Smlouva o dílo

uzavřená dle ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, níže uvedeného dne, měsíce a roku, mezi:

AUTOCONT a.s.

Sídlo:	Hornopolní 3322/34, 702 00 Ostrava – Moravská Ostrava		
Jednající:	Lukáš Jurča, ředitel krajského obchodního zastoupení		
Bankovní spojení:	Česká spořitelna a.s.	číslo účtu:	6563752/0800
IČ:	04308697	DIČ:	CZ04308697
spisová značka OR:	B 11012 vedená u Krajského soudu v Ostravě		

na straně jedné (dále jen jako „zhotovitel“)

a

Vojenská nemocnice Olomouc

Sídlo: Sušilovo nám. 1/5, Klášterní Hradisko, 779 00 Olomouc

IČ: 608 00 691

Zastoupena: plk. gšt. v. z. MUDr. Martin Svoboda, ředitel

na straně druhé (dále jen jako „objednatel“)

(dále zhotovitel a objednatel jen jako „smluvní strany“)

I. Úvodní prohlášení

Smluvní strany prohlašují a činí nesporným, že tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „Technologie bezpečnostního monitoringu vnitřní sítě“.

(dále jen jako „veřejná zakázka“)

II. Dílo

Smluvní strany prohlašují a činí nesporným, že na základě této smlouvy se zhotovitel zavazuje provést pro objednatele na svůj náklad a nebezpečí dílo představující:

- dodávku systému pro pokročilý bezpečnostní monitoring síťové infrastruktury, který zajistí monitorování síťové infrastruktury v reálném čase s pokročilou inteligencí pro analýzu chování sítě a který optimalizuje chování aplikací a chrání systémy před moderními kybernetickými bezpečnostními hrozbami obcházejícími tradiční bezpečnostní prvky;
- dodávku prací, tj. implementace do technologického prostředí zadavatele (instalace, konfigurace, uvedení do provozu),

a to v souladu se zadávacími podmínkami veřejné zakázky, nabídkou zhotovitele, požadavky a účelem zadavatele, a dále technickou specifikací, která tvoří přílohu č. 1 této smlouvy, vymezující podrobněji dílo na základě této smlouvy, a objednatel se zavazuje řádně a včas provedené dílo převzít a zaplatit za něj zhotoviteli cenu.

(dále jen jako „dílo“)

III. Cena díla a platební podmínky

Smluvní strany prohlašují a činí nesporným, že:

a) celková cena díla činí 4.159.098 Kč (slovy: čtyřimilionyjednostopadesátdevěttisícdevadesátosm korun českých) a je nejvýše přípustná (nepřekročitelná) a platná a účinná po celou dobu provádění díla na základě této smlouvy, která zahrnuje mj. dodávku hardwaru a softwaru a dodávku prací včetně servisní podpory po dobu pěti let od protokolárního předání díla bez vad a nedodělků;

b) součástí ceny díla jsou i veškeré související vynaložené náklady (např. náklady na dopravu) nezbytné k řádnému a včasnému provedení díla s tím, že zhotovitel je oprávněn navýšit cenu díla o příslušnou sazbu DPH či jinou daň v souladu s platnými právními předpisy.

Objednatel prohlašuje a činí nesporným, že je povinen zaplatit zhotoviteli cenu díla na základě faktury – daňového dokladu, jejíž přílohou bude i předávací protokol ve smyslu čl. IV. písm. c) anebo d) této smlouvy, kterou je zhotovitel povinen vystavit v souladu s příslušnými právními předpisy bezodkladně po provedení díla bez vad a nedodělků, a to bezhotovostním převodem na bankovní účet zhotovitele č. 6563752/0800 se splatností 21 dnů ode dne jejího vystavení.

Smluvní strany dále prohlašují a činí nesporným, že objednatel je oprávněn vrátit zhotoviteli vystavenou fakturu – daňový doklad v případě, že příslušná faktura – daňový doklad nebude mít některou ze zákonných či smluvních náležitostí či příloh s tím, že v takovém případě je zhotovitel povinen vystavit po doručení vrácené faktury – daňového dokladu bez zbytečného odkladu novou fakturu – daňový doklad se všemi zákonnými i smluvními náležitostmi včetně příloh. Od okamžiku doručení nové faktury – daňového dokladu dle předchozí věty počíná objednateli běžet nová doba splatnosti.

