimi, virtualnimi, industrijskimi, ter OT/IoT platformami in napravami;

Analizirati omrežni promet v celotnem omrežju v realnem času, ne glede na protokol prenosa;

Identificirati in v realnem času prikazati vse fizične in virtualne v omrežje priključene naprave z IP naslovom, ki ustvarjajo promet (osebni računalniki, tanki odjemalci, fizični in virtualni strežniki, omrežne naprave, mobilne naprave, druge naprave) ter jih opremiti z vsemi določljivimi, ali z analizo pridobljenimi meta podatki.

Identificirati in prikazati vse zunanje IP naslove, s katerimi v omrežje priključene naprave izmenjujejo podatke in jih prikazovati v kontekstu posameznih groženj in omogočati pregled omrežnega prometa posameznih naprav in zunanjih IP-jev v realnem času, ter zgodovinskem kontekstu.

Podpirati vsa standardna okolja naročnika, vključujoč: Windows operacijske sisteme, Linux operacijske sisteme, industrijske krmilnike in standardne industrijske protokole (od tega najmanj: MODBUS, Niagara, BAC.net, OPC itd.). Sistem mora omogočati podporo za dodatne protokole CNS/ IoT - radarski protokol ASTERIX in nuditi podporo oz. analizo za posameznih dogodkov (2nd level support za posamezne dogodke – t.i. Ask the Expert).

Delovati na način, da meri vsebinske metrike na podatkih, ki se prenašajo po omrežju in na ta način s pomočjo strojnega učenja identificirati normalno delovanje naprav, ter zaznati behavioristične deviacije, ko se zgodijo.

Zaznane deviacije stopnjevati po različnih nivojih eskalacij in dogodke opremiti z ustreznim verjetnostnim matematičnim modelom, ki analitika opozori na resnost/verjetnost določenega dogodka z oceno (Threat Score).

Samodejno se učiti iz aktivnosti v naročnikovem omrežju, prepoznati standardne aktivnosti naročnika in samodejno prilagajati zaznavo groženj in opozorila glede na standardne/nestandardne aktivnosti v omrežju naročnika, zaznane grožnje jasno identificirati in smiselno razvrščati glede na tip in težo.

Naročniku omogočati vizualno podprto pregledovanje, raziskovanje, analiziranje in razreševanje varnostnih dogodkov in groženj, s prikazom podatkovnega prometa in vseh relevantnih povezanih podatkov v realnem času, v času, ko je dogodek nastal in med njima.

Naročniku omogočati prilagajanje uteži groženj za posamezne vrste aktivnosti v omrežju ter iz naročnikovega razreševanja varnostnih dogodkov učiti in ustrezno prilagajati zaznavo groženj in opozorila ter tako s časom zmanjševati obseg lažno pozitivnih rezultatov.

Omogočati pripravo standardnih poročil o grožnjah ter zaznati in opozoriti na varnostno sumljive aktivnosti oz. aktivnosti v nasprotju s politikami, priporočili in dobrimi praksami, tudi v primeru, ko te aktivnosti izvajajo legitimni akterji ali spletni naslovi.

Omogočati vklop in izklop ter podrobno prilagajanje načina avtomatizirane obrambe na varnostne grožnje oz. anomalije, pri katerem se sistem ob zaznani znani ali neznani varnostni grožnji takoj avtomatizirano odzove z ustrezno akcijo za preprečitev grožnje (blokiranjem specifičnega mrežnega prometa, le škodljivega prometa, ali dostopa celotne naprave - karantena). Zmogljivost avtomatizirane obrambe na varnostne grožnje mora temeljiti na prepoznavanju vzorcev varnostnih groženj in učenju iz aktivnosti v omrežju naročnika. Funkcionalnost avtomatizirane obrambe mora omogočati nastavitev povsem avtonomnega delovanja ali odziva s predhodno odobritvijo.

Za svoje delovanje biti povezan le v notranje omrežje naročnika in se ne sme povezovati izven informacijskega okolja naročnika, ter ne sme posredovati nobenih podatkov, razen z izrecno privolitvijo oziroma konfiguracijo naročnika

Za svoje delovanje podatke, pridobljene v okolju naročnika obdelovati izključno na namenski napravi, nameščeni v okolju naročnika, brez pomoči obdelav izven okolja naročnika (npr. obdelave v oblaku).

