Smlouva č. 195310222
o provedení školení IT specialistů – speciální

I.
Smluvní strany

Česká republika – Ministerstvo obrany
Se sídlem: Tychonova 1, 160 01 Praha 6
IČO: 60162694
DIČ: CZ60162694
Bankovní spojení: Česká národní banka, pobočka Praha, Na Příkopě 28, Praha 1
Číslo účtu: 404881/0710
Zastoupená: [redacted]
Se sídlem na adrese: Sekce vyzbrojování a akvizic MO
odbor komunikačních a informačních systémů
nám. Svobody 471/4
160 01 Praha 6
Informační systém datových schránek (dále jen „ISDS"):
Identifikátor datové schránky: hjyaavk
Kontaktní osoba ve věcech smluvních:
Vendula Tajčová, tel.: +420 973 225 225
Kontaktní osoba ve věcech technických:
[redacted]
Adresa pro doručování korespondence:
Sekce vyzbrojování a akvizic MO
odbor komunikačních a informačních systémů
nám. Svobody 471/4
160 01 Praha 6
(dále jen „objednatel")

a

Everesta, s.r.o.
Zapsaná v obchodním rejstříku u Krajského soudu v Ústí nad Labem, oddíl C, vložka č. 10957
Se sídlem: Mimoňská 3223, 470 01 Česká Lípa
IČO: 25014650
DIČ: CZ25014650
Bankovní spojení: ČSOB
Číslo účtu: 676314683/0300
Zastoupená: [redacted]
ISDS: Identifikátor datové schránky: nfy2yvg
Kontaktní osoba: [redacted]
Telefonické a e-mailové spojení:
[redacted]
Adresa pro doručování korespondence: Mimoňská 3223, 470 01 Česká Lípa
(dále jen „poskytovatel").

Smluvní strany se dohodly, že ve smyslu ustanovení § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“) uzavírají na nadlimitní veřejnou zakázku, zadanou v otevřeném řízení podle ustanovení § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, tuto smlouvu o provedení školení IT specialistů – speciální (dále jen „smlouva“).

II.
Účel smlouvy

Účelem smlouvy je pořízením školení zabezpečit odbornou úroveň personálu potřebnou k zajištění provozu komunikačních a informačních systémů resortu Ministerstva obrany a tím zkvalitnit a zvýšit odbornou profesionalitu pracovníků.

III.
Předmět smlouvy

1. Poskytovatel se zavazuje poskytovat objednateli školení IT specialistů v českém (příp. slovenském nebo anglickém) jazyce, přičemž podrobný popis jednotlivých školení, vč. počtu osob, je uveden v příloze č. 1 této smlouvy „Specifikace předmětu smlouvy“ (dále jen „školení“).
2. Objednatel se zavazuje zaplatit poskytovateli za řádně a včas poskytnuté školení dohodnutou cenu podle čl. IV. této smlouvy.

IV.
Cena za školení

1. Cena za provedené školení podle čl. III. této smlouvy byla stanovena dohodou smluvních stran v souladu s ustanovením zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů.
2. **Celková cena** za školení, která budou po dobu platnosti a účinnosti této smlouvy poskytovatelem provedena, činí **maximálně 1.324.897,60 Kč bez DPH** (slovy: jeden milion tři sta dvacet čtyři tisíc osm set devadesát sedm korun českých šedesát haléřů), tj. **1.603.126,10 Kč vč. 21% DPH.**
3. Cenová specifikace jednotlivých školení je uvedena v příloze č. 2 této smlouvy „Cenový rozklad“. Skutečná cena za školení se vypočítá jako součin počtu skutečných účastníků účastnících se školení dle akceptačního protokolu a ceny za jednoho školeného účastníka daného školení dle přílohy č. 2 této smlouvy.
4. Celková cena bez DPH dle odst. 2 tohoto článku smlouvy je cenou nejvýše přípustnou a není ji možno překročit. Tato cena zahrnuje veškeré náklady poskytovatele spojené s plněním svých závazků (tj. zejména nákladů na dodání veškeré potřebné dokumentace, certifikátů atd.).
5. Daň z přidané hodnoty bude po celou dobu platnosti této smlouvy uplatňována v sazbě podle platného znění zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

V.
Místo a doba plnění

1. Místem pro realizaci jednotlivých školení je školicí středisko poskytovatele nebo jeho poddodavatele na adrese: Opletalova 919/5, Praha 1.
2. Poskytovatel je povinen provést všechna školení **nejpozději do 30. 11. 2019**.