IV. Místo a čas plnění

Smluvní strany prohlašují a činí nesporným, že:

a) zhotovitel je povinen provést na svůj náklad a nebezpečí dílo v sídle Objednatele;

b) zhotovitel je povinen provést dílo do 9. 12. 2022;

c) o předání a převzetí díla bude sepsán a smluvními stranami podepsán předávací protokol, který musí obsahovat alespoň následující skutečnosti:

- identifikace této smlouvy;
- identifikace smluvních stran;
- místo a datum provedení díla, resp. jeho dokončení a předání;
- prohlášení objednatele, zda dílo přebírá s výhradami nebo bez výhrad;
- případné vady a nedodělky díla a lhůtu pro jejich odstranění;

d) zhotovitel je povinen odstranit vady a nedodělky díla ve lhůtě pro jejich odstranění uvedené v předávacím protokole dle písm. c) tohoto čl. smlouvy;

e) v případě odstranění vad a nedodělků ve smyslu písm. c) a d) tohoto čl. smlouvy, bude o předání a převzetí díla bez vad a nedodělků sepsán a smluvními stranami podepsán předávací protokol.

V. Ostatní ujednání

Smluvní strany prohlašují a činí nesporným, že:

a) v případě provádění, byť jen části díla prostřednictvím poddodavatelů zhotovitele, je zhotovitel odpovědný i za případně vzniklou majetkovou újmu (škodu) objednatele

v důsledku porušení smluvních či zákonných povinností daného poddodavatele, jako by ji způsobil sám, a zhotovitel je tak povinen takto vzniklou majetkovou újmu (škodu) objednateli v plném rozsahu nahradit;

b) zhotovitel je povinen být pojištěn po celou dobu účinnosti této smlouvy pro případ způsobení majetkové újmy (škody) třetím osobám v souvislosti se svou činností, resp. v souvislosti s prováděním díla, s minimálním pojistným plněním ve výši 3.000.000,- Kč (slovy: třimiliónykorunčeských), kdy příslušnou pojistku je zhotovitel povinen objednateli předložit bezodkladně na požádání objednatele, nejpozději však do dvou pracovních dnů ode dne doručení výzvy;

c) zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech, které se dozví při anebo v souvislosti s uzavřením této smlouvy a jejím plněním;

d) zhotovitel je povinen archivovat originál této smlouvy včetně jejích případných dodatků a jejích příloh, dále veškeré originály účetních dokladů a dalších dokumentů souvisejících s prováděním díla po dobu minimálně deseti let od protokolárního předání díla objednateli bez vad a nedodělků.

VI. Záruka za jakost díla

Zhotovitel prohlašuje a činí nesporným, že poskytuje na dílo záruku v délce dvacetičtyřměsíců, která počíná běžet okamžikem předání díla bez vad a nedodělků na základě předávacího protokolu ve smyslu čl. IV. této smlouvy.

Smluvní strany prohlašují a činí nesporným, že:

a) pokud objednatel v záruční době zjistí vadu díla, je povinen ji bezodkladně oznámit (postačí e-mailem) zhotoviteli na e-mailovou adresu: servishw@autocont.cz (dále jen jako „reklamace“) s tím, že zhotovitel je povinen vadu odstranit ve lhůtě patnácti dnů od okamžiku doručení reklamace a nahradit objednateli vzniklou majetkovou újmu (škodu) v plném rozsahu se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

b) doba od doručení reklamace zhotoviteli do doby odstranění vytýkané vady na základě reklamace se do záruční doby nezapočítává a o tuto dobu se záruční doba prodlužuje.

VII. Smluvní pokuta

Smluvní strany prohlašují a činí nesporným, že:

a) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. II. této smlouvy, resp. povinnost provést pro objednatele na svůj náklad a nebezpečí dílo v souladu se

zadávacími podmínkami veřejné zakázky, nabídkou zhotovitele, požadavky a účelem zadavatele, a dále technickou specifikací, která tvoří přílohu č. 1 této smlouvy, vymezující podrobněji dílo na základě této smlouvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

b) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. IV. písm. a), b) anebo d) této smlouvy, resp. povinnost provést na svůj náklad a nebezpečí dílo v sídle objednatele, anebo povinnost provést dílo do 9.12.2021 anebo povinnost odstranit vady a nedodělky díla ve lhůtě pro jejich odstranění uvedené v předávacím protokole, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

c) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. V. písm. a) této smlouvy, resp. povinnost být pojištěn po celou dobu účinnosti této smlouvy pro případ způsobení majetkové újmy (škody) třetím osobám v souvislosti se svou činností, resp. v souvislosti s prováděním díla, s minimálním pojistným plněním ve výši 3.000.000,- Kč (slovy: třimiliónykorunčeských), anebo povinnost předložit pojistku objednateli bezodkladně na požádání objednatele, nejpozději však do dvou pracovních dnů ode dne doručení výzvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

d) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. V. písm. b) této smlouvy, resp. povinnost zachovávat mlčenlivost o všech skutečnostech, které se dozví při anebo v souvislosti s uzavřením této smlouvy a jejím plněním, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 1% z celkové ceny díla za každý případ takovéhoto porušení se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

e) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. VI. této smlouvy, resp. povinnost odstranit vadu ve lhůtě patnácti dnů od okamžiku doručení reklamace, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

f) ujednáním o smluvních pokutách ve smyslu písm. a) – e) tohoto článku smlouvy není dotčeno právo objednatele na náhradu majetkové újmy (škody) v plném rozsahu, kdy tímto smluvní strany vylučují ust. § 2050 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

VIII. Odstoupení od smlouvy

Objednatel je oprávněn odstoupit od této smlouvy do doby provedení díla bez vad a nedodělků v těchto případech:

a) bude zahájeno insolvenční řízení ve věci zhotovitele jako dlužníka;
b) bude zahájeno anebo bude zjištěno jakékoliv exekuční řízení proti zhotoviteli jako povinnému;
c) zhotovitel bude v prodlení s provedením díla bez vad a nedodělků alespoň třicet kalendářních dnů;
d) zhotovitel bude provádět dílo v rozporu se zadávacími podmínkami anebo v rozporu s touto smlouvou, ačkoliv byl na tuto skutečnost ze strany objednatele alespoň jedenkrát upozorněn.

IX. Převzetí nebezpečí změny okolností

Zhotovitel prohlašuje a činí nesporným, že na sebe převzal nebezpečí změny okolností ve smyslu ust. § 1765 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

X. Závěrečná ujednání

Smluvní strany prohlašují a činí nesporným, že:

a) tato smlouva nabývá platnosti dnem podpisu obou smluvních stran, účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., zákon o registru smluv, v platném znění, kdy povinným subjektem je objednatel, a zavazuje se tak tuto smlouvu uveřejnit v registru smluv nejpozději do třiceti dnů ode dne podpisu této smlouvy oběma smluvními stranami;

b) tato smlouva je sepsána ve dvou vyhotoveních takto:

- 1x zhotovitel;
- 1x objednatel;

c) rozhodným právem pro tento závazkový vztah je právo české (právní řád České republiky);

d) tuto smlouvu je možné změnit pouze písemně, kdy pro účely této smlouvy se za písemnou formu nepovažuje výměna emailových či jiných elektronických zpráv;

e) vylučují přijetí nabídky s dodatkem nebo odchylkou ve smyslu ust. § 1740 zákona č. 89/2012 Sb., občanský zákoník, v platném znění;

f) pokud nebylo v této smlouvě ujednáno jinak, řídí se právní vztahy vzniklé z této smlouvy příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, v platném znění;

g) tato smlouva byla sepsána dle jejich vážné, pravé a svobodné vůle, kdy na důkaz toho po jejím přečtení činí vlastnoruční podpisy.

Příloha č. 1: technická specifikace

V Olomouci dne

Digitálně podepsal
Bc. Lukáš Jurča
Datum: 2022.07.01
07:27:13 +02'00'

……
Lukáš Jurča, ředitel krajského obchodního zastoupení
(zhotovitel)

V …….. dne …….

MUDr. Martin Svoboda

Digitálně podepsal
MUDr. Martin
Svoboda
Datum: 2022.07.14
08:05:26 +02'00'

……
Vojenská nemocnice Olomouc
plk. gšt. v. z. MUDr. Martin Svoboda, ředitel
(objednatel)

Příloha č. 1 PPZN: Technická zpráva (specifikace)

1. Úvod

Předmětem dodávky je systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje požadavky uvedené níže.

