Crna Gora - Vlada Crne Gore
UPRAVA ZA STATISTIKU
Broj 01-426/24-4993/10
Podgorica, 10. 12. 2024 20___ god.

digit montenegro DOO
Broj 1124
Podgorica, 4.12.24 god.

UGOVOR O JEDNOSTAVNOJ NABAVCI

ANTIVIRUSNI SOFTVER

Ovaj ugovor zaključen je između:

Naručioca: Uprave za statistiku, sa sjedištem u Podgorici, Ul. IV proleterske br.2, PIB 02011506, koga zastupa direktor, Miroslav Pejović (u daljem tekstu Naručilac), i i

Ponuđača: Digit Montenegro doo, sa sjedištem u Podgorici, Ul.Studenska 18, PIB 02247488, koga zastupa izvršni direktor, Duško Petrović, broj žiro računa, naziv banke: 565-113-39, Lovćen banka AD. (u daljem tekstu: IZVRŠILAC).

Član 1

Osnov ugovora: zahtjev za dostavljanje ponuda, šifra postupka br. 83194 od 29.11.2024. godine, ponuda ponuđača „Digit Montenegro" doo broj 116963 od 02.12.2024. god. (zavodni broj 10-426/24-4993/4), obavještenje o ishodu postupka jednostavne nabavke br. 01-426/24-4993/9 od 09.12.2024. godine.

Član 2

Predmet ovog ugovora je nabavka antivirusnog softvera, za period od jedne godine, od dana isporuke licenci, antivirusni softver -Sistem za naprednu zaštitu servera i radnih stanica Trend Micro Trend Vision One - Endpoint Security (Essentials). „Digit Montengro" DOO je dužan da fizički instalirati softver, poveže i integriše u postojeći sistem naručioca, prema zahtjevu naručioca i u skladu sa najboljom praksom i profesionalnim standardima. Integracija podrazumijeva stavljanje ponuđenog softvera u punu funkciju, kako bi opsluživala klijentske zahtjeve. Nakon implementacije, Digit Montengro DOO će dostavtii naručiocu dokumentaciju izvedenog stanja. Digit Montengro DOO će u periodu trajanja licenci pružati tehnicku podršku naruciocu.

Izvršilac posla se obavezuje da će pružati usluge - isporuku licenci za antivirus u svemu prema zahtjevu za dostavljanje ponuda #83194 od 29.11.2024. godine, ponudi ponuđača „Digit Montenegro" doo br. 116963 od 02.12.2024. god. i obavještenju o ishodu postupka jednostavne nabavke br. 01-426/24-4993/9 od 09.12.2024. godine.

Član 3

Mjesto izvršenja ugovora je: Uprava za statistiku, Ul. IV proleterske br.2. Rok izvršenja ugovora: 15 dana od dana zaključenja ugovora.

Član 4

Ukupna cijena za usluge navedene u čl. 2 ovog ugovor je 11.700,00 eura, iznos PDV 2.457,00 eura, ukupna cijena sa PDV- om 14.157,00 eura.

Rok plaćanja je 20 dana od dana dostavljanja fakture, nakon isporuke i implementacije predmeta nabavke i prijema od strane ovlašćenih lica naručioca. Način plaćanja je virmanski.

Plaćanje će se izvršiti na račun izvršioca posla 565-113-39, Lovćen banka AD.

Član 5

Ugovorne strane određuju svoje predstavnike, koji organizuju i koordiniraju aktivnosti Naručioca i Izvršioca:

Predstavnik Naručioca:

Ime: Boro Durković

Telefon: 068/851 577

e-mail:boro.durkovic@monstat.org

Predstavnik Izvšioca:

Ime: Darko Petrović

Telefon: 067/608 602

e-mail: Darko.Petrovic@digit.me

Ugovorne strane se obavezuju da sarađuju sa prestavnicima i zaposlenima druge ugovorne strane, a koji su određeni shodno stavu 1 ovog člana.

Ugovorne strane obavještavaju jedna drugu i bez odlaganja o svim informacijama, činjenicama i okolnostima koje sprečavaju ili ometaju izvršenje ugovornih obaveza. Takvi podaci obuhvataju i promjene predstavnika i njihovih e- mail adresa.

Ugovorne strane su saglasne da razmjenjuju korespodenciju koja se odnosi na izvršenje ovog ugovora preporučenim ili povratnim vrednosnom pošiljkomama ili e-mail.

Član 6

Ukoliko naručilac ima osnovan razlog za nezadovoljstvo radom bilo kojeg člana osoblja izvršioca, u tom slučaju, izvršilac će na osnovu pisanog zahtjeva naručioca, u kome se navodi razlog, obezbjediti kao zamjenu lice sa kvalifikacijama i iskustvom koji su prihvatljivi naručiocu.

Izvršilac nema pravo da zahtjeva pokrivanje dodatnih troškova koji proističu ili su u vezi sa premještanjem ili zamjenom osoblja.

