Kúpna zmluva

uzatvorená v zmysle ustanovenia § 409 a nasl. Obchodného zákonníka
a zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov

č. AOS – I-73/2018

Článok I.
Zmluvné strany

1.1. Predávajúci: airo, s.r.o.

Sídlo: **Ivanská cesta 30/B, 82104 Bratislava**
Zastúpený: Ladislav Liščák - konateľ
Ing. Štefan Kopaj – konateľ
Mgr. Jakub Čeles – konateľ
Vybavuje: Marek Gdovec, t.č. +421 903 733 886, email: marek.gdovec@airo.sk
IČO: 48286621
IČ DPH: SK2120122488
Bankové spojenie: Tatra banka, a.s.
IBAN: SK8211000000002941044557
BIC: ATRSKBX
Údaj o zápise: Zápis v obchodnom registri: Okresný súd Bratislava I, oddiel: Sro , vložka číslo 106156/B

(ďalej len „predávajúci“)

1.2. Kupujúci : Akadémia ozbrojených síl generála Milana Rastislava Štefánika

Sídlo: Demänová 393, 031 01 Liptovský Mikuláš 1
Zastúpený: doc. Ing. Jozef PUTTERA, CSc., rektor
Vybavuje: Ing. Martin DROPPA, t. č.: +421 903824480, e-mail: martin.droppa@aos.sk
IČO : 37 910 337
IČ DPH: SK2021872083
Bankové spojenie: Štátna pokladnica
IBAN: SK86 8180 0000 0070 0016 6299.
BIC: SPSRSKBA
Právna forma: Štátna rozpočtová organizácia

(ďalej len „ kupujúci“)

Článok II.

Predmet kúpnej zmluvy

2.1. Predávajúci sa na základe tejto zmluvy zaväzuje dodať kupujúcemu tovary a poskytnúť súvisiace služby (ďalej len „tovar“), ako je vyšpecifikované v prílohe č. 1 k tejto zmluve. Príloha č.1 tvorí neoddeliteľnú súčasť tejto zmluvy.

2.2. Predávajúci sa zaväzuje dodať tovar vyšpecifikovaný v prílohe č. 1 a zároveň sa zaväzuje previesť na kupujúceho vlastníckeho právo podľa podmienok tejto zmluvy.

2.3. Po odovzdaní tovaru predávajúci odovzdá kupujúcemu všetky potrebné dokumenty a podklady na jeho riadne používanie.

2.4. Zoznam osôb predávajúceho, zodpovedných za plnenie tejto zmluvy, v rozsahu meno, priezvisko, e-mailová adresa, telefónne číslo, funkcia a dokladom (certifikátom) o odbornej spôsobilosti tvorí prílohu č. 2. tejto zmluvy.

Článok III.
Cena a platobné podmienky

3.1. Cena za dodávaný tovar je stanovená na základe cenovej ponuky v zmysle zákona NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov, v jednotkových cenách vyšpecifikovaných v prílohe č. 1 k tejto zmluve. Výška ceny dodávaného tovaru predstavuje sumu 46 874,60 EUR (slovom Štyridsaťšesťtisícosemstosedemdesiatštyri eur šesťdesiat centov) bez DPH, 56 249,52 EUR (slovom Päťdesiatšesťtisícdvestoštyridsaťdeväť eur päťdesiatdva centov) s DPH.
Súčasťou ceny tovaru sú náklady spojené s balením a dopravou tovaru do miesta plnenia, inštaláciu a konfiguráciu tovaru a zaškolenie obsluhy, ako aj nákladov na všetky pomocné práce a materiál. Táto cena je pre obe zmluvné strany cenou záväznou.

3.2. Po prevzatí tovaru zástupcom kupujúceho v mieste plnenia, predávajúci vystaví faktúru a doručí ju na adresu kupujúceho: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Demänová 393, P. O. Box 9, 031 06 Liptovský Mikuláš 6, v dvoch výtlačkoch do 10 (slovom desať) dní po riadnom dodaní tovaru a vykonaní súvisiacich služieb.

3.3. Právo na zaplatenie ceny vzniká predávajúcemu riadnym splnením jeho záväzku spôsobom a v mieste plnenia v súlade s touto zmluvou.

3.4. Kupujúci uhradí oprávnenému účtovanú sumu do 30 dní odo dňa obdržania faktúry. Pre tento účel sa za deň úhrady považuje dátum odpísania z účtu kupujúceho platenej sumy na účet predávajúceho uvedený v čl. I bod 1.1 tejto zmluvy.

3.5. Kupujúci je oprávnený vrátiť bez zaplatenia faktúru, ktorá je nesprávna alebo neúplná, a to do dátumu jej splatnosti. Oprávneným vrátením faktúry prestáva plynúť doba splatnosti, táto začína plynúť znova odo dňa doručenia opravenej faktúry.

Článok IV Doba platnosti zmluvy

4.1. Zmluva sa uzatvára na dobu určitú, najneskôr do 31.12.2018.

Článok V.
Miesto a spôsob plnenia, dodacia lehota a dodacie podmienky

5.1. Miestom plnenia je sídlo kupujúceho.

5.2. Predávajúci sa zaväzuje dodať kupujúcemu tovar v lehote do 15.12.2018 dní od doručenia objednávky. Túto dobu je možno zmeniť len s písomným súhlasom oboch zmluvných strán.

5.3. Prevzatie tovaru v mieste plnenia bude potvrdené zástupcom kupujúceho na dodacom liste.

5.4. Predávajúci je povinný vyrozumieť o termíne dodania tovaru zástupcu kupujúceho najmenej tri pracovné dni pred jeho odovzdaním. Zástupca kupujúceho prezrie dodávaný tovar obvyklým spôsobom a prekontroluje jeho úplnosť.

Článok VI.
Množstvo a kvalita tovaru

6.1. Predávajúci je povinný dodať tovar v množstve, akosti a vo vyhotovení podľa článku II. Tejto zmluvy, spresnený v objednávke.