Součástí dodávky je veškerý potřebný hardware, software, licence a případný drobný a spojovací materiál, včetně implementačních a dokumentačních prací. Zadavatel dodá své vlastní dva SFP+ (10 Gbit) SingleMode moduly do ethernetových switchů pro připojení hardwarového kolektoru/senzoru. Dodavatel dodá analogické dva SFP+ moduly do dodávaného hardwarového kolektoru/senzoru (protikusy), tyto jsou tedy součástí dodávky a musí být kryty stejnou zárukou a podporou jako nabízený kolektor/senzor. Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.

Nabízená technologie musí být určená pro český trh. Jednotlivé komponenty řešení (hardware, software, licence) a jejich PN (produktové číselné označení) musí být dostupné přímo v oficiálním ceníku výrobce pro český trh. Podpora ve všech úrovních musí být zajištěna přímo jejich výrobcem, kterého může zadavatel přímo kontaktovat.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci dodávky dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, dodavatel může nabídnout charakteristiky (funkce) lepší.

Řešení musí splňovat všechny požadavky uvedené v tomto dokumentu.

Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory.

2. Výčet požadovaných vlastností dodávaného hardware a software

2.1 Obecné požadavky

Název, typové označení	**(MA-SC-2k-M-00) GreyCortex Mendel HW zařízení vč. perpetuální SW licence: senzor + kolektor / 2Gbps průtok / 1200 toků za sekundu / 5200 monitorovaných zařízení / Plná funkcionalita / 60+ denní úložiště / 4x1GE monitorovací porty / HW podpora 5 let NBD On-site / softwarová údržba a podpora pro MA-SC-2k po dobu 5 let** **Včetně:** - **HW-E-N20I monitorovací porty 2x10GbE** - **HW-E-SS4 úložiště 4x 3,84TB SSD pro celkovou kapacitu 15 TB (18 měsíců)** - **2x SFP+ (10 Gbit) a propojovací materiál**	

Číslo	Požadované funkcionality/vlastnosti	Nabízené řešení splňuje
	Systém pro analýzu síťového provozu	
1	Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.	ANO
2	Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.	ANO
3	Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.	ANO
4	Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.	ANO
5	Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.	ANO
6	Aktualizace systému musí být možné provádět uživatelsky v offline režimu.	ANO
	Zpracování a ukládání síťových toků	
7	Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.	ANO
8	Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.	ANO
9	Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně **18 měsíců** složené z SSD disků.	ANO
10	**Analýza aplikačních a systémových logů** Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.	ANO
	Uživatelské rozhraní	
11	Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.	ANO
12	Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	ANO
13	● granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute),	ANO
14	● granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),	ANO
15	● vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,	ANO
16	● vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	ANO
	Automatické hlášení (alerty) a reporting	

17	Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.	ANO
18	Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.	ANO
19	Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).	ANO
20	Je požadováno vytváření automatizovaných reportů v českém jazyce.	ANO
	Integrace systému	
21	Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	ANO
22	• syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	ANO
23	• přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	ANO
24	• export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data)	ANO
25	• integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Cisco ISE a Microsoft Active Directory	ANO
26	• integrace s firewally, alespoň Palo Alto, Fortinet a Checkpoint, pro automatické a manuální reakce vyvolané systémem	ANO
27	• integrace s nástroji pro řízení přístupu k síti minimálně Cisco ISE, pro automatickou a manuální reakci systému.	ANO

2.2 Požadavky na architekturu nasazení

	Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje**
	Obecné požadavky pro nasazení	
28	Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.	ANO
29	Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.	ANO
30	Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.	ANO
	Požadavky pro pokrytí IT prostředí	
31	V síti je předpokládáno cca **2000 aktivních zařízení** s průměrným denním celkovým průtokem **do 2Gbps**.	ANO
32	Je požadován **1x HW** datový kolektor/sensor o celkové propustnosti minimálně **2Gbps** s monitorovacím rozhraním **4x 1GE a 2x10GE**. Na zařízení je požadována dostupná historie dat minimálně **18 měsíců** zpětně, uložená na rychlém úložišti typu SSD o velikosti alespoň **14TB**. Požadován je minimálně RAID10 nebo RAID6 se schopností hot-swap.	ANO
33	Je požadován **2x VA** datový sensor pro prostředí VMware o průměrné denní propustnosti minimálně **100 Mbps**.	ANO