Član 7

Izvršilac posla se obavezuje da pruži usluge po opisu, rokovima i cijenama iz izabrane ponude broj #116963 od 02.12.2024. god., kao i odredbama ovog ugovora, a naručilac da primi uslugu i isplati Izvršiocu ugovorenu vrijednost usluge.

Član 8

Izvršilac posla se obavezuje:

- da usluge koje su predmet ovog ugovora izvodi u skladu sa važećim zakonskim propisima, normativima i standardima za ovu vrstu posla;
- izvršilac snosi troškove naknade korišćenja patenata i odgovoran je za povredu zaštićenih prava intelektualne svojine trećih lica;
- da usluge pruža kvalifikovanom radnom snagom sa potrebnim iskustvom za ovu vrstu posla;
- da rukovodi izvršenjem svih usluga;
- da odmah po zahtjevu naručioca, pristupi otklanjanju uočenih nedostataka i propusta u obavljanju posla;
- da poštuje rokove za izvršenje ugovornih obaveza,
- da naknadi svu štetu naručiocu, koja bude prouzrokovana nesavjesnim i nekvalitetnim radom ili krivicom lica koje vrši ugovorene poslove.

Član 9

Naručilac se obavezuje da zvršioca posla uvede u posao. Pod uvođenjem u posao podrazumjeva se obezbjeđenje svih potrebnih uslova za nesmetano obavljanje posla.

Član 10

Ugovorne strane su saglasne da do raskida ovog ugovora može doći ako izvršilac posla ne bude izvršavao svoje obaveze u rokovima i na način predviđen ugovorom i dostavljenom ponudom izvršioca.
Ukoliko izvršilac ne ispuni svoju obavezu naručilac će raskinuti ugovor prostom izjavom, uz ostvarenja prava na naknadu štete.
Pošto je ispunjenje obaveza u rokovima određenim ovim ugovorom njegov bitan elemenat, ugovor će se raskinuti, ako ponuđač ne ispuni obavezu u definisanim rokovima.
Ako ugovorne strane sporazumno raskinu ugovor, sporazumom o raskidu ugovora utvrđuju se međusobna prava o obaveze koje proističu iz ugovora.

Član 11

Izvršilac i njegovo osoblje se obavezuje da u toku važenja ovog Ugovora, ne iznose bilo kakve službene ili povjerljive informacije u vezi ovog ugovora, poslova i aktivnosti naručioca, bez prethodne pisane saglasnosti naručioca. Izvršilac će podatke, koje će mu dostavljati naručilac, čuvati kao poslovnu tajnu i upotrebljavaće ih oni izvršiočevi službenici koji će biti uključeni u realizaciju poslova po ovom ugovoru.

Član 12

Za sve što nije regulisano ovim ugovorom, primjenjivaće se odredbe Zakona o obligacionim odnosima.

Član 13

Eventualne sporove po osnovu primjene ovog ugovora, ugovorne strane će rješavati sporazumno.
Ukoliko se spor ne može riješiti na taj način, za rješavanje spora nadležan je Privredni sud u Podgorici.

Član 14

Ugovor o javnoj nabavci koji je zaključen uz kršenje antikorupcijskog pravila u smislu čl. 25 Pravilnika o načinu sprovođenja jednostavnih nabavki ("Sl.Crne Gore", br. 16/23 od 10.02.2023, 020/23 od 22.02.2023, 036/23 od 29.03.2023.) ništav je.

Član 15

Ovaj Ugovor sačinjen je u 4 (četiri) jednakih primjerka, po 2 (dva) primjerka za svaku ugovornu stranu.

NARUČILAC
Uprava za statistiku

DIREKTOR

Miroslav Pejović

IZVRŠILAC
„Digit Montenegro" doo

IZVRŠNI DIREKTOR

Duško Petrović

PREGLED PONUDE #116963

1 OSNOVNI PODACI O PONUDI

Datum i vrijeme podnošenja	02.12.2024. 23:14
Status ponude	Podnijeta
Ponuda/prijava se podnosi kao	Samostalna ponuda

2 PODACI O PODNOSIOCU

Naziv	Digit Montenegro d.o.o.
PIB	02247488
Država	Crna Gora
Grad	Podgorica
E-mail	info@digit.me

3 PODACI O JAVNOJ NABAVCI

Naziv naručioca	UPRAVA ZA STATISTIKU
Šifra postupka	83194
Opis predmeta javne nabavke	Antivirusni softver
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Vrsta faze	Zahtjev za podnošenje ponuda

