Smlouva č. 185310244
o provedení školení IT specialistů v oblasti Bezpečnost

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: [redacted]
Zastoupená: ředitelem odboru komunikačních a informačních systémů SVA MO
Ing. Petrem ZÁBORCEM
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.: [redacted]
Kontaktní osoba ve věcech technických:
ředitel VÚ 3255 Praha nebo jím písemně pověřená osoba
tel.: + [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

CyberGym Europe, a.s.
Zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 20766.
Se sídlem: Pobočná 1395/1, Michle, 141 00 Praha 4
IČO: 04200721
DIČ: CZ04200721
Bankovní spojení: Raiffeisen Bank
Číslo účtu: [redacted]
Zastoupená: Mgr. Martin Uher – předseda představenstva a JUDr. Petr Vališ – člen představenstva
ISDS: Identifikátor datové schránky: [redacted]
Kontaktní osoba: Ing. Luboš Rejl
Telefonické, faxové a e-mailové spojení: [redacted]
Adresa pro doručování korespondence: Lesní 210, 252 03 Řitka
(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 v oblasti Bezpečnost (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 (slovenském) jazyce v oblasti Bezpečnost. 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 článku 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 4.994.271,- Kč bez DPH** (slovy: čtyři miliony devět set devadesát čtyři tisíc dvě stě sedmdesát jedna korun českých), tj. **6.043.067,91 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 na adrese: Lesní 210, 252 03 Řitka.
2. Poskytovatel je povinen provést všechna školení **nejpozději do 30. 11. 2018**. Poskytovatel je povinen zabezpečit, aby školení, která na sebe odborně navazují, byla realizována v na sebe navazujících, nepřekrývajících se termínech tak, aby byla umožněna účast stejných pracovníků objednatele.

VI.
Podmínky plnění

1. Pověřenou osobou k akceptaci plnění je ředitel VÚ 3255 Praha, tel.: + 420 973 216 004, fax: +420 973 217 377 nebo jím písemně pověřená osoba (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 jak v papírové, tak 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 ve lhůtě **do 10 pracovních dní** od podpisu smlouvy, který bude odsouhlasen zástupcem objednatele.
5. Poskytovatel je povinen vyhotovit po ukončení každého jednotlivého školení **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, a to prostřednictvím zástupce objednatele. Zjistí-li zástupce objednatele, že poskytovatel provádí školení v rozporu s ustanovením této smlouvy a svými povinnostmi, je zástupce objednatele 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 provedená (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. 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

4. 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.

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

6. K faktuře musí být připojen **originál „Akceptačního protokolu"**, který bude obsahovat výčet poskytnutého plnění a bude podepsán zástupcem objednatele a poskytovatele.

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. této smlouvy v době plnění dle čl. V. této smlouvy, je poskytovatel povinen zaplatit objednateli za každé jednotlivé školení a za každý i započatý den prodlení smluvní pokutu ve výši 0,05 % z celkové ceny bez DPH dle čl. IV odst. 2 této smlouvy, 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 povinností poskytovatele uvedených v čl. VI. odst. 2 a 3 této smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 50.000,- 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 a 6 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.

X.
Závěrečná ujednání

1. Smlouva je vyhotovena ve dvou výtiscích o 7 stranách se dvěma přílohami o 7 stranách, z nichž každý má platnost originálu. Každá ze smluvních stran obdrží po jednom výtisku. Smluvní strany jsou oprávněné zhotovit si pro svou potřebu kopie této smlouvy.
2. Smlouva může být změněna nebo doplňována pouze písemnými oboustranně dohodnutými, vzestupně číslovanými 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 na adresu uvedenou v čl. I. smlouvy.
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 (6 stran)
Příloha č. 2 Cenový rozklad (1 strana)

V Praze dne 16.7.2018

Za objednatele:

Ing. Petr ZÁBOREC
ředitel
v zastoupení
[redacted]
Razítko a podpis

MO - Sekce vyzbrojování a akvizic

V Řitce dne 13.7.2018

Za poskytovatele:

Mgr. Martin UHER
předseda představenstva
[redacted]
Razítko a podpis

JUDr. Petr VALIŠ
člen představenstva
[redacted]
Razítko a podpis

CYBERGYM EUROPE
CyberGym Europe, a.s.
Pobočná 1395/1
141 00 Praha 4 - Michle
IČ: 04200721, DIČ: CZ04200721