2.3 Požadavky na schopnost detekce bezpečnostních událostí

	Požadované funkcionality/vlastnosti	Nabízené řešení splňuje
	Monitorování zařízení, segmentů sítě a využívaných síťových služeb	
34	Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	ANO
35	• změna IP/MAC adresy hosta,	ANO
36	• duplicitní IP/MAC adresa,	ANO
37	• změna VLAN,	ANO
38	• vytvoření nové podsítě,	ANO
39	• připojení nového zařízení,	ANO
40	• použití nebo vznik nové služby,	ANO
41	• nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,	ANO
42	• přístup nového zařízení ke službě či zařízení	
43	• ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.	ANO
44	Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.	ANO
	Samostatné učení behaviorálních aktivit a detekce anomálií	
45	Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.	ANO
46	Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	ANO
47	• odchylku od modelu pro přenos dat, toků a paketů,	ANO
48	• odchylku od modelu pro počet komunikačních partnerů,	ANO
49	• odchylku od modelu entropie na komunikačních portech,	ANO
50	• odchylku od modelu pro počet síťových toků a využitých síťových služeb,	ANO
51	• odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).	ANO
52	Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.	ANO
	Identifikace neznámých hrozeb a podezřelých chování	
53	Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	ANO
54	• průzkumné aktivity v síti,	ANO
55	• detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě,	ANO
56	• detekce repetitivních vzorců chování na síti,	ANO
57	• detekce botnetů a ovládání kompromitované stanice,	ANO
58	• detekce příznaků těžení kryptoměn,	ANO
59	• útoky hrubou silou a enumerace dat,	ANO
60	• rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.	ANO

	Detekce na základě databáze známých hrozeb	
61	Systém musí být schopen identifikovat hrozby a reportovat události na základě	ANO
62	• detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik,	ANO
63	• reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.	ANO
64	Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.	ANO
65	Uživatel musí být schopen importovat vlastní záznamy.	ANO
66	Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.	ANO
67	Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).	ANO
68	Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu. Příklad možné syntaxe detekčního pravidla: *alert tcp $HOME_NET any -> any any (msg:”Command Shell Access”; content:”C:\\Users\\Administrator\\Desktop\\hfs2.3b”; sid:1000001; rev:1;)*	ANO
69	**Analýza šifrované komunikace** Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.	ANO
	Asistované učení	
70	Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	ANO
71	• IP adresa,	ANO
72	• MAC adresa,	ANO
73	• hostname,	ANO
74	• segment sítě / podsíť,	ANO
75	• lokalita – ASN, země, apod.	ANO
76	• směr komunikace – určení klienta, nebo serveru,	ANO
77	• detekovaná událost – kategorie, název apod.	ANO
78	• použité služby, protokolu, portu,	ANO
79	• libovolné kombinaci výše popsaných.	ANO
80	Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.	ANO

2.4 Požadavky na zajištění síťové viditelnosti

	Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje**
	Vyhledávání, filtrování a vizualizace dat	
81	Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.	ANO

82	Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	ANO
83	● podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN,	ANO
84	● prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.	ANO
85	Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.	ANO
86	Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.	ANO
87	Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.	ANO
88	Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.	ANO
	Kontextuální informace	
89	Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:	ANO
90	● jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie	ANO
91	● hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu	ANO
92	● IP geolokace	ANO
93	● IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá	ANO
94	● historie použitých MAC adresa a výrobce zařízení	ANO
95	● operační systém a jeho historie na zařízení	ANO
96	● uživatelem zadané poznámky a informace k zařízení	ANO
97	● automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	ANO
98	**Zaznamenávání a ukládání plného provozu** Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.	ANO

2.5 Další požadované oblasti využití

	Požadované funkcionality/vlastnosti	**Nabízené řešení splňuje**
	Monitorování politik kybernetické bezpečnosti	

99	Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, monitorovat definovanou komunikační matici, detekovat její porušení a hlásit nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	ANO
100	Pro účely monitorování politik kybernetické bezpečnosti musí systém podporovat automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.	ANO
	Management bezpečnostních událostí a incidentů	
101	Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	ANO
102	● jednoduchého sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů,	ANO
103	● možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostních incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.),	ANO
104	● možnost exportování dat do emailu, csv, pdf, syslogu a podobně,	ANO
105	● možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.	ANO
	Detekce úniku dat	
106	Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).	ANO
107	Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.	ANO
108	V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	ANO
109	● název souboru,	ANO
110	● velikost souboru,	ANO
111	● HASH souboru.	ANO
	Monitoring výkonu aplikací a sítě	
112	Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:	ANO
113	● přenosová rychlost sítě,	ANO
114	● rychlost odezvy aplikace,	ANO
115	● odezva systému z pohledu uživatele.	ANO
116	Výpočet uvedených výkonnostních parametrů a automatická a detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	ANO
117	● všechny porty a služby TCP,	ANO
118	● pro všechny kombinace služeb a zařízení.	ANO
119	Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.	ANO