4 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Odgovor / napomena	Eksplicitna / Utvrđena vrijednost
Ponuđač je dužan u okviru podnijete ponude, a u skladu sa članom 9 stav 10 Pravilnika o načinu sprovođenja jednostavnih nabavki ("Sl.list Crne Gore", broj 016/23 od 10.02.2023. godine, broj 020/23 od 22.02.2023. godine, 36/23 od 29.03.2023., 114/23 od 19.12.2023. i 49/24 od 29.05.2024.), dostaviti Izjavu ponuđača (Obrazac 2) o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisanu od strane ovlašćenog lica ponuđača, datu na Obrascu 2, koji se nalazi u prilogu zahtjeva za podnošenje ponuda.	Izjavu - Obrazac 2 DIGIT MONTENEGRO DOO dostavlja u prilogu.	-
Mjesto izvršenja ugovora: Uprava za statistiku, Ul. IV proleterske br. 2	Mjesto izvršenja ugovora: Uprava za statistiku, Ul. IV proleterske br. 2	-
Plaćanje je u roku od 20 dana od dana dostavljanja fakture, nakon isporuke i implementacije predmeta nabavke i prijema od strane ovlašćenih lica naručioca.	Plaćanje je u roku od 20 dana od dana dostavljanja fakture, nakon isporuke i implementacije predmeta nabavke i prijema od strane ovlašćenih lica naručioca.	-
Način plaćanja: virmanski	Način plaćanja: virmanski	-
Rok izvršenja ugovora: 15 dana od dana zaključenja ugovora.	Rok izvršenja ugovora: 15 dana od dana zaključenja ugovora.	-
Rok važenja ponude: 90(devedeset) dana od dana otvaranja ponuda	Rok važenja ponude: 90 (devedeset) dana od dana otvaranja ponuda	-

Ponuđač mora biti ovlašćen od strane proizvođača za isporuku traženih softverskih licenci na teritoriji Crne Gore (ukoliko nije proizvođač), što se dokazuje autorizacijom proizvođača softvera (MAF).	Autorizaciju ponuđača DIGIT MONTENEGRO DOO dostavlja u prilogu.	-
Ponuđač je dužan da antivirusni softver fizički instalira, poveže i integriše u postojeći sistem naručioca, prema zahtjevu naručioca i u skladu sa najboljom praksom i profesionalnim standardima. Integracija podrazumijeva stavljanje ponuđenog softvera u punu funkciju, kako bi opsluživala klijentske zahtjeve. Nakon implementacije, izabrani ponuđač dužan je da dostavi naručiocu dokumentaciju izvedenog stanja. Ponuđač je dužan da u periodu trajanja licenci pruza tehnicku podrsku naruciocu.	DIGIT MONTENGRO DOO će u slučaju zaključenja Ugovora fizički instalirati softver, povezati i integrisati u postojeći sistem naručioca, prema zahtjevu naručioca i u skladu sa najboljom praksom i profesionalnim standardima. Integracija podrazumijeva stavljanje ponuđenog softvera u punu funkciju, kako bi opsluživala klijentske zahtjeve. Nakon implementacije, DIGIT MONTENGRO DOO će dostavtii naručiocu dokumentaciju izvedenog stanja. DIGIT MONTENEGRO DOO će u periodu trajanja licenci pružati tehnicku podrsku naruciocu.	-
ISO 9001Dokaz o uspostavljenom sistemu upravljanja kvalitetom.	U prilogu dostavljamo sertifikat ISO 9001Dokaz o uspostavljenom sistemu upravljanja kvalitetom.	-
ISO 27001 Dokaz o uspostavljenom sistemu menadžmenta bezbjednošću	U prilgu dostavljamo sertifikat ISO 27001 Dokaz o uspostavljenom sistemu menadžmenta bezbjednošću	-
ISO 20000-1 Sistem menadžemnta uslugom	U prilogu dostavljamo sertifikat ISO 20000-1 Sistem menadžemnta uslugom	-
ISO 27701 - Sistemi menadžmenta informacijama o privatnosti	U prilogu dostavljamo sertifikat ISO 27701 - Sistemi menadžmenta informacijama o privatnosti	-

5 FINANSIJSKI DIO

Procijenjena vrijednost nabavke: 12.000,00 EUR

Ponuđena cijena bez PDV: 11.700,00 EUR

	Opis	Bitne karakteristike predmeta nabavke	Odgovor	Količina	Cijena po jedinici
1	Antivirusni softver	Sistem za naprednu zaštitu servera i radnih stanica Mogućnost primjene modula zaštite u različitim varijantama i njihovim proizvoljnim kombinacijama, integrisanim u jednu konzolu u cloud-u: • Extended Detection and Response (XDR) senzor, samo XDR komponenta koja može da radi samostalno (na primjer zajedno sa postojećim antimalverom drugog proizvođača). • Standardna zaštita radnih stanica i servera na Windows i MacOS platformama, sa fokusom na desktop i prenosive računare. • Opciona namjenska zaštita virtualnih okruženja i servera na Windows, Linux i AIX platformama sa naprednim funkcionalnostima fokusiranim na servere i virtualna okruženja. • Opcioni Attack Surface Management (ASRM) senzor, koji može da radi samostalno (na primjer zajedno sa postojećim antimalverom drugog proizvođača). Extended Detection and Response (XDR) • Mogućnost čuvanja logova od 30 do 365 dana. • Instalirani XDR mora imati mogućnost da otkrije softverske ranjivosti na operativnom sistemu i	Antivirusni softver Sistem za naprednu zaštitu servera i radnih stanica Trend Micro Trend Vision One - Endpoint Security (Essentials) ima mogućnost primjene modula zaštite u različitim varijantama i njihovim proizvoljnim kombinacijama, integrisanim u jednu konzolu u cloud-u: • Ima Extended Detection and Response (XDR) senzor, samo XDR komponenta koja može da radi samostalno (zajedno sa postojećim antimalverom drugog proizvođača). • Ima standardnu zaštitu radnih stanica i servera na Windows i MacOS platformama, sa fokusom na desktop i prenosive računare. • Ima namjensku zaštitu virtualnih okruženja i servera na Windows, Linux i AIX platformama sa naprednim funkcionalnostima	300,00 licenci	39,00 EUR