6.2. Predávajúci sa zaručuje, že tovar je novo vyrobený, doteraz nepoužívaný, a že zodpovedá požadovanej kvalite, požadovaným technickým parametrom, vyhovuje príslušným STN normám a je bez faktických a právnych vád.

6.3. Na dodávaný tovar sa vzťahuje záruka podľa záručných podmienok 24 mesiacov. Predávajúci zodpovedá za vady a nekompletnosť tovaru v plnom rozsahu. Kupujúci je povinný reklamovať vady tovaru v súlade s článkom VI. bod 6.7. a bod 6.8. tejto zmluvy.

6.4. Záručná doba začína plynúť dňom prevzatia tovaru zástupcom kupujúceho (v deň podpisu dodacieho listu v mieste plnenia).

6.5. Kupujúci je povinný používať predmet zmluvy – tovar v súlade s jeho určením a dodržiavať návody na použitie.

6.6. Záruka sa nevzťahuje na mechanické poškodenie tovaru spôsobené kupujúcim a poškodenie tovaru v dôsledku živelných pohrôm.

6.7. Kupujúci je povinný vady písomne oznámiť predávajúcemu bez zbytočného odkladu po ich zistení, najneskôr do uplynutia dohodnutej záručnej doby. V prípade uplatnenia reklamácie zo strany kupujúceho záručná doba prestáva plynúť a začína znova plynúť od nasledujúceho dňa po dni odovzdania vymeneného (opraveného) vadného tovaru.

6.8. Oznámenie o reklamácii musí byť písomné a musí obsahovať :

- názov, príp. druh reklamovaného výrobku, - popis vady,
- miesto kde sa reklamovaný tovar nachádza,
- číslo dodacieho listu,
- uplatňované nároky z vád tovaru.

6.9. Predávajúci sa zaväzuje vyriešiť oprávnenú reklamáciu do 30 dní odo dňa jej uplatnenia kupujúcim.

6.10. Nároky kupujúceho z vád tovaru budú uplatňované v súlade s § 436 a nasl. Obchodného zákonníka.

Článok VII.
Zmluvné pokuty a sankcie

7.1. V prípade, že predávajúci nedodrží lehotu pre dodanie tovaru dohodnutú v tejto zmluve, uhradí kupujúcemu zmluvnú pokutu vo výške 0,05 % z ceny nedodaného tovaru za každý deň omeškania. V prípade, že predávajúci z tohto dôvodu od zmluvy odstúpi, má kupujúci právo na zaplatenie zmluvnej pokuty vo výške rovnajúcej sa 10% ceny nedodaného tovaru.

7.2. V prípade omeškania kupujúceho s úhradou faktúry, sa tento zaväzuje zaplatiť predávajúcemu úrok z omeškania vo výške 0,05 % z neuhradenej sumy za každý deň omeškania.

7.3. V prípade, že predávajúci nevybaví uplatnenú reklamáciu v dobe dohodnutej v článku VI. bod 6.9. tejto zmluvy, uhradí kupujúcemu zmluvnú pokutu vo výške 33,- EUR (slovom tridsaťtri eur) za každý deň omeškania.

7.4. Zaplatením zmluvnej pokuty sa účastník porušujúci povinnosti vyplývajúce z tejto zmluvy (zakladajúce nárok na zmluvnú pokutu) nezbavuje zodpovednosti za spôsobenú škodu a

ani povinnosti túto nahradiť. Poškodený má právo domáhať sa náhrady škody presahujúcej aj zmluvnú pokutu.

7.5. Dohodnuté zmluvné pokuty a sankcie je povinná strana zaplatiť strane oprávnenej do 30 dní odo dňa ich uplatnenia.

Článok VIII.
Nadobudnutie vlastníckeho práva.

8.1. Kupujúci nadobúda vlastnícke právo k tovaru dňom jeho prevzatia v mieste plnenia a podpisom dodacieho listu a vlastnícke právo nadobúda pripísaním peňazí na účet dodávateľa.

Článok IX.
Osobitné dojednania

9.1. Nedodržanie záväzku dodať tovar v dohodnutom množstve, kvalite a termíne zo strany predávajúceho budú zmluvné stany považovať za podstatné porušenie kúpnej zmluvy (§ 345 ods. 2 Obchodného zákonníka).

9.2. V prípade ak predávajúci nedodrží lehotu plnenia dohodnutú v článku V. bod 5.2. tejto zmluvy ani po písomnom upozornení, má kupujúci právo od tejto zmluvy odstúpiť.

9.3. V prípade ak kupujúci nedodrží lehotu splatnosti faktúry dohodnutú v článku III. bod 3.4 tejto zmluvy ani po písomnom upozornení, má predávajúci právo od tejto zmluvy odstúpiť.

9.4. Predávajúci zabezpečí dodanie technickej dokumentácie a zaškolenie odborného pracovníka kupujúceho.

9.5. Kupujúci požaduje potvrdenie od Cisco (akceptovateľné je potvrdenie z krajín EU), že predložená ponuka má zaručenú autenticitu.

Článok X.
Záverečné ustanovenie.

10.1. Zmeny a doplnky tejto zmluvy je možno vykonávať iba formou písomnej dohody zmluvných strán, ktoré budú neoddeliteľnou súčasťou tejto zmluvy.

10.2. Zmluvné strany sa dohodli, že právne vzťahy vyplývajúce z tejto zmluvy sa riadia ustanoveniami Obchodného zákonníka.

10.3. Táto zmluva nadobúda platnosť dňom jej podpísaním zástupcami obidvoch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v súlade s § 47 a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.

