K U P N Í S M L O U V A

SML/2/2021

1. **Střední škola teleinformatiky, Ostrava, příspěvková organizace**
   adresa: Opavská 1119/12, 708 61 Ostrava - Poruba
   zastoupená: Ing. Pavlem Zubkem, ředitelem školy
   jednání ve věcech:
   a) smluvních: Ing. Pavlem Zubkem, ředitelem školy
   b) technických: Ing. Pavlem Zubkem, ředitelem školy
   c) dotací: Ing. Pavlem Zubkem, ředitelem školy
   telefon: +420 733 615 476
   e-mail: zubek@teleinformatika.eu

   IČO: 00845329
   DPH: není plátcem DPH
   bankovní spojení: ČSOB, a.s. Praha, pobočka Ostrava
   číslo účtu: 118359/0300

   (dále jen kupující)

a

2. **VISITECH, a.s.**
zapsána v *obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 6323*
zastoupena: Pavlem Kocourem, předsedou představenstva
jednání ve věcech technických: Ing. Pavel Meletzký, MBA
se sídlem: Košinova 655/59, 612 00 Brno, Královo pole
IČ: 25543415
DIČ: CZ25543415
telefon: +420 602 495 914
e-mail: pavel.meletzky@visitech.cz
bankovní spojení: Artesa, spořitelní družstvo
č. účtu: 1076980003/ 2220

(dále jen prodávající)

uzavřeli níže uvedeného dne podle ustanovení § 2079 a následujících Občanského zákoníku v platném znění (dále jen občanský zákoník) kupní smlouvu, která má tento obsah:

I. Předmět a místo plnění

1. **Předmětem plnění této smlouvy je dodávka, montáž a konfigurace vybavení pro kybernetickou laboratoř a pořízení** dalšího zboží v rozsahu uvedeném v položkovém rozpočtu, který je přílohou

této smlouvy (dále též „zboží“) v rámci veřejné zakázky **„DODÁVKA IT VYBAVENÍ A VYBAVENÍ PRO VÝUKU ODBORNÝCH PŘEDMĚTŮ“** (dále též „dodávky“). **Při plnění této smlouvy je prodávající povinen vycházet ze zadávací dokumentace ke 3. části předmětné veřejné zakázky - CYLAB** (dále jen „dokumentace“). Místem plnění je Střední škola teleinformatiky, Ostrava, příspěvková organizace, Opavská 1119/12, 708 61 Ostrava – Poruba.

Prodávající prohlašuje, že je odborně způsobilý k zajištění předmětu plnění podle této smlouvy.

2. Prodávající se zavazuje dodat a provést montáž uvedeného zboží v místech plnění a převést na kupujícího vlastnické právo k tomuto zboží. Kupující se zavazuje zaplatit prodávajícímu za uvedené zboží bez vad a nedodělků a montáž bez vad a nedodělků kupní cenu a to na základě předávacího protokolu a soupisu dodávek.
3. Prodávající bere na vědomí, že zboží bude spolufinancováno z prostředků ESF prostřednictvím Operačního program výzkum, vývoj a vzdělávání (OP VVV). Zboží je pořizováno z projektu odborné, kariérové a polytechnické vzdělávání v MSK II, registrační číslo projektu CZ.02.3.68/0.0/0.0/19_078/0019613 (dále též projekt).

   Smluvní strany se dohodly, že kupující je oprávněn odstoupit od této smlouvy, rozhodne-li poskytovatel dotace, že kupujícímu neposkytne na zboží dotaci nebo že dotaci poskytne v nižší výši než, jak o ni kupující žádal. Smluvní strany se tímto dohodly, že odstoupí-li kupující od této smlouvy dle tohoto odstavce, prodávající se tímto vzdává práva na náhradu škody.
4. Zboží musí splňovat požadavky právních předpisů a technických norem.
5. Zboží musí splňovat parametry uvedené v zadávací dokumentaci a parametry uvedené příloze č. 2 k této smlouvě. Tyto parametry je prodávající povinen dodržet. Prodávající odpovídá za to, že práva k užití počítačových programů, která jsou předmětem ochrany dle zákona č. 121/2000 Sb., autorský zákon, jsou poskytována v souladu s tímto zákonem.

II. Cena

1. Smluvní strany se dohodly, že cena za dodávky a montáž provedené v rozsahu uvedeném v čl. I této smlouvy je stanovena v souladu se zákonem o cenách a činí:

Cena celkem bez DPH	5 379 285,00 Kč
DPH samostatně	1 129 649,85 Kč
Cena celkem včetně DPH	6 508 934,85 Kč

2. Položkový rozpočet je uveden v příloze této smlouvy.
3. Cena je maximální a zahrnuje veškeré náklady, které bude prodávající mít s dodáním a montáží zboží kupujícímu včetně přepravy.
4. Pokud je prodávající plátcem DPH, bude k ceně bez DPH připočteno DPH podle zákona č.235/2004 Sb., o dani z přidané hodnoty. Prodávající je odpovědný za to, že sazba DPH je stanovena v souladu s platnými právními předpisy.
5. Smluvní strany se dohodly, že povinnost zaplatit je splněna dnem odepsání příslušné částky z účtu kupujícího.

6. Smluvní strany se dohodly, že prodávající bude ve smlouvě a v dokladech při platebním styku s kupujícím užívat číslo účtu uveřejněné dle § 98 zák. č. 235/2004 Sb. v registru plátců a identifikovaných osob.