		instaliranim aplikacijama (npr. Adobe Reader, gdje je instaliran). • Automatsko slanje potencijalno malicioznih uzoraka, na osnovu XDR analize, u Sandbox sa mogućnošću ručnog otpremanja uzoraka (Manual submission). • Podrška za Windows, MacOS i Linux platformame, uz mogućnost rada sa antimalware agentima drugih proizvođača (3rd party). • Mora imati veliki broj modela detekcije kojima upravlja administrator sistema, na osnovu kojih se vrši XDR korelacija podataka, mogućnost postavljanja izuzetaka za date modele detekcije, kao i pravljenje sopstvenih modela detekcije. • Mora sadržavati specijalizovane Indication of Compromise (IoC) kanale kojima upravlja administrator sistema, a koji prate poznate kampanje zlonamjernih napadačkih grupa u svrhu automatske detekcije i čišćenje detektovanih IoC-a. • Mora sadržavati specijalizovane IoC kanale od nezavisnih dobavljača koji se mogu koristiti za isto kao i postojeći (detekcija i čišćenje). • Mogućnost unosa ručnih IoC objekata, i drugih obavještajnih podataka o prijetnji,	fokusiranim na servere i virtualna okruženja. • Ima opcioni Attack Surface Management (ASRM) senzor, koji može da radi samostalno (na primjer zajedno sa postojećim antimalverom drugog proizvođača). Extended Detection and Response (XDR) • Ima mogućnost čuvanja logova od 30 do 365 dana. • Instalirani XDR ima mogućnost da otkrije softverske ranjivosti na operativnom sistemu i instaliranim aplikacijama (npr. Adobe Reader, gdje je instaliran). • Ima automatsko slanje potencijalno malicioznih uzoraka, na osnovu XDR analize, u Sandbox sa mogućnošću ručnog otpremanja uzoraka (Manual submission). • Ima podršku za Windows, MacOS i Linux platforme, uz mogućnost rada sa antimalware agentima drugih proizvođača (3rd party). • Ima veliki broj		

		koji se zatim mogu koristiti za detekciju i čišćenje. • Podrška sledećih formata unosa IoC-a: STIX, TAXII, MISP, csv. • Jasna vizualizacija XDR detekcije/incidenta, međusobne povezanosti objekata i detaljnih informacija o svakom objektu. • Jasna vizuelizacija EDR podataka krajnjeg uređaja, gdje se može vidjeti kako je proces pokrenut, koje promjene je napravio na sistemu, kakva se mrežna komunikacija odvijala, izmjene u registrima itd. • Mora automatski povezivati pojedinačne detekcije u složene incidente na osnovu uobičajenih objekata (kao što su IP adrese, krajnji uređaji, domeni, identične datoteke, detekcije, itd.). • Širok spektar akcija odgovora: računar/server - izolacija iz mreže, slanje datoteke u Sandbox, preuzmanje datoteke za dalju analizu, prijava na komandnu liniju agenta (naknadno, opcija za prekid procesa, pregled registara, sistema datoteka, memorije, itd.), pokretanje skripte (powershell/bash), blokiranje objekata (datoteka, hash, IP adresa, domen, itd.); E-mail - blokiranje elektronske pošte na osnovu pošiljaoca, premještanje elektronske	modela detekcije kojima upravlja administrator sistema, na osnovu kojih se vrši XDR korelacija podataka, ima mogućnost postavljanja izuzetaka za date modele detekcije, kao i pravljenje sopstvenih modela detekcije. • Sadrži specijalizovane Indication of Compromise (IoC) kanale kojima upravlja administrator sistema, a koji prate poznate kampanje zlonamjernih napadačkih grupa u svrhu automatske detekcije i čišćenje detektovanih IoC-a. • Sadrži specijalizovane IoC kanale od nezavisnih dobavljača koji se mogu koristiti za isto kao i postojeći (detekcija i čišćenje). • Ima mogućnost unosa ručnih IoC objekata, i drugih obavještajnih podataka o prijetnji, koji se zatim mogu koristiti za detekciju i čišćenje. • Ima podršku sledećih formata unosa IoC-a: STIX, TAXII, MISP, csv. • Ima jasnu vizualizacija XDR		