Specifikace předmětu smlouvy

Název školení	Obsah školení	Počet osob
Zabezpečení sítí a hacking v praxi	• Opakování TCP/IP. • Odchytávání dat v síťovém analyzéru. • Vyhledávání informací z Internetových zdrojů. • Analýza prostředí a první útoky. • Hesla a jejich prolamování. • Bezdrátové sítě. • Pokročilejší útoky.	52
Certified Ethical Hacker	• Rozšířené získávání informací z internetových zdrojů – vyhledávače, extrakce metadat, automatické nástroje • Skenování sítí – nmap, amap, unicornscan, hping, idle scan, ARP • Enumerace - NetBIOS, DNS, SNMP, LDAP, metadata • Rozšíření technik MitM – DHCP starvation, VLAN Hopping, MAC flooding, APR, SPAN, skriptování, vetřelecká AP • Systémové útoky – lokální útok, dump hashů z RAM, skriptovací útoky, odposlech hashů, extrakce NT hashe z PPTP, hash injection, RainbowTables, CUDA • Trojské koně a backdoory – jak pracuje malware, BotNet, DDOS a jak jej snadno vytvořit a maskovat, Trojan Construction Kits • Viry a červy – definice typů a metodologie šíření • Sociální inženýrství – sociotechniky, falešné webové stránky, Spear phishing, deployment malwaru • Session Hijacking – zcizení TCP / HTTP session a krádež kybernetické identity • Hacking Web Serverů – DoS a DDoS, Bruteforcing, klonování, testování zranitelností, HTTP split, defacement • Hacking webových aplikací – mapování aplikací, XSS, CSRF, RFI, LFI, hidden field manipulation • SQL injection, LDAP injection • Hacking bezdrátových sítí – pokročilé techniky lámání WEP, WPA1/2-PSK, WPS, vetřelecká AP • Hacking mobilních platforem	29
Zranitelnost webových aplikací – praktická cvičení hackingu	• Úvod do HTTP protokolu • Útoky proti uživatelům • Útoky proti databázi • Útoky proti webové aplikaci	43
Praktické testování bezpečnosti webových aplikací	• Kurz určený vývojářům webových aplikací a začínajícím penetračním testerům, vedoucím pracovníkům IT (CIO) nebo managementu organizace, který je odpovědný za informační bezpečnost (CISO).	34
Bezpečnost Androidu a jeho aplikací včetně hackingu	• Architektura Android OS • Anatomie APK aplikací • Nástroje pro penetrační testování na platformě Android • Nejčastější zranitelnosti mobilních aplikací • Bezpečnostní mechanismy Androidu • Insecure Data Storage • Log Leakage • Reverzování APK aplikací	1

	• Statická analýza kódu • Broken Cryptography • Poor Authorization and Authentication • Insufficient Transport Layer Protection • APK repackage • Hidden APK • Client Side Injection • Obfuscace kódu • Weak Server Side Controls • Checklisty penetračního testování mobilních aplikací	
Ochrana proti hackingu webových aplikací v prostředí NET	• Čtyři základní zásady bezpečnosti • Trocha teorie na úvod • Zabezpečení platformy serveru • Zabezpečení kanálu síťové komunikace • Zabezpečení aplikace • Forms Authentication v ASPNET • Ukládání hesel • ASPNET Membership • ASPNET Roles • Zabezpečení dat šifrování	3
Analytický hacking – pro pokročilé, Certified Security Analyst	• Motivace pro sestavení bezpečnostní analýzy • Pokročilé hledání pomocí Google Hackingu • Analýza provozu TCP/IP • Pokročilé techniky odposlechu • Testování zranitelností pomocí Nessus a dalších skenerů zranitelností • Pokročilé testování bezdrátových sítí • Analýza provozu pomocí SNORTu • Pokročilé exploitace nástroje • Metodika pentestingu • Plánování a rozvrh penetračního testování • Sběr informací • Externí penetrační test • Penetrační testování intranetu • Testování síťové infrastruktury – routerů a switchů, firewallů, IDS, DOS útoků • Testování lámání hesel • Sociální inženýrství • Testování aplikací, fyzické bezpečnosti, databází, VoIP infrastruktury, VPN • Testování detekce virů a trojských koní, správy logů, BlueToth a přenosných zařízení, zabezpečení e-mailové komunikace • Sepisování reportů a výsledné dokumentace • Analýza reportů penetračních testů • Metodika implementace řešení nalezených zranitelností	10
Computer Hacking Forensic Investigator	• Proces forenzního vyšetřování • Prohledávání a zajišťování počítačů • Digitální důkazy • Reakce na útoky • Vytváření laboratorního prostředí pro zajišťování důkazů • Souborové systémy a prozkoumávání disků • Vyhledávání stop a zajišťování důkazů v OS Windows • Extrakce dat a vytváření kopií • Obnova smazaných souborů a oddílů	13