10.4. Táto zmluva sa povinne zverejňuje v súlade so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

10.4. Zmluva je vyhotovená v piatich rovnopisoch, jeden rovnopis obdrží predávajúci, štyri rovnopisy kupujúci.

Za predávajúceho :

V Bratislave, dňa ….. 2018

Ladislav Liščák – konateľ
Ing. Štefan Kopaj - konateľ
Mgr. Jakub Čeles – konateľ

Za kupujúceho :

V Liptovskom Mikuláši, dňa ….. 2018

---

doc. Ing. Jozef PUTTERA, CSc.
rektor

Akadémia ozbrojených síl
generála Milana Rastislava Štefánika

Príloha č. 1 k č. AOS-
Počet listov:

Špecifikácia predmetu plnenia

P.č.	Názov parametra	Jednotka	Cena bez DPH v EUR	DPH v EUR	Cena s DPH v EUR
1	Systém pre centralizované ukladanie a správu logov	1 ks	27 190,60 €	5 438,12 €	32 628,72 €
2	Systém pre monitorovanie a ochranu sieťovej komunikácie	1 ks	19 684,00 €	3 936,80 €	23 620,80 €
Celkom za tovar:			**46 874,60 €**	**9 374,92 €**	**56 249,52 €**

Technická špecifikácia predmetu zákazky:

P. č.	Predmet plnenia	Požiadavky
1.	Systém pre centralizované ukladanie a správu logov: - LOGmanager-M - 5 rokov HW support, - 1 rok SW renewal, - 1x LOGmanager-VF, - 12 TB database	Všeobecné požiadavky: • Systém pracuje ako appliance s jedným uceleným rozhraním pre všetky administrátorské i operátorské činnosti. Nevyžaduje inštaláciu ďalších systémov a aplikácií okrem podpory zberu na iných lokalitách a agenta pre zber Windows logov. • Systém vykonáva spracovanie udalostí z preddefinovaných zdrojov logov aplikácií, operačných systémov a sieťového hardware minimálne v rozsahu podľa zoznamu podporovaných zariadení. • Systém umožňuje doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo zoznamu uvedeného v bode 2 užívateľom bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému - Užívateľsky definované parsery. Dokumentácia systému musí obsahovať prehľadný návod na vytváranie zákazníckych parserov a systém musí obsahovať možnosť testovania a ladenia zákazníckych parserov bez vplyvu na ostatné produkčné funkcie systému. • Parsery a alerty musia umožňovať použitie matematických operácií.

		• Parsery a alerty musia podporovať dekódovanie URL. • Systém prijíma a spracováva logy, udalosti a ďalšie strojovo generované dáta prostredníctvom minimálne nasledujúcich protokolov: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovane) a TCP 20515 (RELP, šifrovane). Systém musí umožňovať príjem logov i na užívateľsky definovaných UDP a TCP portoch. Prijaté logy systém štandardizuje do jednotného formátu a logy sú normalizované - rozdeľované do príslušných polí podľa ich typu. Zároveň systém uchováva i originálne verzie logov. • Systém zachováva pôvodnú informáciu zo zdroja logu o časovej značke udalosti, ale vytvára aj vlastnú dôveryhodnú časovú značku ku každému logu, ktorou sa systém defaultne riadi. • Všetky polia a položky prijaté systémom sú automaticky indexované. Nad všetkými položkami je možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom. • Možnosť zberu udalostí minimálne vo formátoch RAW, Syslog, CEF, LEEF, JSON RFC7159. • Systém nesmie umožniť mazanie alebo modifikovanie uložených logov. Každý log musí mať unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu. • Systém musí umožňovať prijatú správu rozhodnutím konfigurácie alebo parseru zahodiť. • Systém vykonáva centralizovanú konsolidáciu logov. • Systém umožňuje jednoduché vyhľadávanie udalostí (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. • Systém vykonáva ucelenú vizualizáciu logov, udalostí a strojových dát (grafy udalostí). Vizualizácia musí byť dynamická, t.j. voľbou v jednom grafe sa ostatné príslušné grafy v pohľade na dáta upravia podľa požadovanej voľby automaticky. • Systém umožňuje jednoducho vytvárať grafické znázornenie TOP udalostí nad všetkými dátami za určité časové obdobie.

		• Systém vykonáva automatické doplňovanie GeoIP informácií k udalostiam a ich grafické znázornenie na mape bez nutnosti využívať služby tretích strán či externé aplikácie. • Systém vykonáva automatické doplňovanie reverzných DNS záznamov k IP adresám. • V prípade preťaženia systému nesmie dôjsť k strate logov. Všetky prijaté nespracované logy/udalosti musia byť ukladané do vyrovnávacej pamäte. Pri výraznejšom plnení vyrovnávacej pamäte musí byť administrátor systému automaticky informovaný. Veľkosť vyrovnávacej pamäte nesmie byť nižšia ako 50 GB. • Systém umožňuje unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení. • Systém musí mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie. • Systém obsahuje reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov. Pre vytváranie nových pohľadov na dáta nie je požadované používať povinne SQL jazyk. • Systém obsahuje predpripravené pohľady na uložené dáta podľa jednotlivých kategórií zdrojových zariadení i podľa logického členenia. • Systém podporuje a automatizuje priebežné aktualizácie reportov a pohľadov výrobcom. • Konfiguračné a systémové rozhranie a dokumentácia musia byť identické v anglickom i v slovenskom alebo českom jazyku. • Systém musí umožňovať kapacitnú i výkonovú škálovatelnosť. • Čistá kapacita úložného priestoru (kapacita diskového poľa) dostupná pre uložené dáta ponúkaného systému musí byť minimálne 12TB. • Pre diskový subsystém je požadované prevedenie hot-swap, t.j. zo systému musí byť možné vyňať ľubovoľný disk bez straty dát a vplyvu na funkčnosť riešenia. Redundancia diskov nesmie ovplyvňovať požadovanú kapacitu úložiska. • Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe

		systému, preposlanie upozornenia pomocou SMTP alebo Syslog. • Systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, MRTG a pod.) • Systém musí umožňovať autorizovaný prístup k štruktúrovanej databáze logov. • Jednotná centrálna webová konzola pre prístup k logom, alertom, reportom a pre správu systému. Z tejto konzoly sa vykonáva kompletná konfigurácia, správa a analýza logov. Nepripúšťa sa, aby dodaný systém mal viacero konzol pre jednotlivé časti systému. • Systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému. • Systém musí vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní. Jedinou prípustnou výnimkou je monitorovanie systémov Windows (WMI protokol). • Systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Minimálne HW parametre: • 1x HW appliance v rackovom prevedení s výškou max. 1U, vrátane ramena pre organizáciu zapojených káblov umožňujúceho vysunutie zapnutého systému z racku pre servisné účely. • HW appliance obsahuje všetky potrebné komponenty (CPU, RAM, diskový priestor) a je nezávislá na ďalších systémoch. • Min. 1 procesor (min. 10 jadier), podpora HyperThreadingu. • Min. 64GB DDR-4, rozšíriteľná na min. 768GB pre jeden CPU. • Diskový subsystém s čistou dostupnou kapacitou minimálne 12TB pre integrovanú databázu; HW akcelerovaný SAS RAID radič s read-write cache min. 2GB. Radič diskového poľa musí obsahovať zálohovaciu batériu alebo byť vybavený flash pamäťou.