III. Podmínky plnění

1. Prodávající je povinen dodat kupujícímu zboží dle čl. I. bodu 1. této smlouvy bez vad a nedodělků do místa plnění a provést jeho montáž bez vad a nedodělků v místě plnění do **30 dnů** od nabytí účinnosti této smlouvy**.**
2. Prodávající je povinen předat kupujícímu v termínu uvedeném v bodě 1. tohoto článku rovněž veškeré doklady vztahující se ke zboží, zejména záruční listy, návody k použití atd., vše v českém jazyce.
3. Smluvní strany se dohodly, že má-li zboží v době jeho předání kupujícímu vady či nedodělky, je kupující oprávněn odmítnout převzetí zboží. O předání a převzetí bude prodávajícím sepsán protokol, který bude podepsán zástupci obou smluvních stran.
4. Datum převzetí zboží kupujícím je datem zdanitelného plnění.
5. Prodávající je povinen plnit veškeré povinnosti vyplývající z právních předpisů v oblasti pracovněprávní, oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, zejména zákona č. 262/2006. Sb., zákoník práce, ve znění pozdějších předpisů (se zřetelem na regulaci odměňování, pracovní doby, doby odpočinku mezi směnami atp.), zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů (se zvláštním zřetelem na regulaci zaměstnávání cizinců), a to vůči všem osobám, které se podílejí na plnění předmětu této smlouvy. Prodávající je dále povinen plnit veškeré povinnosti vyplývající z právních předpisů v oblasti ochrany životního prostředí, zejména se zřetelem na nakládání s odpady. Plnění těchto povinností je prodávající povinen zajistit i u svých poddodavatelů.
6. Prodávající je povinen zajistit po celou dobu plnění veřejné zakázky sjednání a dodržování smluvních podmínek se svými poddodavateli srovnatelných s podmínkami sjednanými v této smlouvě, a to zejména v rozsahu smluvních pokut i jejich výše, délky záruční doby, splatnosti faktur. Smluvní podmínky se považují za srovnatelné, budou-li smluvní pokuty i jejich výše, délka záruční doby a splatnost faktur shodné jako v této smlouvě. Prodávající je povinen na žádost kupujícího předložit kupujícímu smlouvu uzavřenou se svým poddodavatelem.
7. Prodávající je povinen řádně a včas plnit finanční závazky svým poddodavatelům, přičemž za řádné a včasné plnění finančních závazků se považuje plné uhrazení faktur vystavených poddodavatelem prodávajícímu za práce na dodávce zboží, a to vždy nejpozději do 7 pracovních dnů od připsání platby zadavatele na účet dodavatele. Dodavatel je povinen, pokud o to zadavatel požádá, nejpozději do 7 pracovních dnů od přijetí výzvy, zadavateli prokazatelně doložit (např. výpisem z účtu), kdy mu byla na účet připsána platba zadavatele, a že zaplatil poddodavateli fakturu řádně a včas. Dodavatel se zavazuje přenést totožnou povinnost do případných dalších úrovní dodavatelského řetězce.

IV. Platební podmínky

1. Prodávající je oprávněn vystavit daňový doklad, příp. daňové doklady (dále jen „faktura“) na kupní cenu po předání a převzetí zboží kupujícím se splatností 30 dnů ode dne doručení faktury

kupujícímu. Není-li zboží v době předání kupujícímu bez vad a nedodělků, dohodly se smluvní strany, že prodávající není oprávněn vystavit daňový doklad a nevzniká mu právo na zaplacení kupní ceny, nedohodnou-li se smluvní strany jinak.

Faktury prodávajícího budou mít náležitosti daňového dokladu dle příslušných právních předpisů. Dále musí faktura obsahovat číslo smlouvy kupujícího. Součástí faktury bude příloha – soupis dodávek oceněný podle položkového rozpočtu odsouhlasený kupujícím ve dvou vyhotoveních.

Faktura bude dále obsahovat text: „Tento projekt je spolufinancovaný z prostředků ESF prostřednictvím Operačního program výzkum, vývoj a vzdělávání (OP VVV). Zboží je pořizováno z projektu odborné, kariérové a polytechnické vzdělávání v MSK II, registrační číslo projektu CZ.02.3.68/0.0/0.0/19_078/0019613“.

2. Nebude–li faktura obsahovat některou stanovenou náležitost, bude obsahovat nesprávné údaje nebo bude chybně vyúčtována cena, je kupující oprávněn vadnou fakturu před uplynutím doby splatnosti vrátit prodávajícímu k provedení opravy. Prodávající provede opravu vystavením nové faktury s novou dobou splatnosti nebo vystavením opravného daňového dokladu. V takovém případě není kupující v prodlení s placením faktury. Celá doba splatnosti běží znovu ode dne doručení nově vyhotovené faktury nebo opravného daňového dokladu kupujícímu.

V. Odpovědnost za vady, záruční podmínky

1. Smluvní strany se dohodly, že prodávající poskytuje na zboží záruku v délce stanovené výrobcem, nejméně však v délce 24 měsíců ode dne převzetí zboží kupujícím. Prodávající se zároveň zavazuje provádět opravy zboží uvedeného v čl. I. bod 1 této smlouvy během záruční doby v místě plnění s tím, že prodávající nemá nárok na úhradu dopravy do místa plnění.
2. Záruční doba neběží po dobu, po kterou kupující nemohl zboží užívat. Pro ty části zboží, které byly v důsledku reklamace kupujícího prodávajícím opraveny, běží záruční doba opětovně od počátku ode dne provedení reklamační opravy.
3. Kupující písemně oznámí prodávajícímu výskyt vady a vadu popíše. Jakmile kupující odeslal toto písemné oznámení, má se za to, že požaduje bezplatné odstranění vady, nestanoví-li kupující jinak.
4. Prodávající je povinen odstranit vadu, kterou má zboží v době předání kupujícímu nebo vadu, kterou má zboží v záruční době, nejpozději do 5 dnů ode dne, kdy byla vada prodávajícímu oznámena, a to i v případě, že reklamaci neuznává, nedohodnou-li se smluvní strany jinak.
5. Náklady na odstranění reklamované vady nese prodávající i ve sporných případech až do rozhodnutí soudu.
6. Neodstraní-li prodávající v kupujícím stanoveném termínu vadu, na niž se vztahuje záruka, nebo vadu, kterou mělo zboží v době převzetí kupujícím, je kupující oprávněn pověřit odstraněním vady jinou osobu. Veškeré takto vzniklé náklady je prodávající povinen uhradit kupujícímu.
7. Smluvní strany se dohodly, že zboží má vady, zejména neodpovídá-li právním předpisům, technickým normám, této smlouvě, zadávací dokumentaci, není-li funkční nebo nebyly-li ke zboží předány potřebné doklady dle čl. III. bod 2 této smlouvy.

VI. Smluvní pokuta

1. Kupující má právo požadovat po prodávajícím smluvní pokutu při nedodržení termínu dodávky a montáže zboží dle čl. III. bod 1 této smlouvy ve výši 0,2 % z celkové ceny dle čl. II. této smlouvy za

každý den prodlení a prodávající je povinen požadovanou smluvní pokutu uhradit.