Biti uporabnikom dostopen kot enotna spletna aplikacija v naročnikovem intranetu, brez dodatnih zahtev za uporabnika (razen brskalnika). Od brskalnikov mora podpirati glavne brskalnike (najmanj novi Microsoft Edge ali Google Chrome).

Biti integriran s centralnim imenikom naročnika, Microsoft Active Directory, SIEM sistemom.

Zagotavljati varnostno kopiranje podatkov na podatkovni sistem naročnika (omrežno kopiranje: SCP, CIFS, ali druga ustrezna rešitev).

Celoten čas trajanja pogodbe imeti zagotovljeno podporo proizvajalca pri analizi posameznih zahtevnejših dogodkov, v kolikor naročnik oceni, da jo v določenem trenutku potrebuje in imeti vključeno takšno storitveno podporo proizvajalca, da v primeru vdora oz. incidenta lahko zagotavlja vso potrebno pomoč in analizo naročniku za čim bolj natančno razrešitev incidenta in ustrezno poročanje pristojnim institucijam.

Sistem Antigena Email mora omogočati prepoznavo zlonamernih vsebin v elektronskih sporočilih (linki ali priponke), ocenjevati pošiljatelja glede možnih groženj naročnikovemu sistemu ter biti popolnoma integriran v celoten sistem za upravljanje kibernetске obrambe Darktrace.

2.1.3 Tehnična podpora

V času veljavnosti licenc, tj. v obdobju 4 let, mora biti za naročnika zagotovljena Tehnična podpora proizvajalca z odzivnim časom 4 ure v režimu 8x5 NBD (Next Business Day)..

Za odzivni čas se šteje čas, v katerem proizvajalec potrdi od naročnika prejeto obvestilo o napaki. V primeru okvare opreme ponudnik izvede zamenjavo opreme pri naročniku brez dodatnih stroškov.

Ponudnik mora zagotoviti garancijo s strani proizvajalca in podporo proizvajalca za vso strojno in programsko opremo z možnostjo neposredne prijave napake pri proizvajalcu brez ponudnikovega posredovanja.

Podpora proizvajalca, ki je zahtevana v razpisu, mora biti na voljo na lokaciji naročnika ter za celotno obdobje trajanja najema oziroma nakupa licenc.

Proizvajalec mora po potrditvi prejema naročnikovega obvestila o napaki začeti z odpravo napake.

Rok za odpravo napake ali dostavo nadomestne opreme je tri delovne dni od potrditve proizvajalca o ugotovljeni napaki na opremi.

Predstavniki proizvajalca prevzame opremo (ali del opreme) v popravilo na lokaciji naročnika in jo vrne na naslov naročnika. V kolikor proizvajalec ni sposoben v zahtevanem roku za odpravo napake napako odpraviti, mora zagotoviti popravilo ali zamenjavo pokvarjene enote. Za čas dokler se naprava ne popravi, mora dostaviti naročniku nadomestno opremo z najmanj enako zmogljivostjo, funkcionalnostjo ter vsemi licencami. Nadomestna oprema mora biti pripravljena za takojšnje delovanje ob umestitvi v sistem.

Po popravilu naročnikove opreme se nadomestna oprema zamenja z naročnikovo. Proizvajalec mora obvezno kriti stroške prevoza v obeh smereh, tudi za prevoz nadomestne opreme.

2.1.4 Ostale zahteve

2.1.4.1 Izjava

Ponudnik mora predložiti izjavo proizvajalca ali uradnega zastopnika za območje Slovenije, da ima ponudnik s proizvajalcem ponujene opreme sklenjeno veljavno pogodbo, ki zajema tako dobavo opreme, kot tudi celotno podporo (dostop) do tehnične pomoči, dostop do baze znanj, za blagovno znamko, ki jo ponuja in status Darktrace Partnerja.

2.1.4.2 Usposobljenost kadra

Usposobljenost ponudnikovega kadra za instalacijo, konfiguriranje, vzdrževanje, tehnično podporo opreme ponujenega proizvajalca: ponudnik mora zagotoviti ustrezno veljavno potrdilo/certifikat proizvajalca o opravljenem usposabljanju vsaj za 2 (dva) strokovnjaka z nazivom Darktrace Cyber Engineer .

.....*konec dokumenta*.....