		• Pre diskový subsystém je požadované prevedenie hot-swap diskov zapojených v RAID5. • Minimálne 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pre management HW. • Redundantné ventilátory, vymeniteľné za chodu. • Napájacie zdroje s redundanciou 1+1, vymeniteľné za chodu, účinnosť min. 94% • Virtuálne KVM, tj. prevzatie textovej i grafickej konzoly serveru a prenos povelov z klávesnice a myši vzdialeného počítača. • Servisný procesor alebo karta pre systémový manažment HW poskytujúca podporu vzdialeného manažmentu servera cez internet alebo intranet pomocou bezpečnej kryptovanej komunikácie (SSL, SSH, AES, 3DES), podporu štandardu IPMI 2.0, samotný dedikovaný sieťový 1Gb port. Požadujú sa aj rozšírené funkcie ako : o podpora grafického rozhrania, o dvojitá autentifikácia s integráciou do adresárovej služby (MS AD), o podpora záznamu a spätného prehrávania bootovacej obrazovky. • Dodávateľ musí predložiť potvrdenie vystavené autorizovanou osobou o zhode, že ponúkaný systém spĺňa požiadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov. Toto potvrdenie nie je možné nahradiť certifikátom na spoločnosť dodávateľa (subdodávateľa) alebo výrobcu ponúkaného systému. Nie je ho možné nahradiť ani čestným vyhlásením. Výkonnostné a SW parametre: • Systém funguje formou appliance - všetky časti systému je možné nastaviť v centrálnej správcovskej konzole, nie je nutné editovať žiadne konfiguračné súbory vrátane IP adresácie systému. • Aktualizácie systému sú distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. • Systém musí podporovať downgrade, (možné problémy s novou verziou systému po upgrade). • Priemerný trvalý príjem min. 2000 udalostí za sekundu.

		• Špičkový príjem 4000 udalostí za sekundu po dobu najmenej 10 minút, v prípade vyššieho počtu udalostí ich systém musí byť schopný uložiť do bufferu a spracovať neskôr. • Licenčne neobmedzený počet zariadení pre príjem zasielaných udalostí. Licenčne neobmedzený počet udalostí v GB za deň alebo licencia na minimálne 80GB uložených udalostí za deň. Integrovaná databáza musí mať čistú veľkosť najmenej 12 TB a musí podporovať kompresiu ukladaných dát. • Užívateľská konfigurácia vlastných parserov pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej webovej konzole. Vizuálny programovací jazyk musí užívateľovi umožniť písať vlastné parsery bez nutnosti znalosti programovania (napr. Node-RED, Microsoft VPL, Blockly apod). Vizuálny programovací jazyk nie je prezentovaný textovo, ale graficky formou blokov, ktoré obsahujú aplikačnú logiku. • Konfigurácia užívateľských parserov musí umožňovať automatické doplňovanie DNS reverzných záznamov, GeoIP informácie a identifikáciu výrobcu zariadenia podľa MAC adresy. • Systém musí podporovať integráciu externých zdrojov informácií. • Možnosť on-line ladenia užívateľsky definovaných parserov - pri ich vytváraní je možné vložiť vlastné testovacie správy, pri zmene je okamžite zobrazená výsledná podoba rozparsovaných dát a prípadné chybová hlásenia. • V centrálnej správcovskej konzole je možné pridávať k jednotlivým zdrojom dát, aplikáciám, zariadeniam alebo IP subnetom tzv. značky, označujúce umiestnenie zariadenia, typ zariadenia, kritickosť zariadenia a pod. • V centrálnej správcovskej konzole je pri definícii vlastného parseru možné pridávať značky pre typy udalostí (login, logout apod.). • Všetky pridávané značky sú ukladané s každou prijatou udalosťou, na základe značky je možné filtrovať dáta alebo

		obmedzovať oprávnenia užívateľov systému k jednotlivým udalostiam. • Systém musí byť predpripravený pre zrkadlenie a clustrové zapojenie – 2 nody v režime active / active. • V prípade zapojenia ako dvojnodový cluster sa systém správa ako jeden celok. • V prípade využitia dvoch nodov v clustri sa zrýchľuje vyhľadávanie a sú automaticky prehľadávané všetky dáta na všetkých zariadeniach v clustri. • V prípade rozšírenia systému na dvojnodový cluster musia zariadenia odosielať udalosti iba na jednu virtuálnu adresu a zároveň cluster musí zaisťovať synchronizáciu udalostí medzi nodmi. • Podpora zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém. Alerty systému: • Systém na základe zadaných podmienok splnených v prijatých dátach vygeneruje alerty. • Text alertu môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti. • Predpripravené sety/vzory alertov výrobcom systému. • Užívateľská konfigurácia alertov pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nie je prezentovaný textovo, ale graficky formou blokov, ktoré obsahujú aplikačnú logiku. • Ako výstupné pravidlo alertu musí systém vedieť odoslať udalosť, ktorá alert vyvolala na externý systém minimálne prostredníctvom SMTP alebo Syslog cez TCP protokol. • V alertoch je možné využívať značky (napríklad: pošli alert iba v prípade, že sa udalosť stala na kritickom serveri, ktorý beží v lokalite XY). • Systém podporuje základné funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Zber udalostí v prostredí Microsoft: • Udalosti z prostredia Microsoft sú získavané pomocou agenta inštalovaného priamo na koncovom Windows systéme. Windows agent musí súčasne podporovať