2. Prodávající má právo požadovat smluvní pokutu při nedodržení termínu splatnosti faktury dle čl. IV. této smlouvy ve výši 0,05 % z dlužné částky za každý den prodlení a kupující je povinen požadovanou smluvní pokutu uhradit.
3. Neodstraní-li prodávající vadu, kterou má zboží v době předání kupujícímu nebo vadu, kterou má zboží v záruční době v termínu uvedeném v čl. V. bod 4 této smlouvy, je kupující oprávněn požadovat po prodávajícím smluvní pokutu ve výši 0,05 % z celkové ceny dle čl. II. této smlouvy za každý den prodlení s odstraněním vady a každou jednotlivou vadu.
5. Nesplní-li prodávající kteroukoliv povinnost uvedenou v čl. III. bod 5 této smlouvy, je kupující oprávněn požadovat po prodávajícím smluvní pokutu ve výši 0,4 % z celkové ceny dle čl. II. této smlouvy.
6. Nesplní-li prodávající kteroukoliv povinnost uvedenou v čl. III. bod 6 této smlouvy, je kupující oprávněn požadovat po prodávajícím smluvní pokutu ve výši 0,2 % z celkové ceny dle čl. II. této smlouvy za nedodržení této povinnosti u každého poddodavatele, u něhož nebude příslušná povinnost splněna.
7. Nesplní-li prodávající kteroukoliv povinnost stanovenou v čl. III. bod 7 této smlouvy, je kupující oprávněn požadovat po prodávajícím smluvní pokutu ve výši 0,4 % z celkové ceny dle čl. II. této smlouvy.
8. Poruší-li prodávající jakoukoliv povinnost uvedenou v článku VII. bod 4 této smlouvy, je kupující oprávněn požadovat po prodávajícím smluvní pokutu ve výši 3.000,-Kč za každý zpětně neodebraný kus zboží nebo za každý nepředaný doklad potvrzující provedení ekologické likvidace zboží.
9. Smluvní pokuty a úrok z prodlení jsou splatné do 21-ti dnů ode dne vyúčtování.
10. Smluvní strany se dohodly, že smluvní pokuty sjednané touto smlouvou zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé straně škoda, kterou lze vymáhat samostatně v plné výši. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody.

VII. Další ujednání

1. Vlastnické právo ke zboží přechází na kupujícího převzetím zboží. Tímto dnem přechází na kupujícího odpovědnost ze vzniku škod na zboží. Smluvní strany se dohodly, že po dobu přepravy nese nebezpečí škody prodávající.
2. Prodlení s termínem plnění o více než 5 dnů je podstatným porušením smlouvy a může být důvodem k odstoupení od smlouvy, pokud se smluvní strany nedohodnou jinak.
3. Prodávající je povinen dodržet poddodavatelské schéma předložené v nabídce v rámci zadávacího řízení. V případě, že v průběhu plnění této smlouvy dojde ke změně či doplnění poddodavatele, musí prodávající o této skutečnosti kupujícího neprodleně písemně informovat. V případě, že se bude jednat o poddodavatele ve smyslu § 83 nebo § 85 zákona o veřejných zakázkách, je prodávající povinen jej nahradit poddodavatelem se shodnou kvalifikací. V opačném případě, není prodávající oprávněn poddodavateli umožnit práci na stavbě. Porušení této povinnosti je považováno za podstatné porušení této smlouvy a kupující může od této smlouvy odstoupit.

Prodávající je povinen kdykoliv v průběhu plnění smlouvy na žádost kupujícího předložit kompletní seznam částí plnění plněných prostřednictvím poddodavatelů včetně identifikace poddodavatelů.

4. Prodávající se zavazuje zajistit u kupujícího zpětný odběr jím dodaného zboží a jeho následnou ekologickou likvidaci. Prodávající je na vyžádání povinen kupujícímu předat doklad potvrzující provedení ekologické likvidace zboží.
5. Prodávající je povinen zajistit na žádost kupujícího za cenu dohodnutou s kupujícím po dobu pěti let od ukončení výroby zboží náhradní díly ke zboží, nejedná-li se o vadu v záruční době.

VIII. Závěrečná ustanovení

1. Prodávající prohlašuje, že v rámci zadávacího řízení provedeného dle zákona o veřejných zakázkách uvedl v nabídce veškeré informace a doklady, které odpovídají skutečnosti a měly nebo mohly mít vliv na výsledek zadávacího řízení. Porušení této povinnosti je považováno za podstatné porušení této smlouvy a kupující může od této smlouvy odstoupit.
2. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do konce roku 2031. Pokud je v českých právních předpisech stanovena lhůta delší, musí kupující použít ji. Prodávající je povinen minimálně do konce roku 2028 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (poskytovatel dotačních prostředků, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
3. Strany smlouvy se dohodly na tom, že tato smlouva je uzavřena okamžikem podpisu obou smluvních stran, přičemž rozhodující je datum pozdějšího podpisu. Tato smlouva nabude účinnosti dnem zveřejnění v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, v platném znění. Právní vztahy touto smlouvou neupravené se řídí zákonem č. 89/2012 Sb., občanským zákoníkem, v platném znění.
4. Kupující je povinným subjektem dle zákona č. 340/2015 Sb., o registru smluv, v platném znění. Smluvní strany se dohodly, že povinnosti dle tohoto zákona v souvislosti s uveřejněním smlouvy zajistí Kupující.
5. Smluvní strany souhlasí s uveřejněním v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, v platném znění.
6. Smluvní strany souhlasí s tím, že v registru smluv bude zveřejněn celý rozsah této smlouvy, a to na dobu neurčitou.
7. Změnit nebo doplnit tuto smlouvu mohou smluvní strany, jen v případě, že tím nebude porušen zákon o veřejných zakázkách, a to formou písemných dodatků.
8. Kupující a prodávající jsou oprávněni odstoupit od této smlouvy v případech stanovených v občanském zákoníku a v případech uvedených v této smlouvě.
9. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a že byla uzavřena podle jejich pravé a svobodné vůle, což stvrzují svými podpisy. Smlouva je vyhotovena v elektronické podobě.

10.O přidělení veřejné zakázky a o uzavření této smlouvy rozhodl ředitel školy.

Příloha:

1. Položkový rozpočet
2. Technická specifikace - CYLAB

V Ostravě

Za kupujícího

Ing. Pavel Zubek

Digitálně podepsal Ing. Pavel Zubek
Datum: 2021.11.19 10:46:36 +01'00'

……

Ing. Pavel Zubek, ředitel

V Brně

Za prodávajícího

Pavel Kocour

Digitálně podepsánoPavel Kocour
DN:C=CZ, OID.2.5.4.97=NTRCZ-25543415, O=VISITECH a.s., OU=2, CN=Pavel Kocour, SN=Kocour, G=Pavel, SERIALNUMBER=P157010
Příčina:Schválil jsem tento dokument svým právně závazným podpisem
Umístění:zde lokace podpisu
Datumu:2021.11.22 09:31:15+01'00'
Foxit PDF Reader Verze: 11.1.0

……

VISITECH, a.s.