VI.
Podmínky plnění

1. Pověřenou osobou k akceptaci plnění je [redacted] (dále jen „zástupce objednatele").
2. Poskytovatel je povinen dodat zástupci objednatele **kompletní dokumentaci** v rozsahu školících materiálů v českém, resp. anglickém jazyce, pro každého účastníka školení ještě před zahájením samotného školení, a to v papírové nebo elektronické podobě. Poskytovatel souhlasí s možností rozmnožování dodané dokumentace bez omezení pro potřeby objednatele. U dokumentace, ke které dodavatel nevlastní autorská práva, zabezpečí souhlas majitele těchto práv.
3. Poskytovatel je povinen každé školené osobě vydat v poslední den školení **certifikát** dokládající absolvování jednotlivých školení.
4. Poskytovatel je povinen zpracovat **časový harmonogram** provedení jednotlivých školení, který bude odsouhlasen zástupcem objednatele. Poskytovatel je povinen předložit harmonogram zástupci uživatele k akceptaci nejpozději do 21 dnů od účinnosti smlouvy.
5. Poskytovatel je povinen vyhotovit na konci každého měsíce **akceptační protokol**, který podepíše zástupce objednatele. Akceptační protokol musí obsahovat název provedeného školení, skutečný počet účastníků objednatele na školení, informaci o převzetí kompletní dokumentace a certifikátu, příjmení a jméno zástupce objednatele. Akceptační protokol bude vyhotoven ve třech výtiscích, z nichž dva obdrží poskytovatel. Jeden z těchto výtisků je poskytovatel povinen přiložit k faktuře. Další výtisk obdrží zástupce objednatele.
6. Poskytovatel je povinen umožnit objednateli kdykoliv kontrolu plnění svých závazků. Zjistí-li objednatel, že poskytovatel provádí školení v rozporu s ustanovením této smlouvy a svými povinnostmi, je objednatel oprávněn se písemně dožadovat toho, aby poskytovatel odstranil vady vzniklé vadným prováděním školení a školení prováděl řádným způsobem. Jestliže tak poskytovatel bezodkladně neučiní, jeho postup bude chápán jako podstatné porušení smlouvy a objednatel bude oprávněn od smlouvy odstoupit.
7. Zástupce objednatele je povinen zabezpečit účast školených osob v místě a v době dohodnuté se zástupcem poskytovatele.
8. Zástupce objednatele poskytne potřebnou součinnost poskytovateli pro plnění předmětu smlouvy.

VII.
Fakturační a platební podmínky

1. Smluvní strany se dohodly, že objednatel nebude poskytovat za plnění předmětu této smlouvy zálohové platby.

2. Úhrada ceny dle čl. IV. této smlouvy bude prováděna jednou měsíčně za školení uskutečněná (tzn. odsouhlasená a potvrzená na příslušném Akceptačním protokolu) v předchozím kalendářním měsíci na základě daňového dokladu – faktury (dále jen „faktura"). Příslušná faktura bude objednateli doručena vždy nejpozději do 10. dne následujícího kalendářního měsíce. Faktura bude vyhotovena ve **2 výtiscích (originál a kopie)** v českém jazyce.

3. K faktuře musí být připojen **akceptační protokol ve 2 výtiscích (originál a kopie)**, který bude obsahovat výčet poskytnutého plnění a bude podepsán zástupcem objednatele a poskytovatele.