		pošte u karantin ili brisanje; Korisnik - odjava korisnika, blokiranje korisnika, promjena šifre korisnika. • Logovanje svih gore pomenutih akcija odgovora. • Mogućnost konfiguracije pristupa administratorskoj konzoli na osnovu uloga i dodjele specifičnih prava (Role Based Access Control – RBAC). • Opciono usluga servisa nadgledanja XDR-a (Managed Detection and Response – MDR): 24x7, slanje redovnih izveštaja, filtriranje lažnih pozitivnih rezultata (False Positive), savjetovanje prilikom suočavanja sa detektovanim incidentom, itd. • Podrška za automatizaciju zasnovanu na Playbook-ovima, npr.: podešavanje automatskih radnji odgovora na osnovu detekcije (mogućnost detaljnih podešavanja na osnovu kritičnosti detekcije ili modela detekcije), automatsko izvršavanje skripte na definisanim štićrnim stanicama pod različitim uslovima (zakazano, detekcija, ručno), upozorenje u slučaju otkrivanja nove kritične ranjivosti (notifikacija), itd. • Mogućnost prikupljanja važnih informacija za forenzičku istragu krajnjih tačaka: informacije o sistemu, informacije o korisničkim nalozima,	detekcije/incidenta, međusobne povezanosti objekata i detaljnih informacija o svakom objektu. • Ima jasnu vizuelizaciju EDR podataka krajnjeg uređaja, gdje se može vidjeti kako je proces pokrenut, koje promjene je napravio na sistemu, kakva se mrežna komunikacija odvijala, izmjene u registrima itd. • Automatski povezuje pojedinačne detekcije u složene incidente na osnovu uobičajenih objekata (kao što su IP adrese, krajnji uređaji, domeni, identične datoteke, detekcije, itd.). • Ima širok spektar akcija odgovora: računar/server - izolacija iz mreže, slanje datoteke u Sandbox, preuzmanje datoteke za dalju analizu, prijava na komandnu liniju agenta (naknadno, opcija za prekid procesa, pregled registara, sistema datoteka, memorije, itd.), pokretanje skripte (powershell/bash), blokiranje		

		mrežne informacije, informacije o pokrenutim procesima, lista automatski startovanih objekata (Startup programs), AmCache, ShimCache, itd. • Praćenje indeksa rizika za cijelu organizaciju, kao i praćenja rizika pojedinačnih uređaja i korisnika. • Izvještaj o svim datim preporukama za smanjenje indeksa rizika, za cijelu organizaciju, kao i pojedinačnih uređaja i korisnika. • Izvještaj o loše konfugirisanim sistemima za zaštitu istog proizvođača. • Detekcija uređaja koji nemaju aktivne ključne bezbjednosne funkcije (kao što je antimalver). • Analiza kompanijskih IP adresa i domena koji su izloženi Internetu i pregled servisa koji na njima rade, kao i procjena njihovih rizika. • Automatsko upozorenje u slučaju da se kritična ranjivost pojavi na servisu/serveru izloženom Internetu • Analiza korisnika, mreže i uređaja, uključujući procjenu njihovih rizika. • Mapiranje svih događaja u organizaciji na MITRE tehnike i taktike, sa mogućnošću pretrage i filtriranja po njihovom osnovu. Standardna zaštita radnih stanica • Zaštita radnih stanica i servera od svih	objekata (datoteka, hash, IP adresa, domen, itd.); E-mail - ima blokiranje elektronske pošte na osnovu pošiljaoca, premještanje elektronske pošte u karantin ili brisanje; Korisnik – ima odjavu korisnika, blokiranje korisnika, promjena šifre korisnika. • Ima logovanje svih gore pomenutih akcija odgovora. • Ima mogućnost konfiguracije pristupa administratorskoj konzoli na osnovu uloga i dodjele specifičnih prava (Role Based Access Control – RBAC). • Ima opcionu uslugu servisa nadgledanja XDR-a (Managed Detection and Response – MDR): 24x7, slanje redovnih izvještaja, filtriranje lažnih pozitivnih rezultata (False Positive), savjetovanje prilikom suočavanja sa detektovanim incidentom, itd. • Ima podršku za automatizaciju zasnovanu na Playbook-ovima, npr.: podešavanje automatskih radnji odgovora		