Pavel Kocour, předseda představenstva

položka	název položky	popis položky	ks /MD	cena za jednotku v Kč bez DPH	cena za položku v Kč bez DPH	konkrétní označení nabízeného výrobku	
Antivirový program							
1	**Pokročilá ochrana koncových bodů včetně ochrany virtualizačních platforem a EDR**	Pokročilá ochrana koncových bodů včetně ochrany virtualizačních platforem a EDR dle technické specifikace viz příloha č. 12 - TECHNICKÁ SPECIFIKACE Pokročilé ochrany koncových bodů včetně ochrany virtualizačních platforem a EDR	26	14 500,00 Kč	377 000,00 Kč	Bitdefender Gravity Zone Ultra s EDR	*** viz. pozn.**
2	**Implementace**	Implementace Pokročilé ochrany koncových bodů včetně ochrany virtualizačních platforem a EDR	1	50 000,00 Kč	50 000,00 Kč		
3	**Zaškolení obsluhy**	Zaškolení obsluhy Pokročilé ochrany koncových bodů včetně ochrany virtualizačních platforem a EDR	5	15 000,00 Kč	75 000,00 Kč		
NTA systém pro analýzu sítě							
4	**VA kolektor/senzor**	VA kolektor/sensor dle technické specifikace viz příloha č. 8 - TECHNICKÁ SPECIFIKACE NTA SYSTÉMU	2	179 000,00 Kč	358 000,00 Kč	MA-SC-200-SW - GreyCortex Mendel perpetuální SW licence: senzor + kolektor / 200Mbps průtok / 200 toků za sekundu / 500 monitorovaných zařízení / Plná funkcionalita	*** viz. pozn.**
5	**Maintenance**	Maintenance pro VA kolektor/sensor dle technické specifikace viz příloha č. 12 - TECHNICKÁ SPECIFIKACE NTA SYSTÉMU na dobu 5 let	2	299 000,00 Kč	598 000,00 Kč	MA-SC-200-MS5Y 5letá softwarová údržba a podpora pro MA-SC-200	*** viz. pozn.**
6	**Implementace**	Implementace VA kolektor/sensor dle technické specifikace viz příloha č. 12 - TECHNICKÁ SPECIFIKACE NTA SYSTÉMU	10	15 000,00 Kč	150 000,00 Kč		
7	**Zaškolení obsluhy**	Zaškolení obsluhy VA kolektor/sensor dle technické specifikace viz příloha č. 12 - TECHNICKÁ SPECIFIKACE NTA SYSTÉMU	5	15 000,00 Kč	75 000,00 Kč		
Pokročilý unified security management							
8	**SW licence pro USM (virtual appliance)**	Nástroj USM s podporou výrobce min. na 5let včetně možnosti updatů a upgradů na vyšší verze min. po celou dobu platnosti podpory výrobce. USM musí být dodán formou VA (virtual appliance) s následujícími požadavky. Množství sbíraných událostí: min. 1000 EPS, Množství korelovaných událostí: min. 1000 EPS, Systém detekce vniknutí do sítě: min. 100 Mbps, Počet napojitelných zdrojů logů: min. 75, Analýza datových toků na základě flow dat poslaných do USM nástroje včetně dostupnosti služeb: min. 1Gbps, Skener zranitelností součástí nástroje USM - aktivní skenování sítě za účelem identifikace zranitelností a jejich vyhodnocování, monitoring koncových zařízení, nastavení přizpůsobených reportů dle potřeb zadavatele, Obohacování informací z infrastruktury o informace z reputačních databází, Integrovaná Znalostní databáze hrozeb, aktivní a pasivní skenování sítě za účelem správy zdrojů. Zároveň zadavatel uvádí, že pro účely celkového řešení nesmí být tato technologie dodána formou tzv. Open source řešení.	1	282 560,00 Kč	282 560,00 Kč	USM Appliance, All-in-One 75A (1TB) - Virtual Appliance	*** viz. pozn.**
9	**Maintenance**	Maintenance pro SW licence pro USM na dobu 5 let	1	408 145,00 Kč	408 145,00 Kč	USM Appliance, All-in-One 75A (1TB) - Virtual - 10x5 Support & Maintenance + USM Appliance, All-in-One 75A (1TB) - Virtual - AlienVault Labs Threat Intelligence Subscription	*** viz. pozn.**
10	**Implementace**	Implementace USM	5	15 000,00 Kč	75 000,00 Kč		
11	**Zaškolení obsluhy**	Zaškolení USM	5	15 000,00 Kč	75 000,00 Kč		
Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring							
12	**Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring**	Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring dle technické specifikace viz příloha č. 9 - TECHNICKÁ SPECIFIKACE pro Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring	1	179 000,00 Kč	179 000,00 Kč	AddNet Entrprise Server Edition - 100, AddNet Work server	*** viz. pozn.**
13	**Maintenance**	Maintenance pro Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring na dobu 5 let	1	120 000,00 Kč	120 000,00 Kč	5 letá podpora AddNet Entrprise Server Edition - 100 a AddNet Work server	*** viz. pozn.**
14	**Implementace**	Implementace pro Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring	10	15 000,00 Kč	150 000,00 Kč		
15	**Zaškolení obsluhy**	Zaškolení pro Integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring	5	15 000,00 Kč	75 000,00 Kč		
NGFW							