4. Na faktuře bude uvedena tato adresa objednatele:
   Česká republika - Ministerstvo obrany
   Tychonova 1
   160 01 Praha 6
   IČO: 60162694, DIČ: CZ60162694
   v zastoupení
   Sekce vyzbrojování a akvizic MO
   odbor komunikačních a informačních systémů
   nám. Svobody 471/4
   160 01 Praha 6

5. Faktura musí obsahovat náležitosti stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a § 435 OZ. Kromě toho musí obsahovat tyto údaje a náležitosti:
   - označení dokladu jako „Daňový doklad – faktura" s uvedením evidenčního čísla;
   - obchodní firmu nebo jméno a příjmení, popřípadě název, dodatek ke jménu a příjmení nebo názvu, sídlo a místo podnikání poskytovatele s uvedením IČO a DIČ;
   - název a sídlo objednatele s uvedením IČO a DIČ;
   - číslo smlouvy, podle které se uskutečňuje plnění;
   - rozsah a předmět plnění;
   - jednotkovou cenu v Kč bez DPH a včetně DPH a cenu za školení celkem v Kč bez DPH a včetně DPH;
   - označení peněžního ústavu a čísla účtu poskytovatele, na který má být poukázána platba;
   - počet příloh a razítko s podpisem odpovědné osoby poskytovatele za vystavení faktury.

6. Faktura bude poskytovatelem zaslána objednateli na adresu:
   Sekce vyzbrojování a akvizic MO
   odbor komunikačních informačních systémů
   nám. Svobody 471/4
   160 01 Praha

7. Lhůta splatnosti faktury je 30 dnů ode dne jejího doručení objednateli. Bude-li faktura doručena objednateli v období od 15. prosince příslušného kalendářního roku do 15. ledna roku následujícího, prodlužuje se splatnost takové faktury o 30 dnů. Faktura je považována za uhrazenou dnem odepsání příslušné částky z účtu objednatele a jejím směrováním na účet poskytovatele.

8. Všechny částky v Kč poukazované mezi objednatelem a poskytovatelem na základě smlouvy musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů spojených s převodem na jejich účty.

9. Případný opravný daňový doklad je poskytovatel povinen vystavit a doručit objednateli do 14 dnů od vyžádání objednatelem. Doba splatnosti opravného daňového dokladu, tj. den připsání příslušné částky na účet objednatele, je 30 dnů ode dne jeho doručení.

10. Objednatel je oprávněn fakturu bez jejího uhrazení ve lhůtě její splatnosti vrátit, neobsahuje-li požadované náležitosti, není doložena požadovanými doklady nebo obsahuje nesprávné cenové údaje a náležitosti. Pro zachování lhůty pro vrácení faktury postačí její odeslání poskytovateli v době její splatnosti. Vrácení faktury musí objednatel písemně zdůvodnit. V případě jejího oprávněného vrácení poskytovatel vystaví novou fakturu. Vrácením faktury přestává běžet původní lhůta splatnosti a běží nová 30 denní lhůta splatnosti ode dne doručení nové (opravené) faktury objednateli. Poskytovatel je povinen novou fakturu doručit objednateli do 10 dnů ode dne doručení oprávněně vrácené faktury poskytovateli.

11. Pokud budou u poskytovatele zdanitelného plnění shledány důvody k naplnění institutu ručení za daň podle § 109 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude objednatel při zasílání úplaty vždy postupovat zvláštním způsobem zajištění daně podle § 109a tohoto zákona.

VIII.
Smluvní pokuty a úroky z prodlení

1. V případě prodlení poskytovatele s plněním závazků dle čl. III. odst. 1 této smlouvy v termínech dle odsouhlaseného časového harmonogramu podle čl. VI. odst. 4 této smlouvy, je poskytovatel povinen zaplatit objednateli za každé jednotlivé školení a za každý i započatý den prodlení smluvní pokutu **ve výši 0,3 %** z celkové ceny daného kurzu školení bez DPH, a to až do úplného splnění závazku nebo do zániku smluvního vztahu. Tím nejsou dotčena ustanovení článku IX. smlouvy. Okamžik práva fakturace vzniká prvním dnem prodlení. Pro posouzení skutečnosti, že ze strany poskytovatele došlo ke splnění jeho závazku, jsou rozhodující údaje z příslušných akceptačních protokolů.