		vrsta zlonamjernih programa (virusi, crvi, špijunski softver, grayware i drugi srodni programi). • Klijentski zaštitni zid (Firewall) sa konfiguracijom parametara prema smjeru, vrsti saobraćaja i aplikacije, potpuno integrisan u klijent antivirusa i upravljačku konzolu, sa jednostavnim definisanjem politike zaštitnog zida iz upravljačke konzole. • Zaštita od enkripcije računara (Ransomware): proaktivno blokiranje zlonamjernih programa koji preuzimaju kontrolu nad računarom i/ili šifruju datoteke na računaru, sa mogućnošću pravljenja rezervnih kopija za oporavak šifrovanih podataka ako je proces ransomware-a odgovoran za njihovo šifrovanje. • Statična (analiza svojstva datoteka) i dinamička (analiza ponašanja datoteke) analiza korišćenjem algoritama mašinskog učenja. • Integrisana zaštita u realnom vremenu (real-time) od mrežnih crva i otkrivanje iskorišćavanja ranjivosti na IP nivou (npr. Downad/Conficker i srodne varijante mrežnih crva). • Integrisana detekcija zlonamjernog saobraćaja (klijentski IPS/IDS sistem), uključujući tipične napade na IP nivou	na osnovu detekcije (mogućnost detaljnih podešavanja na osnovu kritičnosti detekcije ili modela detekcije), automatsko izvršavanje skripte na definisanim štićenim stanicama pod različitim uslovima (zakazano, detekcija, ručno), upozorenje u slučaju otkrivanja nove kritične ranjivosti (notifikacija), itd. • Ima mogućnost prikupljanja važnih informacija za forenzičku istragu krajnjih tačaka: informacije o sistemu, informacije o korisničkim nalozima, mrežne informacije, informacije o pokrenutim procesima, lista automatski startovanih objekata (Startup programs), AmCache, ShimCache, itd. • Ima praćenje indeksa rizika za cijelu organizaciju, kao i praćenja rizika pojedinačnih uređaja i korisnika. • Ima izvještaj o svim datim preporukama za smanjenje		

		(Ping of death, SYN flood, Teardrop, itd.); • Automatsko centralizovano čišćenje zaraženih računara bez intervencije administratora; potpuno integrisan u antivirusni klijent (čišćenje zapisa registra, ini zapisa, memorijskih procesa koje su ostavili crvi, itd.). • Automatsko čišćenje špijunskih programa potpuno integrisano u antivirusni klijent. • Zaštita od zlonamjernog koda zasnovanog na vebu (web exploits). • Blokiranje pristupa zlonamjernim veb lokacijama na nivou klijenta na osnovu IP adrese ili URL reputacije, i mogućnost definisanja fleksibilne politike filtriranja u zavisnosti od lokacije i statusa klijenta. • Provjera reputacije fajlova (File Reputation) na klijentu direktnim kontaktiranjem servera ili onlajn servisa proizvođača. • Automatsko prikupljanje informacija o prijetnjama i automatsko ažuriranje baze reputacije proizvođača. • POP3 Mail Scan provjerava da li ima virusa i neželjene pošte integrisane u klijentu. • Praćenje ponašanja klijenta (Behavior Monitoring) sa „In The Cloud“ provjerom da li je aplikacija poznata i bezbjedna (provjera na	indeksa rizika, za cijelu organizaciju, kao i pojedinačnih uređaja i korisnika. • Ima izvještaj o loše konfugirisanim sistemima za zaštitu istog proizvođača. • Ima detekciju uređaja koji nemaju aktivne ključne bezbjednosne funkcije (kao što je antimalver). • Ima analizu kompanijskih IP adresa i domena koji su izloženi Internetu i pregled servisa koji na njima rade, kao i procjena njihovih rizika. • Ima automatsko upozorenje u slučaju da se kritična ranjivost pojavi na servisu/serveru izloženom Internetu • Ima analizu korisnika, mreže i uređaja, uključujući procjenu njihovih rizika. • Ima mapiranje svih događaja u organizaciji na MITRE tehnike i taktike, sa mogućnošću pretrage i filtriranja po njihovom osnovu. Standardna zaštita radnih stanica • Ima zaštitu radnih stanica i servera od		

		nivou starosti i zastupljenosti aplikacije). • Mogućnost vraćanja datoteka koje su stavljene u karantin kao sumnjive, centralno preko administratorske konzole i uz definisanje izuzetaka od budućeg karantina. • Mogućnost definisanja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) za praćenje ponašanja aplikacija , što uključuje sumnjive radnje kao što su: promjene u hosts fajlu, kreiranje duplikata poznatih sistemskih datotekeka, instaliranje novog dodatka za Internet Explorer, promjena podešavanja u Internet Explorer-u, promjena Windows Security Policy podešavanja, umetanje novog dll-a, stvaranje novog startup programa itd. Za svaku od ovih sumnjivih radnji treba da bude moguće definisati različite odgovore: od blokiranja, preko upozorenja i logovanja do dozvole za rad. • Mogućnost definisanja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) za kontrolu pristupa eksternim uređajima na klijentu (prenosivi medijumi povezani preko USB-a). • Blokiranje funkcije Autorun pri	svih vrsta zlonamjernih programa (virusi, crvi, špijunski softver, grayware i drugi srodni programi). • Ima klijentski zaštitni zid (Firewall) sa konfiguracijom parametara prema smjeru, vrsti saobraćaja i aplikacije, potpuno integrisan u klijent antivirusa i upravljačku konzolu, sa jednostavnim definisanjem politike zaštitnog zida iz upravljačke konzole. • Ima zaštitu od enkripcije računara (Ransomware): proaktivno blokiranje zlonamjernih programa koji preuzimaju kontrolu nad računarom i/ili šifruju datoteke na računaru, sa mogućnošću pravljenja rezervnih kopija za oporavak šifrovanih podataka ako je proces ransomware-a odgovoran za njihovo šifrovanje. • Ima statičnu (analiza svojstva datoteka) i dinamičku (analiza ponašanja datoteke) analizu korišćenjem algoritama mašinskog učenja. • Ima		