16	**HW**	NGFW dle technické specifikace viz příloha č. 10 - TECHNICKÁ SPECIFIKACE NGFW	2	79 990,00 Kč	159 980,00 Kč	FortiGate-100F 22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, dual power supplies redundancy.	*** viz. pozn.**
17	**Rozšířená záruka**	Rozšířená záruka výrobce NGFW dle technické specifikace viz příloha č. 10 - TECHNICKÁ SPECIFIKACE NGFW	2	259 500,00 Kč	519 000,00 Kč	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)	*** viz. pozn.**
18	**Implementace**	Implementace NGFW dle technické specifikace viz příloha č. 10 - TECHNICKÁ SPECIFIKACE NGFW	2	15 000,00 Kč	30 000,00 Kč		
19	**Zaškolení obsluhy**	Zaškolení obsluhy NGFW dle technické specifikace viz příloha č. 10 - TECHNICKÁ SPECIFIKACE NGFW	1	15 000,00 Kč	15 000,00 Kč		
Automatizace reakce							
20	**Virtualizační hypervizor**	Virtualizační hypervisor umožňující provoz min. na 3 serverech, každý se 2 CPU, zajišťující živou migraci virtuálních strojů, vysokou dostupnost, replikace, ochranu dat a s možností přístupu ke sdílenému diskovému úložišti. Podpora výrobce min. na 5let vč. možností updatů a upgradů na novější verze min. po celou dobu platnosti podpory výrobce.	1	78 000,00 Kč	78 000,00 Kč	VS7-ESP-KIT-A Academic VMware vSphere 7 Essentials Plus Kit for 3 hosts (Max 2 processors per host)	*** viz. pozn.**
21	**Rozšířená záruka**	Podpora výrobce min. na 5let vč. možností updatů a upgradů na novější verze min. po celou dobu platnosti podpory výrobce.	1	75 000,00 Kč	75 000,00 Kč	VS7-ESP-KIT-G-SSS-A Academic Basic Support/Subscription for VMware vSphere 7 Essentials Plus Kit for 5 years	*** viz. pozn.**
22	**Implementace**	Implementace Virtualizačního hypervizoru	1	15 000,00 Kč	15 000,00 Kč		
HW							
23	**Server pro IT systémy laboratoře**	Server s rackovatelným chassis s maxilmální výškou 2U, počet paměťových slotů min. 24, počet podporvaných pevných disků SAS/SATA min. 16, podpora min. RAID 0, 1, 5, 10, podpora redundantního napájení RPS včetně již osazeného redundatního napájecího zdroje, certifikace 80PLUS, podpora OOB, procesor: minimální výkon dle https://www.cpubenchmark.net : 32100 bodů, min. 1024 GB operační paměť (DDR4 DIMM, frekvence min. 2933 MHz), min. 5TB užitná kapacita v RAID 5 typu HDD (velikost 2,5", rozhraní SAS min. 12Gb/s, rychlost otáček min. 10000), min. 26TB užitná kapacita v RAID 5 typu SSD (velikost 2,5", rozhraní SSD SATA min. 6Gb/s), síťová karta min. 10Gb, min. 2x SFP+, síťová karta min. 4x 1Gb, vzdálený management, support výrobce min. na 5let v režimu min. 9x5 a s opravou následující pracovní den od nahlášení závady, podpora síťových standardů IEEE 802.1Q,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ae,IEEE 802.3u, kompatibilní s VMware ESXi a OS Windows Server 2019.	1	1 310 000,00 Kč	1 310 000,00 Kč	FUJITSU - PY RX2540 M5 2x8 2.5'-3,84SSD SATA Mixed	* viz. pozn.
24	**Maintenance - podpora výrobce**	TP 5y OS,9x5,NBD	1	54 600,00 Kč	54 600,00 Kč	TP 5y OS,9x5,NBD Rec	* viz. pozn.
25	**Implementace**	Implementace Server pro IT systémy laboratoře	5	15 000,00 Kč	75 000,00 Kč		
26	**CENA CELKEM V Kč bez DPH**				5 379 285,00 Kč		
27	**DPH samostatně**				1 129 649,85 Kč		
28	**CENA CELKEM V Kč včetně DPH**				6 508 934,85 Kč		

*** Pokud tento dokument obsahuje požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, která platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, je taková specifikace brána pouze jako typová. Je přípustné veškerý takto specifikovaný materiál nahradit jiným ekvivalentem, u kterého dodavatel garantuje, že bude mít minimálně shodné vlastnosti, technické a kvalitativní parametry a zajistí dodržení všech požadovaných technických a uživatelských standardů.**

Příloha č. 2 - TECHNICKÁ SPECIFIKACE NTA SYSTÉMU

Pokud tento dokument obsahuje požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, která platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, je taková specifikace brána pouze jako typová. Je přípustné veškerý takto specifikovaný materiál nahradit jiným ekvivalentem, u kterého dodavatel garantuje, že bude mít minimálně shodné vlastnosti, technické a kvalitativní parametry a zajistí dodržení všech požadovaných technických a uživatelských standardů.

Obecné požadavky

Systém pro analýzu síťového provozu

Systém 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.

Požadujeme 2 licence virtuální appliance (VA) s podporou na 5 let.

Ve výukové laboratoři je předpokládán datový průtok do maximálního objemu 200Mbps.

SW appliance musí být instalovatelná do virtualizačního prostředí VMware a Hyper-V.

Analýza plného síťového provozu

Dodaný systém musí analyzovat síť čistě na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.

Ukládání síťových toků

Systém ukládá síťové toky ve formátu, který umožní uživatelsky přívětivou analýzu síťové komunikace, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.

Uchování a vyhledávání síťových toků

Je požadována licence pro uchování datových toků v délce minimálně 180 dnů.

Dále je požadováno, aby uživatel mohl v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků a agregovaných síťových statistik na základě minimálně parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.

Automatická identifikace důležitých systémů

Je požadována automatická detekce přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod. Systém musí být schopen upozornit na vznik nových služeb v interní síti a sledovat jejich změny. A to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Direktory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTPS, POP3S, IMAPS, CDP, LLDP, MSSQL, MySQL, TELNET, FTP, TFTP.

Hardwarové požadavky

Síťové porty

Celkem požadujeme licencování minimálně 2 LAN rozhraní 1 Gbps metalika pro sběr dat a 1 LAN rozhraní 1 Gbps metalika pro práci s centrální konzolí.

Požadavky na schopnost detekce bezpečnostních událostí

Monitorování zařízení, segmentů sítě a využívaných síťových služeb

Poskytovaný systém musí identifikovat zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně: změna IP/MAC adresy hosta, duplicitní IP/MAC adresa, změna VLAN, vytvoření nové podsítě, připojení nového zařízení, použití nové služby, nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení.

Systém musí uživateli umožnit pomocí těchto metod nastavovat bezpečnostní politiky pro různé segmenty sítě a na porušení těchto politik reagovat upozorněním.

Detekce síťových služeb

Systém musí být schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu.

Samostatné učení behaviorálních aktivit a detekce anomálií

Systém musí používat matematické metody samostatného učení (např. strojové učení) pro analýzu standardní síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování organizace.

Především systém musí mít schopnost identifikovat nestandardní síťové chování, a to zejména:

- anomální přenosy dat, toků a paketů,
- anomální počet komunikačních partnerů a entropie na portech,
- anomální počet síťových toků a využitých síťových služeb,
- anomálie výkonnosti sítě a aplikací.