2. V případě porušení povinnosti poskytovatele uvedené v čl. VI. odst. 3 této smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši **10.000,- Kč** za každé jednotlivé porušení povinnosti zde specifikované.

3. Poskytovatel není v prodlení se splněním svého závazku z této smlouvy, pokud mu objednatel neposkytl součinnost nezbytnou k jeho splnění. Na neposkytnutí součinnosti je poskytovatel povinen objednatele obratem písemně upozornit, neučiní-li tak má se zato, že objednatel není s poskytnutím součinnosti v prodlení.

4. Uplatnění institutu smluvní pokuty podle smlouvy nevylučuje současné uplatnění nároků na náhradu škody v celém rozsahu. Smluvní pokuty a úrok z prodlení je odpovědná smluvní strana povinna uhradit bez ohledu na skutečnost, zda v důsledku porušení smluvních povinností došlo ke vzniku škody. Smluvní pokutu a úrok z prodlení je smluvní strana povinna uhradit nejpozději do 30 dnů po doručení jejich vyúčtování od strany oprávněné.

5. V případě prodlení s úhradou faktury, zaplatí povinná strana straně oprávněné úrok z prodlení v zákonné výši dle nařízení vlády za každý i započatý den prodlení.

IX.
Zánik smluvního vztahu

Smluvní strany se dohodly, že závazek ze smluvního vztahu zaniká v těchto případech:

a) splněním všech závazků řádně a včas,

b) písemnou dohodou smluvních stran, spojenou se vzájemným vyrovnáním účelně vynaložených a prokazatelně doložených nákladů,
c) jednostranným odstoupením od smlouvy pro její podstatné porušení některou ze smluvních stran s tím, že podstatným porušením smlouvy se rozumí neprovedení i jednotlivého školení řádně a/nebo včas a nedodržením ustanovení čl. VI. odst. 3 této smlouvy,
d) jednostranným odstoupením objednatele od smlouvy pro případ vyhlášení insolvenčního řízení vůči majetku poskytovatele, v němž bylo vydáno rozhodnutí o úpadku nebo byl-li vůči majetku poskytovatele insolvenční návrh zamítnut pro nedostatek majetku k úhradě nákladů insolvenčního řízení,
e) jednostranným odstoupením objednatele od smlouvy v případě, že zjistí, že poskytovatel uvedl v nabídce nepravdivé informace nebo doklady, které měly nebo mohly mít vliv na výsledek zadávacího řízení.
f) písemnou výpovědí objednatele i bez udání důvodu s 2 měsíční výpovědní lhůtou, přičemž výpovědní lhůta začne běžet dnem následujícím po dni doručení této výpovědi poskytovateli.

X.
Závěrečná ujednání

1. Smlouva je vyhotovena v elektronické podobě o 7 stranách se 2 přílohami o 4 stranách.

2. Smlouva může být měněna či doplňována vzájemně odsouhlasenými a podepsanými písemnými a vzestupně očíslovanými dodatky, které se stávají její nedílnou součástí. Za změnu smlouvy se nepovažuje změna identifikačních údajů některé ze smluvních stran, kontaktních údajů nebo oprávněných osob. Tato změna bude druhé smluvní straně písemně oznámena elektronickou cestou prostřednictvím ISDS nebo na e-mailovou adresu.

3. Smluvní strany se dohodly, že si bezodkladně sdělí skutečnosti, které se týkají změn některého ze základních identifikačních údajů, včetně právního nástupnictví.

4. Poskytovatel souhlasí, aby smlouva po jejím podpisu byla zveřejněna.

5. Vztahy mezi smluvními stranami se řídí právním řádem České republiky. Práva a povinnosti smluvních stran touto smlouvou výslovně neupravené se přiměřeně řídí příslušnými ustanoveními OZ.

6. Poskytovatel odpovídá za případné porušení práv z průmyslového, nebo jiného duševního vlastnictví třetích osob, jestliže jsou součástí poskytované služby.