		povezivanju USB diskova sa klijentom. • Kontrola pristupa mrežnim resursima i dijeljenim diskovima (network shares). • Provjera web saobraćaja, koja sprječava pokretanje zlonamjernih veb skripti i iskorišćavanje bezbjednosnih propusta u pretraživaču, u realnom vremenu. • Otkrivanje i evidentiranje aktivnosti C&C komunikacije sa granularnom konfiguracijom akcija po detekciji mrežne komunikacije prema C&C serverima. • Podrška za VDI okruženja (virtuelizacija desktopa): mogućnost ograničavanja potrošnje resursa virtuelnih radnih stanica na nivou host-a - VMware vCenter (VMware View), Citrix XenServer 5.5 (Citrix XenDesktop 4). Mogućnost prethodnog skeniranja Master VDI image-a i kontrolisanog postavljanja komponenti za ažuriranje na pojedinačnim VDI host-ovima • DLP dodatak koji se može naknadno uključiti, integrisan u identično administrativno okruženje sa sledećim funkcionalnostima: o mogućnost napredne kontrole USB uređaja prema proizvođaču (ID dobavljača, serijski brojevi) o Mogućnost napredne kontrole	integrisanu zaštitu u realnom vremenu (real-time) od mrežnih crva i otkrivanje iskorišćavanja ranjivosti na IP nivou (npr. Downad/Conficker i srodne varijante mrežnih crva). • Ima integrisanu detekciju zlonamjernog saobraćaja (klijentski IPS/IDS sistem), uključujući tipične napade na IP nivou (Ping of death, SYN flood, Teardrop, itd.); • Ima automatsko centralizovano čišćenje zaraženih računara bez intervencije administratora; potpuno integrisan u antivirusni klijent (čišćenje zapisa registra, ini zapisa, memorijskih procesa koje su ostavili crvi, itd.). • Ima automatsko čišćenje špijunskih programa potpuno integrisano u antivirusni klijent. • Ima zaštitu od zlonamjernog koda zasnovanog na vebu (web exploits). • Ima blokiranje pristupa zlonamjernim veb lokacijama		

		informacija poslatih preko perifernih uređaja (COM/LPT port, IEEE 1394, uređaji za obradu slike, modem, PCMCIA port, Bluetooth, mobilni uređaji, print screen) o Mogućnost kontrole sadržaja na različitim transportnim kanalima uključujući: elektronsku poštu (SMTP), Veb (HTTP, HTTPS), FTP i SMB protokoli o Kreiranje politika u zavisnosti od lokacije klijenta/računara. o Kontrola informacija kroz: unaprijed definisane politike koje uključuju: PCI DSS pravila za otkrivanje prenosa brojeva kartica ili bankovnih računa; lične podatke kao što su OIB ili JMBG brojevi; izvorni kodovi često korišćenih programskih jezika i drugi; definisanje sopstvenih politika korišćenjem proizvoljnih ključnih riječi ili regularnih izraza. o Moguće radnje u slučaju kršenja pravila: blokiranje prenosa, omogućavanje prenosa sa evidentiranjem incidenata, prikazivanje poruke upozorenja korisniku sa opcijom da se dozvoli slanje. o Mogućnost provjere cijelog računara na osjetljive informacije, uz mogućnost evidentiranja pronađenih informacija. o Mogućnost propuštanja osjetljivih podataka na	na nivou klijenta na osnovu IP adrese ili URL reputacije, i mogućnost definisanja fleksibilne politike filtriranja u zavisnosti od lokacije i statusa klijenta. • Ima provjeru reputacije fajlova (File Reputation) na klijentu direktnim kontaktiranjem servera ili onlajn servisa proizvođača. • Ima automatsko prikupljanje informacija o prijetnjama i automatsko ažuriranje baze reputacije proizvođača. • Ima POP3 Mail Scan koji provjerava da li ima virusa i neželjene pošte integrisane u klijentu. • Ima praćenje ponašanja klijenta (Behavior Monitoring) sa „In The Cloud“ provjerom da li je aplikacija poznata i bezbjedna (provjera na nivou starosti i zastupljenosti aplikacije). • Ima mogućnost vraćanja datoteka koje su stavljene u karantin kao sumnjive, centralno preko administratorske konzole i uz definisanje izuzetaka od		