2.6 Záruka a podpora

	Požadované funkcionality/vlastnosti	Nabízené řešení splňuje
120	Podpora výrobce v režimu 8x5 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu v českém jazyce v pracovní době (8x5) s lhůtou pro vyřešení požadavku Next-Business-Day, to vše po dobu 5 let.	ANO
121	Hardwarová záruka on-site Next-Business-Day Fix Time po dobu 5 let.	ANO
122	On-line přístup ke všem verzím firmwaru/softwaru a k on-line znalostní bázi výrobce v režimu 24x7 po dobu 5 let.	ANO
123	Profylaktická kontrola dodaných zařízení dodavatelem nejméně 3x ročně po dobu 5 let. Zadavatel předpokládá dobu trvání jedné profylaktické kontroly 2 hodiny, tj. 6 hodin ročně. Dodavatel může stanovit dle implementované technologie dobu delší. Cenu této služby zahrne do tabulky v kapitole 8.	ANO
124	Aktualizace firmwaru/softwaru dodaných zařízení dodavatelem dle potřeby či dle požadavku zadavatele po dobu 5 let. Zadavatel odhaduje souhrnnou dobu aktualizací 6 hodin ročně. Dodavatel může stanovit dle implementované technologie a svých zkušeností dobu delší. Cenu této služby zahrne do tabulky v kapitole 8.	ANO

3. Ostatní podmínky

Zadavatel požaduje zboží nové, plně funkční a kompletní, nikoliv demo, repasované nebo jakkoliv již dříve použité.

Dodavatel je povinen s dodávkou doložit prohlášení výrobce zboží nebo jeho oficiálního zastoupení o tom, že na zboží identifikované podle sériových čísel bude zadavateli jakožto koncovému zákazníkovi poskytnuta záruka výrobce v plném, výrobcem poskytovaném rozsahu a že zboží je určeno pro český, resp. evropský trh.

4. Implementační služby

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalovány a zprovozněny a po jejich nasazení řádně dokumentovány a otestovány, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry. Součástí implementace je i konfigurace aktivních prvků – nastavení SPAN portů atd.

5. Školení

Součástí dodávky je administrátorské školení tří zaměstnanců zadavatele v rozsahu nejméně 2 dny.

6. Předávací kritéria

Předpokladem pro předání řešení do provozu bude splnění následujících akceptačních testů.

1) Veškeré komponenty systému jsou řádně licencované.
2) Byly dodány fyzické zařízení dle požadované technické specifikace.
3) Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele.
4) Dochází k záznamu flow a zrcadleného provozu, informace jsou dostupné k zobrazení a dalšímu zpracování.

5) Výsledná informace (graf nebo tabulka) definovaná libovolně nastaveným základním filtrem (např. IP adresa, podsíť, služba, událost, …) v 24hodinovém intervalu musí být zobrazena do 20s.
6) Funguje asistované učení při označení falešně pozitivní detekce.
7) Systém korektně načítá VLAN-ID ze zrcadlené komunikace a umožňuje filtrování informací podle VLAN-ID.
8) Systém zobrazuje netflow na základě adres nebo portů po překladu NAT.
9) Systém graficky znázorňuje skutečně přenesená data (In/Out) filtrovaná podle jednotlivých zdrojů flow nebo fyzických/logických interface.
10) Systém detekuje známé hrozby na základě databáze známých hrozeb (je aktivně využíváno alespoň 40.000 detekčních pravidel/signatur a alespoň 100.000 záznamů typu Threat Intelligence).
11) Byla vytvořena a dodána instalační dokumentace.
12) Bylo provedeno školení v požadovaném rozsahu.

Na závěr zástupci zadavatele potvrdí splnění všech akceptačních podmínek pro předání řešení do provozu potvrzením „akceptačního protokolu“.