7. Smluvní strany prohlašují, že jim nejsou známy žádné skutečnosti, které by uzavření smlouvy vylučovaly a berou na vědomí, že v plném rozsahu nesou veškeré právní důsledky plynoucí z vědomě jimi udaných nepravdivých údajů. Na důkaz svého souhlasu s obsahem smlouvy připojují pod ní své podpisy.

8. Jednacím jazykem při jakémkoliv ústním jednání či písemném styku souvisejícím s plněním této smlouvy je český jazyk.

9. Tato smlouva nabývá platnosti dnem jejího podpisu poslední smluvní stranou a účinnosti dnem zveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňováním těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

10. Nedílnou součástí smlouvy jsou přílohy:

Příloha č. 1 Specifikace předmětu smlouvy (3 strany)
Příloha č. 2 Cenový rozklad (1 strana)

Za objednatele:

[redacted]

podepsáno elektronicky

Za poskytovatele:

[redacted]

podepsáno elektronicky

Specifikace předmětu smlouvy

P.č.	Název školení	Obsah školení	Počet osob
1	Release, Control and Validation ITIL® Intermediate	• Service Management prakticky • Procesy umožňující nasazení, řízení a hodnocení služeb • Change management • Kontrola a testování služeb • Service Asset and Configuration Management • Knowledge Management • Service Request Fulfilment • Release and Deployment Management • Service Evaluation • Příprava a certifikační zkouška	4
2	Service Design ITIL® Intermediate	• Úvod do Service Design • Principy Service Design • Procesy Service Design • Aktivity v oblasti SD technologií • Organizace Service Design • Nástroje a technologie • Analýza a výběr implementačních hledisek, rizik, rozhodujících faktorů úspěchu • Příprava a certifikační zkouška	4
3	Service Transition ITIL® Intermediate	• Úvod do Service Transition • Principy Service Transition • Procesy Service Transition • Management a operativní řízení aktivit Service Transition • Aktivity ST v oblasti komunikace, úkolů a organizačních změn • Organizace Service Transition • Technologická hlediska • Analýza a výběr implementačních hledisk, rizik, rozhodujících faktorů úspěchu • Příprava a certifikační zkouška	4
4	ISO/IEC 27001 ISMS Foundation	• Využití ISMS (Information Security Management System). • Metodika pro splnění právních, regulačních a smluvních cílů organizace z pohledu informační bezpečnosti. • Techniky analýzy rizik. • Implementace Cyber Security Best Practice.	5
5	ISO/IEC 20000 Foundation	• Úvod do IT Service Managementu • ISO/IEC 20000: požadované znalosti • ISO/IEC 20000 certifikační schema • Využití ISO normy a návaznost na ITIL® • Service management procesy a požadavky • Implementace a posouzení požadavků normy • Jak se připravit na certifikaci a dále obstát u certifikačních auditů • Příprava a údržba IT Service Managementu v praxi: případové studie • Cvičné testy, příprava na certifikační test ISO/IEC 20000 Foundation • Certifikační test	4
6	ISO/IEC 27001 ISMS Intro	• ISMS podle ISO 27001 • zkušenosti ISO 27001 Lead Auditora	4
7	ISO/IEC 27001 ISMS Lead Auditor	• Práce s normou ISO/IEC 27001, principy systému managementu ISMS, přínosy a rizika systému, analýza rizik, politika – cíle ISMS, prohlášení o aplikovatelnosti, dokumentace ISMS, řízení bezpečnostních incidentů, řízení opatření k nápravě a preventivních opatření, řízení interních auditů. • Práce s normou EN ISO 19011, etapy interních auditů - plánování, provedení a vyhodnocení interního auditu systému managementu; simulace interního auditu v prostředí IT - zaměření na požadavky ISO/IEC 27001. • Role auditora bezpečnosti v systému managementu.	1