		osnovu rezonovanja korisnika (unos razloga). • Podrška za ograničavanje opterećenja CPU-a prilikom zakazanog antimalver skeniranja (Scheduled Scan). • Integrisana podrška za distribuciju komponenti ažuriranja u scenarijima sa nižim propusnim opsegom (Update Relay). • Podrška za više izvora ažuriranja komponenti na osnovu IP adrese klijenta. • Verifikacija digitalnog potpisa MSI paketa prije instaliranja programa i mogućnost zabrane instalacije nepoznatih programa preuzetih preko Veb ili email kanala. • Automatska integracija sa rješenjem za otkrivanje naprednih prijetnji kroz Sandbox: automatska prevencija napada na krajnju tačku na osnovu informacija dobijenih od Sandbox-a (sumnjivi saobraćaj, promjene sistema itd.). • Podrška za rad sa nekoliko zasebnih korisnika/organizacija na istom sistemu (multi-tenancy). • Podrška za zaštitu Microsoft Windows (Server i Desktop) i MacOS, 32 i 64-bitne operativne sisteme.	budućeg karantina. • Ima mogućnost definisanja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) za praćenje ponašanja aplikacija , što uključuje sumnjive radnje kao što su: promjene u hosts fajlu, kreiranje duplikata poznatih sistemskih datotekeka, instaliranje novog dodatka za Internet Explorer, promjena podešavanja u Internet Explorer-u, promjena Windows Security Policy podešavanja, umetanje novog dll-a, stvaranje novog startup programa itd. Za svaku od ovih sumnjivih radnji ima mogućnost definisanja različitih odgovora: od blokiranja, preko upozorenja i logovanja do dozvole za rad. • Ima mogućnost definisanja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) za kontrolu pristupa eksternim uređajima na klijentu		

			(prenosivi medijumi povezani preko USB-a). • Ima blokiranje funkcije Autorun pri povezivanju USB diskova sa klijentom. • Ima kontrolu pristupa mrežnim resursima i dijeljenim diskovima (network shares). • Ima provjeru web saobraćaja, koja sprječava pokretanje zlonamjernih veb skripti i iskorišćavanje bezbjednosnih propusta u pretraživaču, u realnom vremenu. • Ima otkrivanje i evidentiranje aktivnosti C&C komunikacije sa granularnom konfiguracijom akcija po detekciji mrežne komunikacije prema C&C serverima. • Ima podršku za VDI okruženja (virtuelizacija desktopa): mogućnost ograničavanja potrošnje resursa virtuelnih radnih stanica na nivou host-a - VMware vCenter (VMware View), Citrix XenServer 5.5 (Citrix XenDesktop 4). Ima mogućnost prethodnog skeniranja Master VDI		

			image-a i kontrolisanog postavljanja komponenti za ažuriranje na pojedinačnim VDI host-ovima • Ima DLP dodatak koji se može naknadno uključiti, integrisan u identično administrativno okruženje sa sledećim funkcionalnostima: o mogućnost napredne kontrole USB uređaja prema proizvođaču (ID dobavljača, serijski brojevi) o Mogućnost napredne kontrole informacija poslatih preko perifernih uređaja (COM/LPT port, IEEE 1394, uređaji za obradu slike, modem, PCMCIA port, Bluetooth, mobilni uređaji, print screen) o Mogućnost kontrole sadržaja na različitim transportnim kanalima uključujući: elektronsku poštu (SMTP), Veb (HTTP, HTTPS), FTP i SMB protokoli o Kreiranje politika u zavisnosti od lokacije klijenta/računara. o Kontrola informacija kroz: unaprijed definisane politike koje		

			uključuju: PCI DSS pravila za otkrivanje prenosa brojeva kartica ili bankovnih računa; lične podatke kao što su OIB ili JMBG brojevi; izvorni kodovi često korišćenih programskih jezika i drugi; definisanje sopstvenih politika korišćenjem proizvoljnih ključnih riječi ili regularnih izraza. o Moguće radnje u slučaju kršenja pravila: blokiranje prenosa, omogućavanje prenosa sa evidentiranjem incidenata, prikazivanje poruke upozorenja korisniku sa opcijom da se dozvoli slanje. o Mogućnost provjere cijelog računara na osjetljive informacije, uz mogućnost evidentiranja pronađenih informacija. o Mogućnost propuštanja osjetljivih podataka na osnovu rezonovanja korisnika (unos razloga). • Ima podršku za ograničavanje opterećenja CPU-a prilikom zakazanog antimalver skeniranja (Scheduled Scan). • Ima		

			integrisanu podršku za distribuciju komponenti ažuriranja u scenarijima sa nižim propusnim opsegom (Update Relay). • Ima podršku za više izvora ažuriranja komponenti na osnovu IP adrese klijenta. • Ima verifikaciju digitalnog potpisa MSI paketa prije instaliranja programa i mogućnost zabrane instalacije nepoznatih programa preuzetih preko Veb ili email kanala. • Ima automatsku integraciju sa rješenjem za otkrivanje naprednih prijetnji kroz Sandbox: automatska prevencija napada na krajnju tačku na osnovu informacija dobijenih od Sandbox-a (sumnjivi saobraćaj, promjene sistema itd.). • Ima podršku za rad sa nekoliko zasebnih korisnika/organizacija na istom sistemu (multi-tenancy). • Ima podršku za zaštitu Microsoft Windows (Server i Desktop) i MacOS,		

			32 i 64-bitne operativne sisteme.		

6 POJAŠNJENJE PONUDE

Nema unijetih pojašnjenja ponude.