	• Zajišťování důkazů pomocí AccessData FTK • Zajišťování důkazů pomocí EnCase • Steganografie a její odhalování • Využívání nástrojů pro lámání hesel • Zajišťování logů a analýza síťového provozu • Zjišťování útoků na bezdrátové sítě • Zjišťování útoků na web • Zajišťování e-mailové komunikace, její vyšetřování a odhalování zločinu prostřednictvím e-mailu • Zajišťování důkazů z mobilních telefonů a počítačů • Vypracování vyšetřovacích zpráv	
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)	2
Pokročilá analýza malwaru a reverzní inženýrství včetně praktických ukázek	• Cíle a techniky analýzy malwaru a reverzního inženýrství • Pokročilé techniky statické a dynamické analýzy (manuální rozbalení) • Techniky deobfuskace • Analýza rootkitů a bootkitů • Analýza exploitů (pdf, doc, swf atd.) • Analýza malwaru pro alternativní operační systémy (Android, Linux, Mac OS)	1
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	3
Pokročilá digitální forenzní analýza	• Hloubková forenzní analýza Windows • Obnova dat • Forenzní analýza sítě a cloudu • Forenzní analýza operační paměti • Analýza časové osy	4
Windows Application Troubleshooting & Fighting Malware	• Architektura Windows • Procesy a thready • Memory management • Local Security Authority • Bezpečnostní subsystém • Aplikační monitoring • Nástroje Sysinternals • Filemon, regmon, procmon • Process explorer • TCP View • PSTools • Autoruns • Aplikační troubleshooting • User Account Control	2

	• Application Compatibility • 64-bit platforma • WOW • Fighting malware • Rootkity • RootkitRevealer • Ochrana proti malware • Data Execution Prevention • Service Hardening • Windows Firewall • Intrustion Detection/Prevention System • Forefront	
Network Security Administrator	• Principy počítačových sítí – úvodní rekapitulace TCPIP • Síťové protokoly, masky, aplikační protokoly • Hrozby fyzické bezpečnosti • Principy zabezpečení sítě, úkoly bezpečnostních administrátorů, auditorů • Úvod do bezpečnostních norem • Bezpečnostní politiky, klasifikace informací, incident handling • Hrozby síťové bezpečnosti – napíchnutí médií,skenování portů, CVE, trojské koně, červy, MitM, Buffer Overflow, Session Hijacking • Intrusion Detection System (IDS), Intrusion Prevention System (IPS) • Firewally – typy firewallů dle funkcionalit, fyzických řešení, úrovně v TCP/IP stacku • Packet filtering – sekvencování, fragmentace, kontrola flagů • Honeypoty – klasifikace dle velikostí, provozních sítí, architektury • Řešení problémů sítí – probírání strategie, nástroje pro řešení problémů a vyhodnocování slabé výkonnosti sítě, nejčastější typy problémů • Zabezpečování operačních systémů – práva a oprávnění, EFS, firewally,kerberos, IPSec • Správa updatů • Správa a analýza logů – typy logů, nástroje pro jejich parsování, strategie rotace logů • Aplikační zabezpečení – správa uživatelů, cookies, sessions, logování, SSL • Bezpečnost webových serverů – DDOS, reflection attack, XSS, CSRF, session hijacking, ověřování uživatelů, autorizace • E-mailová bezpečnost – servery, šifrování, protokoly, bezpečnostní rizika • Autentizace pomocí tokenu, Smart Card, RSA SecurID, principy podepisování a šifrování • VPN – principy, zprovozňování, audit, nejčastější chyby • Bezdrátové sítě – typy sítí, zranitelnosti, monitoring • Zajištění dostupnosti – cluster, strategie zálohování, redundance • Úvod do testování zranitelností sítě	2
Encryption Specialist	• Úvod do kryptografie a její vývoj • Symetrická kryptografie a hashe • Teorie čísel a asymetrická kryptografie • Aplikace šifrování	1
Příprava na certifikaci – Security	• Základy bezpečnosti • Bezpečnostní hrozby a zranitelnosti • Síťová bezpečnost • Zabezpečení aplikací, dat a prvků • Správa identit a přístupu • Správa PKI a certifikátů	1

	• Monitoring bezpečnosti • Zajištění dostupnosti, zachování chodu firmy a incident response	
Penetrační testování a etický hacking v sítích WAN	• 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 potenciální útoky na VPN • Činnosti prováděné po zjištění napadení počítače	1
Mistrovství v etickém hackingu kategorie 3 (praktické cvičení)	• Úvod do automatického testování • Metodika penetračních testů • Mapování sítě pomocí automatických nástrojů • Použití nástroje Nessus • Použití nástroje SNORT • Defaultní hesla • Backdoory a bugy v sítových prvcích • Testování síťové infrastruktury (routery, switche aj.) • Testování bezpečnosti webových aplikací • Použití nástroje Acunetix Vulnerability Scanner • Testovací metodika OWASP • Testování e-mailové komunikace • Testování mobilních aplikací • Reverzní inženýrství a mobilní aplikace • Hodnocení rizik a hrozeb • Tvorba reportů z penetračních testů • Sociotechnika a hacking HW prostředky • Autorun u vyměnitelných disků • Rubber Ducky • Bad USB • HW keylogery • HW Videologgery	3
Praktická analýza útoků pro experty kategorie 4	• DoS, DDoS útoky • Anonymizace a Proxy servery • Anonymizace a VPN • Anonymizační sítě (TOR) • BIOS • Logování ve Windows, v Linuxu, na síťových prvcích • Logování u internetových providerů a u provozovatelů internetových serverů • Získávání stop a zajišťování důkazů • Obnova smazaných souborů a oddílů v operačním systému Windows/Linux • Steganografie	1