		ako monitoring interných windows logov, tak i monitoring textových súborových logov. • Agent zabezpečuje zber nemodifikovaných udalostí a detailné spracovávanie auditných informácií. • Agent podporuje nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly. • Filtrácia odosielaných udalostí agentom sa konfiguruje pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nie je prezentovaný textovo, ale graficky formou blokov, ktoré obsahujú aplikačnú logiku. • Windows agent nevyžaduje administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizácia Windows agenta sa nevykonáva z Group Policy. • Agent automaticky prekladá zástupné kódy v správach na text (napr. Logon Type 2 = Interactive, Logon Type 3 = Network, atď.). • Windows agent má buffer pre prípad straty spojenia medzi koncovým systémom a centrálnym úložiskom logov. • Komunikácia Windows agenta a centrálneho systému musí byť šifrovaná. • Windows agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale je možné z centrálnej správcovskej konzoly nastaviť i zber všetkých ostatných logov v zložke Protokoly aplikácií a služieb. • Windows agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v Prehliadači udalostí (Event Viewer) na koncovom systéme. • Počet inštalácií Windows agenta nesmie byť licenčne obmedzený. • Podpora pre zber udalostí z iných lokalít. • Systém musí obsahovať riešenie, ktoré zbiera udalosti na pobočkách alebo v záložnom datacentre a umožňuje ich odoslanie po saturovanej linke bez straty dát.

		• Systém musí podporovať centralizovanú správu pre zber udalostí z viacerých lokalít priamo z centrálneho úložiska dát. • Riešenie pre zber udalostí z iných lokalít musí byť schopné automaticky nadviazať spojenie s centrálnym úložiskom dát a prenášané dáta šifrovať. V prípade výpadku spojenia medzi inou lokalitou a centrálou musí spojenie automaticky obnoviť. • Riešenie musí komunikovať po definovanom IP protokole, aby mohla byť centrálne nastavená kvalita služby (QoS) pre prenos udalostí. • Riešenie musí poskytovať kapacitu vyrovnávacej pamäte pre minimálne 100GB udalostí, ktoré na inej lokalite môžu vzniknúť počas výpadku spojenia medzi inou lokalitou a dátovým centrom. • Riešenie pre zber udalostí z iných lokalít musí mať výkon minimálne 5 tisíc udalostí /s. a to i pri trvalej záťaži. • Riešenie pre zber udalostí z iných lokalít musí poskytovať podporu pre UDP i TCP zdroje a pre aktívny zber z Windows agentov. • Riešenie pre zber udalostí z iných lokalít musí byť poskytované ako fyzický systém aj ako virtuálny systém pre VMware ESXi a Hyper-V. Výber fyzického alebo virtuálneho riešenia je voliteľný na základe možností dostupných na predmetnej vzdialenej lokalite podľa voľby obstarávateľa. • Riešenie pre zber udalostí z iných lokalít musí byť schopné komunikovať s centrálou i cez viacnásobný preklad adries (NAT). Podpora • HW - požadovaná je min. 5-ročná servisná podpora na hardware appliance, oprava s garantovanou odozvou nasledujúci pracovný deň na mieste inštalácie, náhradné diely dostupné minimálne 5 rokov. Dodávateľ je povinný priamo pri dodávke predložiť certifikát o platnosti záruky poskytovanej výrobcom na požadované obdobie a zároveň poskytnúť linku na webový nástroj pre overenie záruky poskytovanej výrobcom • Požadované predplatné SW modulov systému vrátane aktualizácií systému a parserov na 1 rok. Podpora musí obsahovať

		aktualizáciu SW minimálne 4x ročne, opravy chýb a telefonická a emailová podpora s diagnostikou. Predplatné SW modulov systému vrátane aktualizácií systému a parserov dostupné ako platená služba minimálne 5 rokov bez nutnosti výmeny HW appliance za novšie prevedenie. Zdroje logov • Dodávaný systém musí podporovať zber logov min. z nasledujúcich zariadení a systémov: AD, Checkpoint FW, AsyncOS, Cisco LAN switch, Exchange server, TM DDI (trend micro deep discovery inspector) , ESET management, Cisco WLC Wifi, Cisco Prime, Cisco VoIP, E-learning. • Požadovaná retencia logov udalostí pre okamžité spracovanie systémom pre uvedené počty zariadení pri predpokladanej silnej prevádzke 12 hodín počas 5 dní v týždni je min. 300 dní. Systém musí zároveň archivovať staršie záznamy na externé médium s možnosťou pripojenia a prehľadávania archívov po dobu 10 rokov. Služby: • Súčasťou dodávky systému pre centralizované ukladanie a správu logov sú jednorazové implementačné služby minimálne v nasledujúcom rozsahu: o nastavenie a konfigurácia systému v IT prostredí obstarávateľa, o konfigurácia Windows systémov pre zasielanie logov do systému, o overenie funkčných a výkonových parametrov Windows agentov, o predvedenie vytvorenia a uloženia vlastného dashboardu a reportu, o predvedenie vytvorenia a uloženia užívateľsky definovaného parseru, o predvedenie nastavenia značkovania udalostí a vytvárania upozornení s limitom alebo koreláciou, o nastavenie a predvedenie odoslania udalosti, ktorá vyvolala alert na externý Syslog server cez TCP protokol, o nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom obstarávateľa, o zaškolenie obsluhy a správy systému pre min. 2 zamestnancov