Samostatné učení je požadováno na všech síťových službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 síťové vrstvy.

Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik

Systém musí být schopen detekovat neznámé hrozby, jako jsou trojské koně, botnety, apod.

Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:

- průzkumné aktivity v síti,
- potenciální úniky dat,
- detekce strojového chování, které nevytvářejí lidští uživatelé sítě,
- detekce repetitivních vzorců chování na síti,
- detekce botnetů o ovládání kompromitované stanice,
- detekce zapojení do sítě pro těžení kryptoměn,

- útoky hrubou silou, rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a HTTP prostřednictvím DNS.

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.

Asistované učení a korelace událostí

Systém musí být schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.

Systém musí být schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí – minimálně v rozsahu kritické a důležité.

Aktuální databáze blacklistů

Systém musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v sítí prostřednictvím minimálně denně aktualizovaných reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze.

Požadavky na zajištění síťové viditelnosti

Rychlé vyhledávání a filtrování všech dat

Systém musí být schopen podporovat okamžité vyhledávání a vizualizaci pro forenzní analýzu a podporu pro tzv. threat hunting (analýza bezpečnostních událostí při ověřování bezpečnostních incidentů).

Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí a zaznamenaných síťových toků, a to minimálně podle parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.

Systém musí být schopen v reálném čase filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.

Uživatel musí mít možnost ukládat definované filtry a sdílet je s dalšími uživateli.

Ukládání a vyhledávání aplikačních metadat

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, MS-SQL, SIP, Kerberos, SSL/TLS.

Kontextuální informace

Systém musí být schopen získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace pro detekované události a ukládané záznamy síťových toků a agregované síťové statistiky minimálně v tomto rozsahu:

- jméno uživatele a další jeho parametry z doménového řadiče (minimálně MS Active Directory),

- automatická detekce a zobrazování hostname na základě zpracování aktuálních dat z DNS a DHCP provozu,
- IP reputace, vč. údaje, jestli je IP adresa blacklistovaná nebo podezřelá,
- zobrazování síťových toků příslušných k detekované události MAC adresa a výrobce zařízení,

Monitoring výkonu aplikací

Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty (thresholdy) nebo jiné parametry) vytváří model normálního chování pro výkonnostní parametry minimálně odezva sítě, odezva aplikace a odezva z pohledu uživatele.

Zaznamenávání a ukládání plného provozu

Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6.

Jednotné grafické rozhraní

Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, konfigurace alertů, reportů a dashboardů.

Uživatelské profily a nastavení

Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:

- granulární nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu,
- granulární nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),
- vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.

Požadavky na procesní zpracování kybernetických událostí

Management bezpečnostních událostí a incidentů

Systém musí poskytovat integrované rozhraní pro:

- reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),
- spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,
- jednoduché sdílení informací o bezpečnostních incidentech, možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).

Účast v ISIRT týmu

Tato skupina činností představuje řešení kybernetických bezpečnostních událostí a incidentů ve spolupráci s NÚKIB.

Požadavky na integraci, reporting a alerting

Integrace

Systém musí být schopen rychlé a jednoduché uživatelské integrace s nástroji třetích stran bez vyžití složitých nástrojů jako API minimálně s:

- nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,
- nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů jako výše.

Automatické bezpečnostní hlášení (alerty)

Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a SNMP trap o:

- všech identifikovaných událostech,
- událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.

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 aplikace.

Možnost automatizovaného reportingu

Možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email, apod.).

Je požadována podpora reportů v českém jazyce.

Implementační práce a dokumentace

Instalace veškerých dodaných hardwarových komponent do racku včetně instalace veškeré kabeláže

Dokumentace je požadovaná v českém jazyce.

Dokumentace musí obsahovat minimálně:

- popis dodaného nástroje a jeho případných komponent (výrobce, typ, sériové číslo, servisní číslo, licence),
- textový popis fungování řešení jako celku,
- název nástroje (zařízení) v síti Zadavatele, jeho IP adresy a všechna přidělená jména,
- detailní nákres a popis zapojení (porty nástroje a jejich konfigurace, VLAN, konfigurace portů aktivních prvků, ke kterým je nástroj připojen),
- popis přístupů ke správě nástroje: použité rozhraní (LAN, USB apod.), adresa rozhraní, způsob přístupu (webový prohlížeč, SSH apod.),

- přehled přístupových údajů k nástroji tak, aby Zadavatel měl po převzetí neomezený přístup ke všem částem a komponentám nástroje.

Popis přístupu k technické podpoře nástroje: kontaktní údaje, autentizační údaje, pravidla pro komunikaci s technickou podporou.

Technická podpora

Dodavatel garantuje vzdálenou podporu min. formou emailu a telefonní hot-line v režimu 8x5 v českém jazyce.

Dodavatel zajištuje možnost eskalovat kritické incidenty na podporu výrobce.

Servisní podpora výrobce na aktualizaci SW na min. 5 let. Podpora obsahuje vždy aktuální verze SW a opravy chyb.

Podpora pro zajištění výukového programu a demonstraci cyber aktivit

Dodavatel garantuje zajištění demonstračního provozu pro průběh výuky.

Jedná se o:

- Zajištění pcap souborů obsahujících reálné síťové útoky pro opakovanou analýzu studenty
- Zajištění prostředí pro simulované posílání zaznamenaných dat z pcap souborů z open source nástrojů ve virtualizačním prostředí VMware.
- Zajištění 4h/rok prezentace školení používání dodaného nástroje pro studenty.

Je předpokládána celková pracovní náročnost 5 člověko dnů.

Příloha č. 2 - TECHNICKÁ SPECIFIKACE NGFW

Pokud tento dokument obsahuje požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, která platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, je taková specifikace brána pouze jako typová. Je přípustné veškerý takto specifikovaný materiál nahradit jiným ekvivalentem, u kterého dodavatel garantuje, že bude mít minimálně shodné vlastnosti, technické a kvalitativní parametry a zajistí dodržení všech požadovaných technických a uživatelských standardů.

Obecné požadavky

Za účelem zabezpečení síťového perimetru je požadována dodávka 2 ks zařízení typu Next Generation Firewall (dále jen NGFW) ve formě hardware appliance s podporou výrobce v řežimu 24x7 a aktualizací všech požadovaných bezpečnostních funkcí po dobu 5 let.