8	Mistrovství v etickém hackingu (HACK3)	• Kurz pro administrátory, kteří mají na starosti zabezpečení IT infrastruktury. • Rozšíření dovednosti účastníků z oblasti bezpečnosti a hackingu o komplexní testovací postupy a následné sestavení finální analýzy a reportingu.	6
9	Analýza útoků pro experty (HACK4)	• Nejnovější techniky v oboru analýzy a vyšetřování počítačových útoků a zajišťování důkazů o nich. • Shromažďování důkazů pro následné právní kroky a správné metody identifikace stop po kybernetickém napadení. • Moderní nástroje pro detekci stop po útočnících i při použití anonymizačních postupů, metody následné obnovy zničených či poškozených dat, a vypracování závěrečné zprávy včetně auditu pro prevenci podobných útoků v budoucnu.	6
10	Základy digitální forenzní analýzy	• Úvod do digitální forenzní analýzy • Reakce v reálném čase a sběr důkazů • Obsah registru Windows • Analýza artefaktů Windows • Forenzní analýza prohlížečů • Analýza e-mailů	1
11	Základy analýzy malwaru a reverzního inženýrství	• Cíle a techniky analýzy malwaru a reverzního inženýrství • Obsah Windows, spustitelné soubory, x86 asssembler • Techniky základní statické analýzy (extrakce řetězců, analýza importu, přehled vstupů spustitelných souborů, automatické rozbalování atd.) • Základní techniky pro dynamickou analýzu (debugging, monitorovací nástroje, zachytávání provozu atd.) • Analýza souborů .NET, Visual basic a Win64 • Techniky pro analýzu skriptů a nespustitelných souborů (dávkové soubory, Autoit, Python, Jscript, JavaScript, VBS)	1
12	Bezpečnost v prostředí Windows a internetových služeb (BZP1)	• Úvod do problematiky bezpečnosti • Protokol TCP/IP • Typy útoků • Charakteristika základních operačních systémů a útoků na ně • Obrana proti útokům • Doporučená opatření	2
13	Penetrační testování a etický hacking v sítích LAN (BZP3)	• Základní příkazy ve Windows 7 pro práci s uživateli, procesy, sítí, službami a registrem • Základy použití analyzátoru sítí Ethereal/Wireshark a Network Monitor v prostředí windows • Úvod do etického hackingu • Specializované skenery a jejich použití pro kontrolu WWW serverů • Základy virů, jejich dělení a postup odstranění virové nákazy spojený s praktickou ukázkou • Popis útoků na síťové vrstvě • Obcházení firewallů, IDS a honeypotů • Ochrana vzdálených přístupů pomocí VPN a možné potenciální útoky • Činnosti prováděné po zjištění napadení počítače	2
14	Zabezpečení bezdrátových sítí WIFI (BZP4)	• Úvod, princip činnosti a základy zabezpečení WiFi sítí. • Ukázka dohledání WiFi sítí v Linuxu a Windows – Wardriving. • Přehled standardů 802.11g a 802.11n. • Autentizační metody používané ve WiFi sítích. • Možnosti využití standardu 802.1x ve WiFi sítích. • Nedostatky a slabiny těchto sítí. • Ukázka zachycení provozu ve WiFi síti v prostředí Windows a Linux. • Nastavení a ověření funkce WiFi sítě na základě protokolové analýzy. • Útoky na WiFi sítě a přístupové body. • Pasivní útok hrubou silou na WEP klíč – ukázka. • Možnosti aktivních útoků na WEP, WPA a WPA2. • Doporučení pro nasazení autentizačních mechanismů ve WiFi prostředí. • Aspekty spolehlivosti WiFi sítě. • Použití falešného access pointu pro získání přístupu do WiFi sítě.	2