	• Lámání hesel • Sledování emailové komunikace • Získávání důkazů z mobilních zařízení • Vypracovávání závěrečných vyšetřovacích zpráv	
ASA Firewall	• Úvod do problematiky firewallů (typy firewallů) • Cisco 5500 ASA - přehled modelů, vlastností a licencí • Základní konfigurace - princip bezpečnostních úrovní, základní inbound a outbound přístup • Správa firewallu - instalace, upgrade softwaru, řízení přístupu, syslog, SSH, telnet, password recovery • Rozšířená konfigurace - kontrola přístupu, filtrování dle obsahu, funkčnost protokolů na vyšších vrstvách, seskupování objektů, modulární politika, VLANy, směrování • Hloubková inspekce provozu - Deep Packet Inspection • AAA model - využití a konfigurace autentizace, autorizace a účtování • Konfigurace rozšířené síťové ochrany - Botnet Traffic Filter, Threat Detection • Nástroje pro troubleshooting - Packet Tracer, Capture • Cisco Adaptive Security Device Manager (ASDM) - grafické rozhraní a jeho využití při konfiguraci PIX a ASA • Konfigurace transparentního firewallu • Konfigurace virtuálního firewallu • Failover (základní failover, stateful failover, LAN Based failover) • Novinky v Cisco Firewallech	1
Firepower services	• Instalace Firepower modulu v ASA • Základní konfigurace FMC • Intrusion Policy • File Policy • Network Analysis Policy • DNS Policy, SSL policy • Identity policy (user agent)	1

Příloha č. 2 smlouvy č. 185310244

CENOVÝ ROZKLAD

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
Zabezpečení sítí a hacking v praxi	52	19.310,00	23.365,10	1.004.120,00	1.214.985,20
Certified Ethical Hacker	29	21.575,00	26.105,75	625.675,00	757.066,75
Zranitelnost webových aplikací – praktická cvičení hackingu	43	22.075,00	26.710,75	949.225,00	1.148.562,25
Praktické testování bezpečnosti webových aplikací	34	24.165,00	29.239,65	821.610,00	994.148,10
Bezpečnost Androidu a jeho aplikací včetně hackingu	1	29.120,00	35.235,20	29.120,00	35.235,20
Ochrana proti hackingu webových aplikací v prostředí NET	3	24.350,00	29.463,50	73.050,00	88.390,50
Analytický hacking – pro pokročilé, Certified Security Analyst	10	30.127,00	36.453,67	301.270,00	364.536,70
Computer Hacking Forensic Investigator	13	31.308,00	37.882,68	407.004,00	492.474,84
Základy analýzy malwaru a reverzního inženýrství	2	24.117,00	29.181,57	48.234,00	58.363,14
Pokročilá analýza malwaru a reverzní inženýrství včetně praktických ukázek	1	26.967,00	32.630,07	26.967,00	32.630,07
Základy digitální forenzní analýzy	3	25.750,00	31.157,50	77.250,00	93.472,50
Pokročilá digitální forenzní analýza	4	31.208,00	37.761,68	124.832,00	151.046,72
Windows Application Troubleshooting & Fighting Malware	2	34.630,00	41.902,30	69.260,00	83.804,60
Network Security Administrator	2	28.176,00	34.092,96	56.352,00	68.185,92
Encryption Specialist	1	36.997,00	44.766,37	36.997,00	44.766,37
Příprava na certifikaci – Security	1	34.868,00	42.190,28	34.868,00	42.190,28
Penetrační testování a etický hacking v sítích WAN	1	28.357,00	34.311,97	28.357,00	34.311,97
Mistrovství v etickém hackingu kategorie 3 (praktické cvičení)	3	39.880,00	48.254,80	119.640,00	144.764,40
Praktická analýza útoků pro experty kategorie 4	1	52.550,00	63.585,50	52.550,00	63.585,50
ASA Firewall	1	55.550,00	67.215,50	55.550,00	67.215,50
Firepower services	1	52.340,00	63.331,40	52.340,00	63.331,40
Celková cena za školení				**4.994.271,00**	**6.043.067,91**