Základní požadavky

- 2x hardware appliance o velikosti 1 RU
- Podpora režimu vysoké dostupnosti (active/active i active/passive)
- Správa zařízení pracujících v režimu vysoké dostupnosti musí probíhat skrze jedno konfigurační rozhraní, je požadována automatická synchronizace provozních a stavových informací mezi jednotlivými zařízení v jednom celku vysoké dostupnosti
- Podpora virtualizace uvnitř hw appliance formou vytváření virtuálních kontextů
- Musí umožňovat práci přes grafické konfigurační rozhraní a příkazový řádek
- Minimální počty požadovaných síťových rozhraní (portů):
  - 12x GE RJ 45
  - 8x GE SFP
  - 2x 10 GE SFP+, SFP+ Short Range moduly musí být součástí dodávky
  - Management rozhraní 1x RJ 45
  - Konzole sériové linky pro přístup k příkazovému řádku
- Redundantní zdroj napájení, každý s min. 100-240 V AC
- Podpora plnohodnotné inspekce sítového provozu minimálně v režimech:
  - NAT/router
  - L2 transparentní režim (dva a více sítových rozhraní)
  - L2 interface pair (dvě sítové rozhraní)

Výkonové požadavky

Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání.

- Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz musí být 18 Gbps (udp pakety o velikosti 512 B)
- Minimální počet současně navázaných spojení firewallu 1.5 M
- Minimální počet nových spojení za sekundu 50 tisíc
- Výkon zařízení min. 15 M paketů / sekundu
- Propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)
  - Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) min. 1.5 Gbps

    - Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 1 Gbps
    - Propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 2.5 Gbps
    - Propustnost funkce rozpoznávání sítových aplikací na L7 min. 2 Gbps
- Propustnost IPSEC VPN v konfiguraci AES256/SHA256 min. 10 Gbps
- Propustnost funkce SSL inspekce provozu min. 1 Gbps
- Počet konfigurovatelných virtuálních kontextů na každém zařízení min. 10

Funkční požadavky

- Podpora a zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) minimálně s ohledem na tyto bezpečnostní funkce:
    - Funkce rozpoznávání kancelářských a průmyslových aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací a 700 průmyslových aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly musí být možné uspořádat do kategorií; Databáze podporovaných aplikací musí být automaticky aktualizována min. po celou dobu platné podpory výrobce nabízeného NGFW
    - Funkce ochrany před síťovými útoky vycházející z aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min. 10 000 signatur v databázi; podpora zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) min. po celou dobu platné podpory výrobce nabízeného NGFW
    - Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předání zkoumaných souborů pro analýzu v prostředí typu sandbox
    - Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, vycházející z aktualizované databáze min. po celou dobu platné podpory výrobce nabízeného NGFW
    - Funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky z SSL inspekce požadujeme minimálně:
        - na základě administrátorem definovaných adres
        - na základě kategorie URL, vycházející z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví, atd.)
- Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
- Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky
- Funkce QoS, traffic shaping
- Funkce klientské VPN (přístup do vpn v tunelovém režimu s vpn klientem a přístup do vpn přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů; ssl vpn nebo ipsec vpn)
- Site-to-site ipsec vpn s podporou statického i dynamického routování
- Podpora OT/ICS/IoT protokolů (minimálně klasifikace provozu, identifikace zařízení, ochrana zařízení před síťovým útokem)

Příloha č. 2 - TECHNICKÁ SPECIFIKACE
PRO INTEGROVANÝ BEZPEČNOSTNÍ PROVOZNÍ NÁSTROJ (DDI/IPAM/NAC) + L2 MONITORING

Pokud tento dokument obsahuje požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, která platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, je taková specifikace brána pouze jako typová. Je přípustné veškerý takto specifikovaný materiál nahradit jiným ekvivalentem, u kterého dodavatel garantuje, že bude mít minimálně shodné vlastnosti, technické a kvalitativní parametry a zajistí dodržení všech požadovaných technických a uživatelských standardů.

Obecné požadavky

- Zavedení L2 monitoringu pro jednoznačnou lokalizaci zařízení v síti
- Zavedení integrovaného systému správy IP adresního prostoru, a základních síťových služeb – DHCP a DNS
- Zavedení NAC – řízení přístupu do sítě formou 802.1x/MAC autentizace a následné autorizace (řízení přístupu zařízení do VLAN)

Systém pro integrovaný bezpečnostní provozní nástroj (DDI/IPAM/NAC) + L2 monitoring

- Zavedení sofistikovaného adresního plánování, ověření stavu sítě formou detailního L2 monitoringu (IP/MAC/lokalita/port) a zavedení integrovaných DHCP a DNS služeb
- Zavedení NAC funkcionality – formou 802.1x/MAC autentizace s následným přiřazením zařízení do VLAN (autorizace). Tato funkcionalita bude k dispozici rovněž pro možné budoucí rozšíření pro BYOD a mobilní zařízení, kde navíc budou zavedeny nástroje pro jejich automatizovanou administraci uživateli (samoobslužný portál) nebo pracovníky recepce (guest zóny).
- Systém bude nasazen ve virtuálním prostředí (řídící server). Pro zajištění maximální provozní spolehlivosti budou dodány fyzické appliance, na kterých budou provozovány workservery.
- Systém umožňuje nastavení integrace se systémem ADS, který může systém velmi vhodně doplňovat v oblasti Flow monitoringu a pokročilé Behaviorální analýzy sítě.

Rozsah nasazení

- Centralizované nasazení s centrálním řízením a zálohou
- IPAM – Adresní plánování
    - do max. 100 síťových zařízení
- Kompletní L2 monitoring
    - IP/MAC/lokalita/aktivní_prvek/port s úplnou historií pro forenzní audit
- Integrovaný DDI – DHCP, DNS servery, připravené na distribuované nasazení

- NAC modul – integrovaný Radius server připravený na distribuované nasazení

- SIO – Switch interoperability modul (Komunikace s aktivními prvky)
    - utilizace aktivních prvků na úroveň portu
    - přiřazení zařízení ke konkrétnímu portu aktivního prvku
    - zálohování konfigurací aktivních prvků

- NAC modul (Řízení přístupu do sítě)
    - 802.1x/MAC autentizace a autorizace

Požadované výstupy řešení

- Detailní L2 monitoring - jednoznačná lokalizace zařízení v síti a úplná historie stavu sítě

- DDI – zavedení integrovaných vysoce spolehlivých základních síťových služeb DDI (IPAM/DHCP/DNS)

- NAC – snadné zavedení a správa (802.1x / MAC autentizace s ochranou a následnou autorizací)

- BYOD – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení

- Podstatné zvýšení provozní spolehlivosti DDI/NAC služeb díky vícenásobné redundanci a nadstandardní škálovatelnosti