		• Návrh a ukázka protiopatření pro zvýšení bezpečnosti vaši WiFi sítě.	
15	Penetrační testování a etický hacking v sítích WAN (BZP6)	• Ohledání cílů v prostředí Internetu • Nástroje hackerů pro Linux a Windows • Trasování cesty k cíli a ohledání firewallů pomocí firewallkingu • Standardní a specializované skenery • Zjišťování zranitelnosti cílů ve WAN • Využití nalezených zranitelností pro získání a eskalaci práv na vzdáleném systému • Automatizace penetračních testů pomocí nástroje Metasploit • Základy psaní shell kódů, jejich dělení a postup ustavení spojení se vzdáleným cílem • Popis útoků na síťové vrstvě • Použití technik využívajících přetížení zásobníku • Obcházení firewallů, IDS a honeypotů • Demonstrace útoků na WWW a proxy servery • Ohledání služeb VPN na vzdálených systémech a možné útoky na VPN • Činnosti prováděné po zjištění napadení počítače	1
16	Synergy administration (H0LN3S)	• Introduce Composable Infrastructure and Synergy domains • Explore the functional architecture of the Synergy environment • Including management infrastructure • Compute modules • Interconnect modules • Local storage systems • Power and cooling	5
17	McAfee ePolicy Orchestrator a VirusScan Enterprise	• Instalace ePolicy Orchestrator • Webové rozhraní a dashboardy • System Tree a správa koncových bodů • Instalace a správa McAfee Agenta • Správa Extensions a Packages • Seznámení s VirusScan Enterprise • Instalace VirusScan Enterprise na koncový bod • On-Access a Access Protection politiky • Definice On-Demand skenu • Queries, Reporting a Automatic Responses	2
18	Upgrade z VirusScan Enterprise na ENS 10.5	• Novinky v ENS 10.5, popis modulů, jednotné zadávání pravidel • Architektura a příprava ePolicy Orchestratoru • Příprava na upgrade • Ověření kompatibility systémů • Výhody nástroje Upgrade Assistant • Migrace politik • Instalace na koncové stanice • Ladění politik a porovnání s předešlou architekturou	2

CENOVÝ ROZKLAD

P.č.	Název školení	Počet osob	Cena za školení 1 osoby v Kč bez DPH	Cena za školení 1 osoby v Kč vč. DPH	Cena za školení požadovaného počtu osob v Kč bez DPH	Cena za školení požadovaného počtu osob v Kč vč. DPH
1	Release, Control and Validation ITIL® Intermediate	4	34.840,00	42.156,40	139.360,00	168.625,60
2	Service Design ITIL® Intermediate	4	28.142,40	34.052,30	112.569,60	136.209,22
3	Service Transition ITIL® Intermediate	4	22.880,00	27.684,80	91.520,00	110.739,20
4	ISO/IEC 27001 ISMS Foundation	5	19.760,00	23.909,60	98.800,00	119.548,00
5	ISO/IEC 20000 Foundation	4	18.616,00	22.525,36	74.464,00	90.101,44
6	ISO/IEC 27001 ISMS Intro	4	6.240,00	7.550,40	24.960,00	30.201,60
7	ISO/IEC 27001 ISMS Lead Auditor	1	26.936,00	32.592,56	26.936,00	32.592,56
8	Mistrovství v etickém hackingu (HACK3)	6	25.480,00	30.830,80	152.880,00	184.984,80
9	Analýza útoků pro experty (HACK4)	6	25.480,00	30.830,80	152.880,00	184.984,80
10	Základy digitální forenzní analýzy	1	18.720,00	22.651,20	18.720,00	22.651,20
11	Základy analýzy malwaru a reverzního inženýrství	1	54.080,00	65.436,80	54.080,00	65.436,80
12	Bezpečnost v prostředí Windows a internetových služeb (BZP1)	2	11.336,00	13.716,56	22.672,00	27.433,12
13	Penetrační testování a etický hacking v sítích LAN (BZP3)	2	14.456,00	17.491,76	28.912,00	34.983,52
14	Zabezpečení bezdrátových sítí WIFI (BZP4)	2	13.312,00	16.107,52	26.624,00	32.215,04
15	Penetrační testování a etický hacking v sítích WAN (BZP6)	1	15.184,00	18.372,64	15.184,00	18.372,64
16	Synergy administration (H0LN3S)	5	39.520,00	47.819,20	197.600,00	239.096,00
17	McAfee ePolicy Orchestrator a VirusScan Enterprise	2	26.832,00	32.466,72	53.664,00	64.933,44
18	Upgrade z VirusScan Enterprise na ENS 10.5	2	16.536,00	20.008,56	33.072,00	40.017,12
Celková cena za školení					**1.324.897,60**	**1.603.126,10**

[redacted]

[redacted]