		obstarávateľa pre roly administrátor, supervízor, operátor, o vytvorenie a odovzdanie prevádzkovej dokumentácie systému.
2.	Systém pre monitorovanie a ochranu sieťovej komunikácie: - Dve (2) fyzické zariadenia Palo Alto - Networks PA-850 zapojené v clustri, vrátane predplatného modulov Threat Prevention, - PANDB URL filtering a WildFire	Všeobecné požiadavky: • Systém pre monitorovanie a ochranu sieťovej komunikácie musí byť schopný identifikovať používateľov na základe Active Directory, MS Exchange, Citrix, LDAP, Terminal Services, agentom na koncových staniciach, XML API vrátane integráciou nástrojov tretích strán, web portál, regex parsing syslogových správ - musí voliteľne fungovať ako prijímač syslog správ. • Identifikácia používateľov pomocou Microsoft AD musí byť možná aj bez klienta na koncových zariadeniach. • Identifikácia používateľov pomocou Microsoft AD bez nutnosti inštalácie klienta na doménové kontrolery. Agent pre komunikáciu s AD musí byť zabudovaný priamo v systéme pre monitorovanie a ochranu sieťovej komunikácie. Systém pre monitorovanie a ochranu sieťovej komunikácie musí podporovať min. 99 doménových kontrolerov. • Systém musí mať podporu min. pre 3 rôzne Microsoft AD domény súčasne. • Riešenie musí podporovať agenta pre identifikáciu používateľov pre OS Microsoft Windows, Mac OS X, Linux, Android a iOS. Ten istý agent musí fungovať aj ako VPN klient. • VPN klient musí podporovať zmenu hesla pre AD užívateľa pri exspirácii hesla v AD. • Systém musí obsahovať agenta pre identifikáciu používateľov na Microsoft a Citrix terminal serveroch. • Politiky systému musia obsahovať aspoň tieto rozhodovacie kritériá: src/dst zóna, src/dst adresa, port/protokol, src user/group, aplikácia, web filtering kategória. • Systém musí umožňovať logovanie spojení definovateľné per politika a taktiež odosielanie logov cez syslog, email, http, snmp na systém pre centralizované ukladanie a správu logov definovateľné politikou. Systém pre monitorovanie a ochranu sieťovej komunikácie musí

		umožňovať oddelené zapnutie a vypnutie logovania na začiatku spojenia a po ukončení. • Systém musí podporovať autentifikáciu používateľov pomocou sekvencií. Požadovaná je možnosť definovať minimálne 3 typy autentifikácií v rámci jedného autentifikačného profilu, napr. LDAP, Radius, lokálna DB v rámci systému pre monitorovanie a ochranu sieťovej komunikácie. • Systém musí mať integrovaný systém ochrany proti sieťovým útokom (IPS). Databáza signatúr IPS musí byť uložená priamo na zariadení. Aplikácia IPS profilu na prechádzajúcu komunikáciu musí byť konfigurovateľná. Databáza signatúr musí byť poskytovaná výrobcom systému pre monitorovanie a ochranu sieťovej komunikácie. • Systém musí mať natívne integrovaný systém detekcie a riadenia aplikácií bez nutnosti zapnutia tejto funkcionality v separátnom module. Systém musí byť schopný detegovať aplikácie nezávisle na použitom porte/protokole. Taktiež musí umožňovať vytvorenie vlastných signatúr pre aplikácie priamo cez webové rozhranie. Aplikácie musia byť identifikované priamo v systéme pre monitorovanie a ochranu sieťovej komunikácie a musia byť jedným z rozhodovacích kritérií v rámci bezpečnostných politík. • Systém musí umožňovať riadenie aplikácií na základe "the Principle of Least Privilege", to znamená že systém musí byť schopný blokovať všetky aplikácie okrem tých ktoré sú explicitne povolené v rámci politík. • Systém musí byť schopný dekryptovať SSL pre odchádzajúcu aj prichádzajúcu komunikáciu a musí byť schopný zablokovať exploity (IPS), vírusy a škodlivý kód (AntiVirus a AntiSpyware) v rámci SSL komunikácie. Systém musí umožňovať vytvorenie výnimiek z SSL dekryptovania minimálne na základe URL kategórie. • Systém musí mať funkcionalitu SSL mirror portu, ktorou je schopný posielať dekryptovanú prevádzku na externé

		systémy (DLP) bez použitia ICAP protokolu. • Systém musí byť schopný dekryptovať SSH s možnosťou blokovania SSH tunneling-u na základe selektívnych politík. • Systém musí umožňovať blokovanie súborov na základe typu (filetype) a obsahu. Systém musí tiež obsahovať ochranu proti úniku citlivých dát (DLP) minimálne na úrovni pattern matching (regexp). • Systém musí umožňovať kontrolu prechádzajúcej komunikácie na prítomnosť vírusov a škodlivého kódu. Databáza signatúr musí byť uložená priamo na zariadení. AV databáza musí byť poskytovaná výrobcom systému pre monitorovanie a ochranu sieťovej komunikácie. AV musí byť schopný kontrolovať minimálne nasledovné protokoly: SMTP, POP3, IMAP, HTTP, HTTPS, FTP. • Systém musí obsahovať funkcionalitu DNS sinkholing, ktorá umožňuje detegovať infikovanú koncovú stanicu na základe DNS dotazov na známe malware domény. • Systém musí byť schopný zabrániť zero-day útokom na základe typu a obsahu komunikácie ako aj na základe aplikácie a používateľa. Je požadovaná pokročilá detekcia pomocou lokálneho alebo externého/cloud-based sandbox systému. Tento systém musí byť poskytovaný výrobcom systému pre monitorovanie a ochranu sieťovej komunikácie a musí poskytovať updaty signatúr pre AV, URL kategórií, DNS, C&C. Externý cloud-based sanbox musí byť fyzicky umiestnený na území Európskej únie. Externý sandbox musí byť schopný vytvárať vírusové a DNS signatúry do 10 minút, s minútovými aktualizáciami. • Systém pre monitorovanie a ochranu sieťovej komunikácie musí poskytovať možnosť obmedzenia šírky pásma na základe src alebo dst IP, protokolu, user identity, aplikácie a času (od – do, dni v týždni, dni v týždni + čas, atd.) • Systém musí byť schopný blokovať komunikáciu na adresy riadiacich centier botnetov.

		• Systém musí poskytovať ochranu pred DoS útokmi aspoň na úrovni limitovania počtu súčasných spojení per source alebo destination IP, user identity a aplikácie. • Systém musí byť schopný integrácie s poskytovateľmi Indicators of compromise (IOC, napr. TOR exit addresses) tretích strán. Tieto IOC musí byť systém pre monitorovanie a ochranu sieťovej komunikácie schopný použiť v politikách a blokovať. • Systém musí byť schopný integrácie s poskytovateľmi poskytujúcimi IP NetBlocks napr. Google NetBlock, Office365 NetBlocks atď., ktoré musí byť tento systém schopný použiť v politikách. • Systém umožňuje vytvoriť prehľad o aktivite vybraného používateľa alebo skupiny používateľov v posledných niekoľkých dňoch. Prehľad sa musí dať vytvoriť priamo na systéme pre monitorovanie a ochranu sieťovej komunikácie, bez pridaných externých zariadení v tabuľkovej alebo grafickej podobe. • Systém musí mať integrovanú ochrana proti botnetom - reputácia IP adries, DNS a URL záznamov. • Systém umožňovať riadenie prístupu na web stránky podľa kategórií a užívateľských identít. URL databáza musí obsahovať min. 63 kategórií (kategórie definované užívateľom sa do požadovaného počtu nezahŕňajú), pričom je požadované, aby systém obsahoval minimálne kategórie: malware, spam, private-ip-addresses a proxy avoidance , phishing resp. kategórie s týmto obsahom. URL databáza musí byť poskytovaná výrobcom systému pre monitorovanie a ochranu sieťovej komunikácie. • Systém musí umožňovať blokovanie zadávania doménových užívateľských mien a hesiel na základe URL kategórie ako ochrana proti phishingu. • Aplikačná kontrola musí byť natívnou funkciou systému pre monitorovanie a ochranu sieťovej komunikácie, bez nutnosti špecifického zapnutia tejto funkcionality.

		• Kontrola a rozpoznávanie min. 2500 rôznych aplikácií (napríklad Skype, Tor, BitTorrent, eMule, UltraSurf atď.). • Pre identifikáciu aplikácie nesmie byť potrebné v konfigurácii zariadenia definovanie počtu alebo rozsahu portov, na ktorých je aplikácia identifikovaná. Predpokladá sa, že všetky aplikácie možno nájsť na všetkých 65 535 dostupných portoch. Výkon brány musí byť rovnaký ako pri plnom duplexe a nesmie byť menej ako 1,9 Gbps. • Nie je dovolené blokovať aplikácie (P2P, IM, atď.) prostredníctvom iných ochranných mechanizmov ako je systém pre monitorovanie a ochranu sieťovej komunikácie. • Možnosť vytvorenia vlastných signatúr aplikácií priamo cez webové rozhranie systému pre monitorovanie a ochranu sieťovej komunikácie. • Systém pre monitorovanie a ochranu sieťovej komunikácie musí podporovať možnosť blokovania SaaS home/personal aplikácií, napr. Office365 Home/Personal a zároveň povolenie tej istej korporátnej aplikácie napr. Office 365 Business. • Pokročilá ochrana pred vírusmi, trojskými koňmi a spyware schopná detegovať, odhaliť, sledovať a zastaviť cielené aj náhodné hrozby. Minimálne HW parametre: • Systém pre monitorovanie a ochranu sieťovej komunikácie musí byť dodaný ako dve (2) HW appliance v zapojení vysokej dostupnosti (HA cluster) s možnosťou výberu režimu Active-Active alebo Active-Passive a možnosťou zmeniť tento režim kedykoľvek. HW aj SW súčasti systému pre monitorovanie a ochranu sieťovej komunikácie musia byť poskytované rovnakým výrobcom vrátane všetkých databáz (ako napr. antivírus, IDS/IPS, URL DB a pod.). • Komunikačné porty - min. 4x 10/100/1000 + 4x SFP 1 Gbps + 4x SFP+ 10 Gbps pre každé fyzické zariadenie clustra. • Min. 1 dedikovaný port pre OOB manažment pre každé fyzické zariadenie clustra.

		• Min. 1 konzolový port pre každé fyzické zariadenie clustra. • Napájanie 2x redundantný zdroj AC 230V pre každé fyzické zariadenie clustra. • Interný storage systému pre monitorovanie a ochranu sieťovej komunikácie pre ukladanie interných logov musí mat kapacitu minimálne 240GB a technológiu SSD pre každé fyzické zariadenie clustra. • Zariadenia musia byť dodané s montážnymi koľajnicami pre štandardný 19" rack, umožňujúcimi bezproblémovú manipuláciu a prístup k zariadeniam. • Systém pre monitorovanie a ochranu sieťovej komunikácie musí podporovať najmenej 5 virtuálnych smerovačov so samostatnými smerovacími tabuľkami a umožňuje spustiť viac než jednu smerovaciu tabuľku v jednej inštancii bezpečnostného systému pre každé fyzické zariadenie clustra. • Management systému pre monitorovanie a ochranu sieťovej komunikácie platformy musí byť fyzicky oddelený, musí používať vyhradené CPU (jadrá), RAM, NIC. • Priepustnosť systému riadenia s aplikačnou kontrolou min. 1,9 Gbps. • Priepustnosť systému riadenia FW + AV +IPS + Aplikačná kontrola min. 780Mbps s full-duplex. • Min. počet súbežných spojení: 192 000. • Min. počet nových spojení za sekundu: 9 500. • Priepustnosť IPSEC protokolu min. 500Mbps. • Minimálny počet IPSEC tunelov: 2000. • Systém pre monitorovanie a ochranu sieťovej komunikácie musí umožňovať secure remote access pomocou SSL VPN. Počet súčasných SSL VPN používateľov min. 1000 • Systém pre monitorovanie a ochranu sieťovej komunikácie musí mat podporu agregáciu portov (802.1ad) Sieťová funkcionalita: • Všetky sieťové porty, s výnimkou manažment portu a dedikovaných HA portov musia byť konfigurovateľné do režimu routeru (t. j. vo 3. vrstve modelu OSI), prepínacieho režimu (t.j. vo 2. vrstve

		modelu OSI), transparentného režimu a do režimu pasívneho počúvania (sniffer). Porty v nastavenom transparentnom režime nemôžu mať Layer 2 a 3 adresy, rovnako ako nemôžu zaviesť segmentáciu siete do samostatných kolíznych domén v zmysle Ethernet / CSMA. Porty v nastavenom transparentnom režime musia preposielať všetku non-ip prevádzku. • Systém pre monitorovanie a ochranu sieťovej komunikácie musí podporovať protokol Ethernet s podporou VLAN s označením IEEE 802.1q. Sieťové rozhrania pracujúce v transparentnom režime L2 a L3 musia umožňovať vytváranie tagov VLAN. Zariadenie musí podporovať 4000 VLAN. • Systém musí podporovať rôzne módy pre sieťové rozhrania: L2 (transparent), L3 a tap (sniffer) mod aj pre IPV6. • Podpora NAT módov (IPv4): Static IP, dynamic IP, dynamic IP and port (port address translation) , NAT64. • Zariadenie musí podporovať dynamické routing protokoly RIP, OSPF, OSPFv3, BGP, PIM a IGMP. Riešenie musí podporovať virtuálne routovacie tabuľky - min. 5. • Zariadenie musí podporovať policy based forwarding založený nie len na zdrojových IP ale aj na používateľoch alebo skupinách používateľov a na aplikáciách. • Zariadenie musí podporovať PPPoE. • Systém pre monitorovanie a ochranu sieťovej komunikácie musí mať stavovú synchronizáciu TCP, UDP a NAT spojení. Manažment systému: • Zabezpečovací modul systému pre monitorovanie a ochranu sieťovej komunikáciel musí vykonávať správu sieťového pásma (QoS) v rámci označovania balíkov so značkami DiffServ, ako aj nastavenie priority, maximálnej šírky pásma a garantovanej šírky pásma pre ľubovoľnú aplikáciu. Systém musí umožniť vytvorenie minimálne 8 tried pre rôzne typy sieťovej prevádzky. • Riešenie musí umožňovať konfiguráciu bezpečnostných politík z centrálnej správcovskej konzoly cez GUI rozhranie na ľubovoľnom zariadení v clustri, pričom

		prevedené zmeny sa automaticky replikujú na druhé zariadenie. Pravidlá z centrálneho managementu môžu byť definované ako nadradené alebo podradené k lokálnym pravidlám. • Riešenie musí umožňovať vzdialené pripojenie k zariadeniu pomocou SSH alebo HTTPS protokolu. • Systém musí byť schopný pracovať v konfigurácii zabezpečenej proti výpadkom v režime Active-Passive alebo Active-Active. Modul ochrany proti prerušeniu prevádzky musí monitorovať a zistiť poškodenie hardvérových a softvérových komponentov bezpečnostného systému a sieťových prepojení. • Systém musí umožňovať porovnávanie zhromaždených informácií a vytvárať reporty založené na nich. Zhromaždené údaje musia obsahovať min. informácie o sieťovej prevádzke, aplikáciách, hrozbách a filtrovaní webových stránok. • Systém musí umožňovať vytváranie reportov, prispôsobovať ich požiadavkám, uložiť ich v systéme a spúšťať ručne alebo automaticky v konkrétnych časových intervaloch. Výsledok správ musí byť k dispozícii min. vo formátoch PDF, CSV a XML. • Systém musí podporovať debugovanie problémových scenárov na úrovni L2 - L7. Musí tiež obsahovať tcpdump-like utilitu ktorá bude produkovať výstup v pcap formáte. Tcpdump-like utilita musí byť súčasťou webového rozhrania. • Systém musí podporovať možnosť konfigurácie cez XML API a taktiež možnosť zálohovania konfigurácie cez XML API. • Systém musí podporovať automatický denný export logov cez SCP a FTP. Podpora: • Požadovaný je licenčný model funkčných modulov per zariadenie (nelimitovaný počtom užívateľov) zabezpečujúci funkčnosť min. 1 rok vrátane nároku na najnovšie signatúry. Súčasťou dodávky musia byť predplatné pre moduly základnej ochrany pred hrozbami, URL filtrovanie a Advanced Threat Protection - ochrana proti neznámym hrozbám a 0-day útokom.

		• HW záruka - Minimálne 3 roky telefonickej a technickej podpory výrobcu s nahlásením poruchy 5 dní v týždni, 8 hodín denne, vrátane nároku na najnovší firmvér a softvér. • Výmena poškodeného zariadenia musí byť vykonaná do 3 pracovných dní. Služby: • Súčasťou dodávky systému pre monitorovanie a ochranu sieťovej komunikácie sú jednorazové implementačné služby minimálne v nasledujúcom rozsahu: o nastavenie a konfigurácia systému v IT prostredí obstarávateľa, o implementácia existujúcich bezpečnostných politík obstarávateľa, o zaškolenie obsluhy a správy systému pre min. 2 zamestnancov obstarávateľa pre roly administrátor, supervízor, operátor; vytvorenie a odovzdanie prevádzkovej dokumentácie systému.
3.	Súčasťou dodávky celého predmetu obstarávania je vzájomné prepojenie a integrácia systému pre centralizované ukladanie a správu logov a systému pre monitorovanie a ochranu sieťovej komunikácie.	

Zoznam osôb zodpovedných za plnenie zmluvy obsahujúci osoby a doložený nasledovnými certifikátmi:

- Minimálne jeden expert s platnou technickou certifikáciou výrobcu systému pre centralizované ukladanie a správu logov pre implementáciu a podporu uvedeného systému.

Ing. Rudolf Törvényi, rudolf.torvenyi@airo.sk, +421 903 570 391, technický špecialista, certifikát „LOGmanager System Expert - ID certifikátu: SWLGM50-20180718“
Ing. Štefan Kopaj, stefan.kopaj@airo.sk, +421 915 226 771, technický špecialista, certifikát „LOGmanager System Expert - ID certifikátu: SWLGM51-20180718“

- Minimálne jeden expert s platnou technickou certifikáciou výrobcu systému pre monitorovanie a ochranu sieťovej komunikácie pre implementáciu a podporu uvedeného systému.

Ing. Rudolf Törvényi, rudolf.torvenyi@airo.sk, +421 903 570 391, technický špecialista, certifikát „Palo Alto Networks Accredited Systems Engineer – Platform Professional - ID certifikátu: RWDDGHHC1JQQ13KF“