- Plná heterogennost - bezproblémová spolupráce běžnými síťovými technologiemi

- Možnost návazné integrace s nástrojem ADS pro zrychlení a zjednodušení administrátorských zásahů v případě řešení bezpečnostních incidentů

Podpora technologií zahrnuje

- Službu produktového update – poskytování bezplatných nových verzí software

- Službu poskytování prodloužené záruky na softwarové produkty (po dobu placení podpory 5 let)

- Službu helpdesk – telefonická podpora v pracovní době 9-17 a elektronická podpora 24x7 - příjem požadavků na technickou pomoc (hlášení vad)

- Základní úroveň SLA podpory – garantovaný response-time 8 pracovních hodin na zahájení řešení problémů

- Službu systémového update – poskytování nových verzí a bezpečnostních update pro hw appliance

Příloha č. 2 - TECHNICKÁ SPECIFIKACE POKROČILÁ OCHRANA KONCOVÝCH BODŮ VČETNĚ OCHRANY VIRTUALIZAČNÍCH PLATFOREM A EDR

Pokud tento dokument obsahuje požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, která platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, je taková specifikace brána pouze jako typová. Je přípustné veškerý takto specifikovaný materiál nahradit jiným ekvivalentem, u kterého dodavatel garantuje, že bude mít minimálně shodné vlastnosti, technické a kvalitativní parametry a zajistí dodržení všech požadovaných technických a uživatelských standardů.

Obecné požadavky

Řešení musí umožnit zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux.

Řešení pro komplexní ochranu PC, Linux, Mac, fyzické a virtuální serverové infrastruktury musí být spravováno z jedné on-premise webové konzole.

Musí být zajištěna technická podpora výrobce nebo jeho zastoupení v českém jazyce ve formě telefonické i písemné v režimu min. 8x5 po celou dobu platnosti licence.

Uživatelské prostředí a správa řešení musí být lokalizováno do českého jazyka, včetně instalačního návodu.

Detailní požadavky na správu a funkcionalitu

1. **Konzole pro centrální správu řešení:**
   - Řešení musí mít komponentu správy dodanou jako jednotnou virtuální appliance (virtuální image), která obsahuje všechny role/služby. Image musí být kompatibilní s virtualizační platformami:
     a. VMware vSphere, View;
     b. Citrix XenServer, XenDesktop, VDI-in-a-Box;
     c. Microsoft Hyper-V;
     d. Red Hat Enterprise Virtualization;
     e. Kernel-based Virtual Machine či KVM;
     f. Oracle VirtualBox

   - Řešení konzole centrální správy musí být dodáno včetně databáze

   - Jakákoliv role/služba centrální správy může být instalována samostatně nebo na stejném virtuálním stroji jako další role/služby

- Musí umožňovat nastavení řešení ve vysoké dostupnosti minimálně pro komunikaci koncových stanic se serverem centrální správy, připojení administrátorů ke konzoli centrální správy, dostupnost databáze celého řešení a dostupnost aktualizací pro koncové stanice

- Musí umožňovat jednoduchou aktualizaci architektury – jedním kliknutím se provede aktualizace celého řešení

- Možnost napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce

- Možnost naplánovat zálohu databáze centrální konzole do síťové lokality přímo v uživatelském rozhraní správcovské konzole (bez nutnosti použití řešení třetí strany)

- Možnost restartování serveru nebo desktopu přímo z konzole centrální správy

- Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)

- Možnost nastavit tzv. centrální karanténu, pro dostupnost souborů v karanténě i v případě odpojení koncové stanice

- Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)

- Možnost nastavení více předdefinovaných rolí uživatelům např.
  a. Hlavní: spravuje komponenty řešení
  b. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení
  c. Uživatel: spravuje a vytváří reporty

- Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení

- Přístup k webové správě musí být zabezpečený (HTTPS)

- Webový server musí umožnit import digitálních certifikátů vydaných licencovanou certifikační autoritou nebo vlastní organizací přímo z konzole centrální správy bez zásahu technické podpory dodavatele či výrobce

- Musí umožňovat před instalací administrátorskou volbu, které moduly ochrany mají být nainstalovány

- Instalace může být provedena několika způsoby, alespoň:
  a. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován
  b. Instalace vzdáleně přímo z konzole správy

c. Distribuce instalačního balíčku pomocí GPO či SCCM

- Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN

- Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů

- Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou

- Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)

2. Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):

- Podpora operačních systémů:
  a. Windows 7 a vyšší
  b. Windows Server 2008 R2 a vyšší
  c. Ubuntu 14.04 LTS a vyšší
  d. Red Hat Enterprise Linux
  e. CentOS 6.0 a vyšší
  f. Mac OS X El Capitan (10.11) a vyšší včetně MAC s procesory M1

- Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)

- Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru

- Aktualizace bezpečnostního obsahu alespoň jednou za hodinu

- Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)

- Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
- Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)

- Detekce O-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení

- Detekce O-day útoků na základě odhalování anomálního chování

- Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení

- Detekce 0-day bezsouborových útoků

- Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)

- Ochrana souborů proti zašifrování Ransomware spuštěném na chráněné stanici – automatické ukončení procesu ransomware a obnovení zašifrovaných souborů do původního stavu

- Ochrana sdílených složek/souborů proti zašifrování Ransomwarem spuštěném na jiné stanici s přístupem k těmto sdíleným složkám/souborům – automatické ukončení spojení z nakažené stanice a obnovení zašifrovaných souborů do původního stavu

- Možnost automatické detonace podezřelých souborů v Sandboxu

- Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne

- Možnost ručního vložení vzorku do Sandboxu

- Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP

- Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy

- Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.

- Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku

- Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování

- Ochranu proti podvodným a phishingovým webovým stránkám

- Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID

- Application Whitelisting - Detekce aplikací na koncových stanicích a možnost blokace spouštění všech procesů a aplikací, které nebudou výslovně povoleny

- Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)

- Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS

- Řešení musí umožňovat připojení na konzoli koncové stanice s možností výpisu procesů, registrů a souborů, vytvoření, změnu či výmaz souborů či registrů a ukončení procesu

-

3. Ochrana virtualizovaných koncových bodů (Windows, Linux)

- Produkt umožňuje integraci s VMware vShield, VMware NSX-V a VMware NSX-T

- Komponenta centrální správy umožňuje integraci s několika VMware vCentry

- Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzv. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné, aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen

- „Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením

- Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)

- Detekce na základě virových definicí (tzn. signatur)

- Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP