[redacted]

Rámcová dohoda o provedení kurzů v oblasti IT - část 1.
Sp. zn. SpMO 16819/2022-1980

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:
Informační systém datových schránek (dále jen „ISDS“):
Identifikátor datové schránky: hjyaavk
Kontaktní osoba ve věcech smluvních: [redacted]
Kontaktní osoba ve věcech technických: [redacted]
Adresa pro doručování korespondence: [redacted]
(dále jen „objednatel“)

a

Poskytovatel:	**GOPAS, a.s.**
zapsaná v obchodním rejstříku	vedená Městským soudem v Praze, oddíl B, vložka 7753
Sídlo:	Kodaňská 1441/46, 101 00, Praha 10
IČ:	63911035
DIČ:	CZ63911035
jejímž jménem jedná:	Ing. Petr Daniel, předseda správní rady
Bankovní spojení:	[redacted]
Číslo účtu:	
Zástupce kupujícího oprávněný:	

jednat ve věcech technických:	[redacted]
kontakt:	
Datová schránka:	mi5ea5m
Adresa pro doručování korespondence:	Kodaňská 1441/46, 101 00, Praha 10

(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 veřejnou zakázku, malého rozsahu ve smyslu ustanovení § 27 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, tuto rámcovou dohodu o provedení vzdělávacích kurzů v oblasti IT (dále jen „*smlouva*“).

II.

Účel smlouvy

Účelem smlouvy je pořízením vzdělávacích kurzů k zabezpečení zvýšení kvalifikace a osvojení si znalostí a dovedností [redacted] a tím zkvalitnit a zvýšit jejich odbornou profesionalitu.

III.

Předmět smlouvy

1. Poskytovatel se zavazuje poskytovat na svůj náklad a nebezpečí pro objednatele vzdělávací kurzy v oblasti IT v českém jazyce v kurzech podrobně popsaných v příloze č. 1 této rámcové dohody „Specifikace předmětu smlouvy“ (dále jen „kurzy“) a to postupně po dílčích plněních (tj. po částech) a objednatel se zavazuje po částech tyto služby převzít a zaplatit dohodnutou cenu odpovídající poskytnutému kurzu. Po absolvování každého kurzu obdrží od poskytovatele posluchač osvědčení o absolvování kurzu.
2. Smluvní strany prohlašují, že předmět smlouvy není plněním nemožným, a že smlouvu uzavřely po pečlivém zvážení všech možných důsledků.

IV.

Cena za kurzy

1. Smluvní strany se ve smyslu zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, dohodly, že předpokládané plnění za trvání smlouvy je maximálně **862 980,00-Kč** bez DPH (slovy: osmsetšedesátdvatisícdevětsetosmdesát), tj. **1 044 205,80,- Kč vč. 21% DPH**. Cenová specifikace jednotlivých kurzů je uvedena v příloze č. 2 této smlouvy „Cenový rozklad“. Skutečná cena za kurzy se vypočítá jako součin počtu skutečných účastníků účastnících se kurzů dle akceptačního protokolu podle přílohy č. 4 a ceny za jednoho školeného účastníka daného kurzu dle přílohy č. 2 této smlouvy.

2. Celková cena dle odst. 1 tohoto článku smlouvy za poskytnuté plnění 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, školícího zázemí atd.).

3. 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. Tato rámcová dohoda se uzavírá do **30. 11. 2022**, a to ode dne podpisu rámcové dohody posledním z účastníků smlouvy.
2. Místem pro realizaci jednotlivých školení je školicí středisko poskytovatele nebo jeho poddodavatele na adrese: Kodaňská 1441/46, Praha 10 / Nové Sady 996/25, 602 00, Brno, Líbalova 2348/1, 149 00, Praha 4 (kurz IBM).
3. Poskytovatel zahájí jednotlivá školení ve stanoveném rozsahu a počtu účastníků podle dílčích objednávek objednatele a to nejpozději do 14 dnů od prokazatelného obdržení každé dílčí objednávky, nebude-li dohodnuto jinak.
4. Poskytovatel je povinen zabezpečit, aby kurzy, která na sebe v jednotlivých oblastech odborně navazují, byla realizována v na sebe navazujících, nepřekrývajících se termínech tak, aby byla umožněna účast stejných pracovníků objednatele.

VI.

Výzva k poskytnutí plnění a podmínky plnění

1. Osobou k akceptaci plnění [redacted] nebo jím písemně pověřená osoba (dále jen „zástupce objednatele“).
2. Výzvou k poskytnutí plnění (dále jen „Výzva“) se pro účely této smlouvy rozumí jednostranný úkon objednatele adresovaný poskytovateli ve smyslu čl. **VI. odst. 3.** této smlouvy, kterým objednatel specifikuje konkrétní dílčí plnění (tj. části služeb) co do rozsahu plnění, přičemž vzor výzvy k poskytnutí plnění je připojen jako příloha č. 3 této smlouvy.

   Objednatel je povinen vyplnit v dílčí výzvě tyto údaje:

   - číslo výzvy k poskytnutí plnění;
   - specifikaci dílčího plnění, tj. části služeb (zejména označení kurzu a upřesnění počtu posluchačů);
   - cenové údaje k dílčímu plnění;
   - den zahájení dílčího plnění (tj. části služeb); a
   - den ukončení dílčího plnění (tj. části služeb).
3. Objednatel zasílá poskytovateli výzvy prostřednictvím elektronického nástroje *Národní elektronický nástroj* nebo prostřednictvím e-mailové adresy [redacted] úkonem s označením „Výzva k poskytnutí plnění“, přičemž výzva poskytovatele je k úkonu „Výzva k poskytnutí plnění“ připojena jako její příloha.

4. Poskytovatel je povinen nejpozději do 5ti pracovních dnů ode dne uveřejnění úkonu „Výzva k plnění“ prostřednictvím elektronického nástroje *Národní elektronický nástroj*:

4.1 přijmout výzvu k plnění, a to prostřednictvím elektronického nástroje Národní elektronický nástroj, nebo:

4.2 sdělit objednateli na tel. č. + [redacted] a současně také prostřednictvím e-mailové adresy zadavatele [redacted] že Výzvu ve smyslu této rámcové dohody považuje za neplatnou včetně popisu všech jejich vad, přičemž neplatnou Výzvou k poskytnutí plnění se pro účely této smlouvy rozumí:

4.2.1 výzva k poskytnutí plnění, která není zadavatelem vyplněna ve všech svých částech tak, jak stanovuje tato smlouva;

4.2.2 výzva k poskytnutí plnění, ve které jsou vyplněné údaje v rozporu s touto smlouvou;

4.2.3 výzva k poskytnutí plnění, ve které jsou vyplněné údaje nad rámec stanovený touto smlouvou;

4.2.4 výzva k poskytnutí plnění, která není zadavatelem poskytovateli zaslána na příslušném formuláři; nebo

4.3 Výzva k poskytnutí plnění se považuje za schválenou a pro obě smluvní strany závaznou dnem jejího přijetí poskytovatelem ve smyslu čl. **VI. odst. 4.1** této smlouvy nebo marným uplynutím lhůty stanovené v čl. **VI. odst. 4.** této smlouvy.

4.4 S neplatnou Výzvou k poskytnutí plnění nejsou spojeny žádné účinky v souvislosti s touto smlouvou, vyjma povinnosti poskytovatele vyplývající z čl. **VI. odst. 3.** této smlouvy.

5. Poskytovatel je povinen dodat zástupci objednatele **kompletní dokumentaci** v rozsahu školících materiálů v českém jazyce, pro každého účastníka kurzu ještě před jeho samotným zahájením, a to v papírové nebo v 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.

6. Poskytovatel je povinen každé osobě účastnící se daného kurzu vydat v jeho poslední den konání **certifikát** dokládající jeho absolvování.

7. Poskytovatel je povinen vyhotovit na konci každého měsíce **akceptační protokol**, který podepíše zástupce objednatele. Akceptační protokol musí obsahovat název provedeného kurzu, skutečný počet účastníků objednatele na kurzu, 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.

8. 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 kurzů a kurzy prováděl řádným způsobem. Jestliže tak poskytovatel bezodkladně neučiní, jeho postup bude chápán jako podstatné porušení smlouvy a objednatel bude oprávněn od smlouvy odstoupit.

9. Zástupce objednatele je povinen zabezpečit účast školených osob v místě a v době dohodnuté se zástupcem poskytovatele.

10. 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 každé dílčí objednávky bude prováděna bezhotovostně po každém uskutečněném kurzu na základě daňového dokladu – faktury (dále jen „faktura"). Příslušná faktura bude objednateli doručena vždy nejpozději do 15. dne následujícího kalendářního měsíce. Faktura bude vyhotovena ve **2 výtiscích (originál a kopie)** v českém jazyce. K faktuře musí být připojen **originál „Akceptačního protokolu"**, který bude obsahovat výčet poskytnutého plnění a bude podepsán zástupcem objednatele a poskytovatele.

3. Na faktuře bude uvedena tato adresa objednatele:

Česká republika - Ministerstvo obrany
Tychonova 1
160 01 Praha 6
IČO: 60162694, DIČ: CZ60162694

[redacted]

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 kurz 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:

[redacted]

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. Příslušná částka odstupného dle **čl. IX. odst. 1.** této smlouvy bude stranou této smlouvy hrazena bankovním převodem na účet číslo 19-26030881/0710 vedený u České národní banky. Uhrazením se pro účely této smlouvy rozumí připsání předmětné peněžité částky na bankovní účet druhé strany.

VIII.

Smluvní pokuty a úroky z prodlení

1. V případě prodlení poskytovatele s plněním závazků dle **čl. III. odst. 1** této smlouvy v termínech a rozsahu stanovených objednatelem v dílčích objednávkách podle **čl. V. odst. 3** této smlouvy, je poskytovatel povinen zaplatit objednateli za každé jednotlivé školení (kurz) a za každý i započatý den prodlení smluvní pokutu ve výši 0,2 % z celkové ceny daného kurzu 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 ve smyslu ustanovení **čl. VII. odst. 2** této smlouvy.

2. V případě porušení povinnosti poskytovatele uvedené v čl. **VI. odst. 6** této smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 5.000,- 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.

Odstupné, odstoupení od smlouvy a zánik smluvního vztahu

1. Smluvní strany si ujednaly, že poskytovatel může závazek z této smlouvy zrušit zaplacením odstupného ve výši 10% z celkové ceny této smlouvy zaokrouhleno na celé stokoruny nahoru, ve smyslu ustanovení § 1992 OZ. Právo zrušit závazek zaplacením odstupného však nemá, pokud je poskytovatel v prodlení s plněním závazků nebo pokud i jen z části plnil objednateli.

2. 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.

3. Právo zadavatele ukončit závazek ze smlouvy na veřejnou zakázku i z jiných důvodů ve smyslu ustanovení § 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů není touto smlouvou dotčeno.

X.

Závěrečná ujednání

1. Smlouva je vyhotovena ve dvou výtiscích o 9 stranách se 4 přílohami o 12 listech, 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 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 sjednaly, že doručování se provádí na doručovací adresy uvedené v záhlaví této rámcové dohody, a to prostřednictvím osoby, která provádí přepravu zásilek (kurýrní služba), nebo prostřednictvím držitele poštovní licence podle zvláštního právního přepisu, doporučeně s dodejkou, nebo osobně proti potvrzení o převzetí nebo doručením prostřednictvím datové schránky. V případě, že smluvní strana odmítne doručovanou zásilku převzít, platí den odmítnutí převzetí za den doručení. V případě, že smluvní strana nevyzvedne zásilku v úložní době u držitele poštovní licence, má se za to, že zásilka byla doručena třetím dnem od uložení a to, i když se smluvní strana o uložení nedozvěděla.

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

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

6. 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.

7. Smluvní strany se v souladu s ustanovením § 558 odst. 2 OZ dohodly, že obchodní zvyklosti nemají přednost před smlouvou.

8. Zpracování případných osobních údajů fyzických osob v souvislosti s plněním předmětu této smlouvy, a to jak na straně kupujícího, tak i poskytovatele, bude prováděno v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), jakož i v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, přičemž jednotlivé smluvní strany se zavazují před případným zpracováním osobních údajů dotčených fyzických osob zajistit splnění právních podmínek dle uvedených právních předpisů pro takovéto zpracování.

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

10. 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.

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

12. 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.

13. Nedílnou součástí smlouvy jsou přílohy:

Příloha 1	Specifikace předmětu smlouvy (9 listů)
Příloha 2	Cenový rozklad (1 list)
Příloha 3	Výzva k poskytnutí plnění (1 list)
Příloha 4	Akceptační protokol (1 list)

V Brně dne

Za objednatele:

V Praze dne

Za poskytovatele:

[redacted]

Příloha 1 ke smlouvě Sp. zn. SpMO 16819/2022-1980 část – 1.
Počet listů: 9

Specifikace předmětu smlouvy

1. Kurz Bezpečnost a hacking android aplikací:

Obsah kurzu – minimální náplň školení v teoretické i praktické výuce
- pochopení architektury Android OS; - vysvětlení APK aplikací; - jaké je zabezpečení Android OS; - seznámení s nástroji pro penetrační testování Android OS; - seznámení s nejčastějšími zranitelnostmi Android a aplikací; - statická analýza kódu; - reverzování APK aplikací; - detailní vysvětlení Insecure Data Storage; - detailní vysvětlení Log Leakage; - detailní vysvětlení Broken Cryptography; - detailní vysvětlení Poor Authorization and authentication; - detailní vysvětlení Insufficient transport layer protection; - detailní vysvětlení APK repackage; - detailní vysvětlení Hidden APK; - detailní vysvětlení Client side injection; - detailní vysvětlení obfuskace kódu; - detailní vysvětlení Weak server side controls; - tvoření checklistů penetračního testování mobilních aplikací. **Délka trvání kurzu:** minimálně 5 dní/40 standardních hodin. **Požadavky na školitele:** Osobní dlouholetá (min. 5 let) zkušenost s úspěšným prováděním uvedených bodů náplně kurzu. Četná zkušenost s přednášením o této problematice před publikem či žáky. **Předpokládaný počet vyškolených osob:** 5 osoby. **Další požadavky na dodavatele:** - kvalitní školící zázemí určené výhradně pro účely školení v oblasti IT, s patřičným technickým vybavením; - poskytnutí žákům veškerých výukových materiálů a pomůcek nutných k absolvování kurzu.

2. Kurz pokročilé práce v nástroji IBM Security:

Obsah kurzu – minimální náplň školení v teoretické i praktické výuce
Vytváření typů log source: - úprava událostí z neobvyklých zdrojů; - využití DSM editoru. **Využití sbírek referenčních dat:** - ukládání a správa referenčních dat; - využití referenčních dat v rámci vyhledávání v QRadaru, filtrech, a odpovědích na pravidla. **Tvorba vlastních pravidel:** - vývoj a údržba pravidel pro detekci neobvyklé aktivity v síti; - možnosti vytváření pravidel z různých umístění. **Tvorba vlastních skriptů:** - vývoj a údržba skriptů k automatizaci reakce na pravidla. **Vývoj pravidel pro detekci anomálií:** - vývoj a údržba pravidel pro detekci anomálií. **Délka trvání kurzu:** minimálně 2 dny/16 standartních hodin. **Požadavky na školitele:** certifikát od firmy IBM, že může provádět školení tohoto produktu. **Předpokládaný počet vyškolených osob:** 4 osoby. **Další požadavky na dodavatele:** - dodavatel doloží certifikát školitele od firmy IBM, že může provádět školení tohoto produktu; - zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení; - poskytnutí výukových a studijních materiálu v elektronické podobě ke z důvodu kontroly ze strany objednatele; - zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem.

3. Kurz skriptování v PowerShell a PowerShell Core:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
Úvod do PowerShell a PowerShell Core: - verze PowerShell a PowerShell Core na různých operačních systémech; - požadavky PowerShell a PowerShell Core; - ovládání příkazové řádky; - ovládání vývojového prostředí PowerShell_ISE; - náhled na integraci ve Visual Studio. **Práce s PowerShell a PowerShell Core:** - spuštění zabudovaných EXE programů, cmdlet a volání .NET statických metod; - úvod do typů proměných, objektů a jejich vlastnosti (properties) a metod (methods); - běžné zabudované cmdlety pro správu operačního systému a cloudu jako jsou Get-, Set-, New-, Move- a další; - získání nápovědy, aliasy, komentáře; - koncept PSDrive, práce se soubory, registry a certifikáty; - spouštění scriptů z BAT, z naplánovaných úloh a psexec; - připojování na vzdálené počítače pomocí PSRemoting (Enter-PSSession); - (Ne)Typované proměnné a automatické konverze hodnot; - práce s typy číselnými, textovými, datem a časem, výčty (enum), GUID apod.; - práce s CMI a WMI, generování náhodných čísel, stahování a zpracování webových stránek a přístup na webové služby (web service); - práce se textovými soubory, CSV/TSV soubory, INI a XML soubory, vstup a výstup z/do souborů. **Syntaxe interpretru PowerShell a PowerShell Core:** - syntaxe interpretru příkazového řádku (command line parsing); - syntaxe interpretru ve vývojářském režimu (expression parsing); - základní elementy příkazové roury (pipe) a její možnosti; - základní element jazyka if, while, do, for, foreach, apod.; - základy vytváření složitějších funkcí a modulů; - zpracování chyb a vyjímek (try, catch, finally); **Délka trvání kurzu:** minimálně 5 dní/40 standartních hodin. **Předpokládaný počet vyškolených osob:** 4 osoby. **Další požadavky na dodavatele:** - zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení; - poskytnutí výukových a studijních materiálu v elektronické podobě ke z důvodu kontroly ze strany objednatele; - zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem.

4. Kurz ochrana sítí:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
IDS/IPS - intrusion detection system/intrusion preverntion systém: - princip pravidel sledování síťové komunikace; - správa a vytváření vlastních pravidel; - konfigurace systému pro sledování provozu; - konfigurace SPAN portu; - inline režim; - změny v TCP provozu. **HoneyPots**: - role honeypotu v síťové bezpečnosti; - lightweight vs. full honeypot; - praktická implementace honeypot systémů; - sledování systémů; - správná implementace sítě pro minimalizaci dopadu honeypot napadení. **EndPoint Security**: - správná implementace sítě pro minimalizaci dopadu honeypot napadení; - Windows Endpoint Security; - Linux Endpoint Security; - Mobile Endpoint Security; - OS Hardening; - Šifrování disků; - HIPS. **Effective Malware protection - Application Whitelisting a Macro whitelisting** - analýza prostředí z pohledu spouštěného kódu; - analýza prostředí z pohledu procesů; - sledování logů a doplňování nových pravidel; - Vynucení pravidel; - analýza office dokumentů v bezpečném prostředí; - správa CodeSigning certifikátů; - správa trusted publishersl. **Passwordless environment and Multifactor authentication** - ověřování pomocí klíčů v SSH; - ověřování pomocí SmartCard ve Windows Prostředí; - virtual Smart Card; - PKI management a Deployment certifikátů. **802.1x a WPA Enterprise a zabezpečení síťových segmentů** - analýza prostředí před nasazením opatření; - RADIUS, NAC - Network Access Controller;

- Radius server konfigurace;
- doporučení pro certifikáty Radius serveru;
- konfigurace supplicant řešení pro Microsoft i Linux;
- deployment certifikátů pro supplicanty;
- doporučení pro Windows/Linux deployment;
- implementace DHCP Snoopingu;
- implementace ARP Inspection;
- implementace IP Source Guard;
- MAC whitelisting;
- switchport port security maximum.

SIEM

- princip sledování událostí ve Windows;
- princip sledování událostí na Linuxu;
- princip sledování událostí u síťových prvků;
- sběr událostí;
- analýza událostí.

Délka trvání kurzu: minimálně 5 dní/40 standartních hodin.

Předpokládaný počet vyškolených osob: 4 osoby.

Další požadavky na dodavatele:

- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě ke z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem.

5. Kurz kryptografie a šifrování:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce	
Úvod do kryptografie a její vývoj:	
- principy kryptografie;	- historický vývoj;
- monoalfabetická substituční šifra;	- Cézarova šifra;
- Atbaš;	- ROT13;
- Vigenerova šifra, příklad a prolomení;	- ADFGVX šifra;
- Playfairova šifra;	- Enigma;
- CrypTool.	
Symetrická kryptografie a hashe:	
- symetrická kryptografie;	- teorie informace;
- Kerckhoffsuv princip;	- Subsituce;
- Transpozice;	- Substituce a Transpozice;
- Binární ano, or, xor;	- bloková šifra vs. streamová šifra;
- Feistelova šifra;	- DES, 3DES, DESx, AES;
- Blowfish;	- Serpent;
- Twofish;	- Skipjack;
- IDEA, ECB, CBC, RC4, MD5, MD6.	
Teorie čísel a asymetrická kryptografie:	
- asymetrická kryptografie;	- prvočísla;
- Fibonacciho posloupnost;	- Narozeninový paradox;
- generátory náhodných čísel;	- Diffile-Hellman;
- Rivest Shamir Adlemna (RSA);	- jak funguje RSA;
- příklad RSA;	- DSA;
- podepisování pomocí DSA;	- eliptické křivky;
- variace eliptických křivek;	- Elgamal.
Aplikace šifrování:	
- digitální podpis;	- co je to digitální certifikát;
- X.509;	- obsah certifikátu X.509;
- certifikační autorita;	- registrační autorita;
- PKI – infrastruktura veřejného klíce;	- digitální certifikáty;
- správa certifikátu;	- protokoly pro ověřování certifikátu serveru;
- důvěryhodnost certifikátu;	- používání certifikátu ve webových službách;
- MS Certifikační služby;	- Windows certifikáty a certmgr.msc;
- Pretty Good Privady (PGP);	- Certifikáty PGP;
- SSL, TLS;	- šifrování souboru pomocí EFS;
- zálohování EFS klíčů;	- obnova EFS klíčů;

- BitLocker, Truecrypt;
- Steganografie – vývoj, implementace a analýza.

Aplikace šifrování:

- lámání šifer;
- kryptoanalýza;
- frekvenční analýza;
- lámání moderních šifer;
- lineární kryptoanalýza;
- diferenční kryptoanalýza;
- integrální kryptoanalýza;
- Rainbow Tables;
- lámání hesel;
- nástroje.

Délka trvání kurzu: minimálně 3 dny/24 standartních hodin.

Požadavky na školitele: certifikát jako školitel EC-Council.

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na dodavatele:

- dodavatel doloží certifikát školitele od EC-Council;
- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě ke z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem.

6. Kurz praktické hekování:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
- principy ukládání hesel v operačních systémech; - přenos hesel při síťovém ověřování; - downgrade ověřovacích metod; - utoky na hesla hrubou silou pomocí CPU, grafických karet a distribuovaného útoku; - Rainbow Tables - principy vyhledávání, způsob generování pro konkrétní prostředí a druhy útoků, analýza time/memory tradeoff efektu; - druhy rámců používaných v bezdrátových sítích; - analýza bezdrátových sítí v dosahu; - yneužití neautorizovaných rámců; - WiFi Injection a monitor mód WiFi karet; - útoky na WEP sítě; - útoky na WPA1 PSK a WPA2 PSK sítě; - prolamování EAPOL rámců pomocí grafických karet; - vetřelecká AP; - WPS - zasílání falešných certifikátů, importování kořenových certifikačních autorit a vytváření legitimních falešných certifikátů obcházení HTTPS zabezpečení; - využití Metasploit Frameworku pro exploitaci síťových služeb; - skrývání prostředků pomocí rootkitů. **Délka trvání kurzu:** minimálně 5 dní/40 standartních hodin. **Předpokládaný počet vyškolených osob:** 4 osoby. **Další požadavky na dodavatele:** - zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení; - poskytnutí výukových a studijních materiálu v elektronické podobě ke z důvodu kontroly ze strany objednatele; - zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem.

7. Kurz praktického hekování - middle:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
Systémové útoky aneb deset nejčastějších hříchů IT pracovníků, kvůli kterým přicházíme o firmu: - zneužívání nejčastejších chyb v administraci ke kompletní kompromitaci sítě; - proč nevinné přesměrování lokálních zdrojů v RDP může vést k ovládnutí sítě; - RDP MitM a session recording aneb vzdálený záznam klávesnice a obrazovky admina; - chybné používání identit pro administraci, spuštění úloh a služeb; - Offline útoky pro ovládnutí domény; - hesla a vykrádání tajemství z počítačů; - zneužívání shadowcopy pro vykrádání databází, Active Directory a file serverů; - zneužívání lokálních účtů ve výchozím nastavení; - vykrádání paměti počítače; - vykrádání profilů a šifrovacích tajemství; - Pass The Hash aneb jak s údaji z paměti ovládnout vzdálené systémy a proč není třeba lámat hesla; - NTLM Relay aneb jak položit zcela vzdálené systémy, kam nikdo nechtěl přistupovat jen během útoků MitM; - Responder a podvrh legitimních cílů aneb jak snadno nalákat oběť a zneužít její výchozí nastavení; - Pass The Ticket aneb vykrádání Kerberosu; - Kerb roasting aneb kompromitace účtů služeb; - Golden Ticket prakticky - průstřel celého AD forestu pomocí jediné domény; - DMA útoky aneb jak obejít ochranu BitLocker. **Malware a vše na co jste se báli zeptat aneb jak ovládnout firmu na dálku a proč je většina firem prostřelená zevnitř:** - princip komunikace a proč útoky zevnitř vedou; - jak zneužít nejčastější cesty spuštění malwaru k infiltraci prostředí; - možnosti ovládání a sledování obětí; - skrývání malware - kam se skrýt, aby vás nikdo nehledal; - Wmi filtry; - využívání více úrovní streamů; - opomíjená nastavení office; - skrývání v registrech; - šifrování; - neobvyklé metody spouštění kódu; - využívání skrytých kanálů a tuneling v jiných protokolech; - Pivoting aneb jak prostoupit z napadeného počítače dál do nepřístupného prostředí; - automatizace prostupu prostředím; - infekce obsahu při MitM útocích;

- Fileless backdooring;
- asynchronní komunikace;
- skrývání malwaru pomocí Application Compatibility Toolkitu a tvorba shimů.

USB Hid útoky aneb jak zneužít cokoli v USB ke kompletní kompromitaci systému:

- falešné USB flash disky dynamicky měnící svůj obsah pro ovládnutí sítě;
- způsob vytváření objektů na HID sběrnici;
- ovládání počítačů pomocí HID injection;
- způsoby zcizení síťového provozu a SSL inspekce;
- přihlášení k systému bez fyzického přístupu;
- reverzní SSH tunel pro ovládnutí počítače;
- Kali Nethunter jako penetrační platforma;
- P4wnP1 a BashBunny jako prostředek pro penetrační testování.

MouseJacking a KeyJacking:

- zneužívání zranitelných klávesnic a myší pro ovládnutí vzdálených počítačů.

Úvod do Android Hackingu:

- generování malwaru pro mobilní prostředí;
- prostřelování slabin na zastaralých systémech;
- zneužívání oprávnění aplikací;
- možnosti sledování mobilních zařízení.

DoS attacks:

- Flooding cílů
- Reflection attacks
- Amplification effect

Délka trvání kurzu: minimálně 5 dní/40 standartních hodin.

Požadavky na školitele: certifikát jako školitel Hacking v praxi.

Předpokládaný počet vyškolených osob: 3 osoby.

Další požadavky na dodavatele:

- dodavatel doloží certifikát školitele od Hacking v praxi;
- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem.

8. Kurz Pokročilé praktické hekování:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
Pokročilé síťové útoky: - SPAN a RSPAN; - Vlan Hopping; - útoky na 802.1x; - Man in the Middle i bez APR; - statické zásahy do cache; - statické zásahy do routingu; - podvrhávání DHCP serveru; - DHCP Starvation attacks; - DNS spoofing a poisoning; - DNS typy záznamů a chyby v zabezpečení. **Falešná AP a WPA-Enterprise útoky** - probourávání identit pomocí falešných AP; - zneužívání falešných AP pro otrávení klientů; - zneužívání Hosted Networks jako backdoor do podnikového prostředí. **Průzkum síťového prostředí** - skenování živých cílů i bez nmapu; - skenování cílů, se kterými nejde komunikovat; - Enumerace aneb zjišťování detailů o napadeném prostředí; - SNMP aneb Security Not My Problem a jak může vést až k podrobení sítě. **Útoky na routery** - síťové útoky; - instalace backdoorů do firmware; - praktické otevření administrace pomocí CSRF útoků; - přetečení paměti. **Web útoky** - Session Hijacking; - Cross Site Request Forgery; - Cross Site Scripting; - Error Based SQL Injection vs. blind SQL injection; - Command injection; - Click jacking; - praktické vyzkoušení útoků k ovládání klientů, serverů i celkovému otevření sítě. **SDR - Software Defined Radio** - princip SDR útoků; - praktické testování SDR; - útoky na BLE.

IoT hacking

- statická analýza firmware;
- Credential bruteforcing;
- napadání síťové komunikace;
- Command injection.

Délka trvání kurzu: minimálně 5 dní/40 standartních hodin.

Požadavky na školitele: certifikát jako školitel Hacking v praxi.

Předpokládaný počet vyškolených osob: 3 osoby.

Další požadavky na dodavatele:

- dodavatel doloží certifikát školitele od Hacking v praxi;
- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

9. Kurz základy bezpečnosti a zabezpečení sítí:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
Základy bezpečnosti - cyklus informační bezpečnosti; - základy bezpečnostních politik; - ověřovací metody; - základy kryptografie. **Bezpečnostní hrozby a zranitelnosti** - sociální inženýrství; - hrozby fyzického přístupu; - hrozby v síťovém prostředí; - rizika a zranitelnosti bezdrátových sítí; - rizika chybně naprogramovaných aplikací. **Síťová bezpečnost** - přehled síťových zařízení z pohledu bezpečnosti; - koncept síťové bezpečnosti; - ukázky síťových útoků; - zabezpečení běžného síťového provozu; - zabezpečení infrastruktury bezdrátových sítí. **Zabezpečení aplikací, dat a prvků** - základní pravidla zabezpečení stanic; - základní pravidla zabezpečení serverů; - zabezpečení dat; - zabezpečení mobilních zařízení; - možnost zabezpečení aplikací. **Správa identit a přístupu** - typy autentizací; - Smart karty a tokeny; - strategie skupin; - správa přístupu pomocí ACL; - RADIUS server a 802.1x; - VLAN management; - správa přístupu do VPN; - WPA1/2 Enterprise. **Správa PKI a certifikátů** - koncept PKI; - možnost využití certifikátů - instalace Enterprise certifikační autority a správa šablon; - zálohování a obnova certifikační autority;

- automatické vs. ruční vydávání certifikátů;
- správa a zálohování privátních klíčů.

Monitoring bezpečnosti

- auditování v OS
- auditování sítě;
- IDS/IPS;
- Honeypots;
- antiviry.

Zajištění dostupnosti, zachování chodu firmy a incident response

- základní koncepty zajištění funkčnosti firmy;
- SLA;
- vysoká dostupnost;
- zálohování a obnova;
- co dělat, když dojde k napadení firmy.

Délka trvání kurzu: minimálně 5 dní/40 standartních hodin.

Požadavky na školitele: certifikát jako školitele CompTIA Security+.

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na dodavatele:

- dodavatel doloží certifikát školitele od CompTIA Security+;
- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

10. Kurz Úvod do programování v Python:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
Úvod - historie a základní vlastnosti Pythonu; - instalace; - konvence psaní kódu, základy syntaxe; - vývojové prostředí. **Základní datové typy a proměnné** - řetězce; - čísla; - Boolean; - operátory pro práci s řetězci; - aritmetické operátory; - operátory porovnání a logické operátory; - konverze; - proměnné; - anotace typů a hints; - formátování řetězců. **Řízení běhu programu** - příkaz if; - příkazy while a for; - Range, break a continue. **Funkce** - definice funkcí a procedur; - předávání parametrů; - standardní hodnoty parametrů; - rozsah platnosti proměnných; - rekurze. **Ladění programu (debugging) a zachytávání výjímek** - ladění programu; - princip zpracování chyb v Pythonu; - mechanismus výjimek; - příkazy try, except, raise, finally; - základy práce s kolekcemi; - list (seznam); - indexování a řezy; - měnitelné vs. neměnitelné typy; - Tuple (N-tice); - množina (set);

- slovník (dictionary);
- operace s řetězci.

Built-in Functions

- přehled základních vestavěných funkcí;
- funkce pro práci se stringem;
- matematické funkce;
- konverzní funkce.

Moduly a balíčky

- princip modulů pro vytváření knihoven funkcí;
- standardní moduly;
- Pip;
- virtuální prostředí (venv).

Základy OOP

- mechanismy OOP, základní vlastnosti OOP;
- třídy, instance, instanční proměnné a metody;
- Práce s objekty;
- statické metody;
- dědičnost, abstraktní třída, finální třída.

Práce se soubory

- základy práce se soubory;
- otevírání souborů, čtení, zápis.

Délka trvání kurzu: minimálně 5 dní/40 standartních hodin.

Požadavky na školitele: certifikát jako školitel Python I – úvod do programování.

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na dodavatele:

- dodavatel doloží certifikát školitele od Python I – úvod do programování;
- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

11. Kurz pokročilé techniky v Python:

Obsah kurzu - minimální náplň školení v teoretické i praktické výuce
Pokročilé OOP techniky - opakování OOP v jazyce Python; - magické metody; - dědičnost, polymorfismus; - Properties; - statické metody. **Pokročilé konstrukty jazyka** - generátory a iterátory; - generátorová notace; - dekorátory. **Základy funkcionálního programování v Pythonu** - Lambda výrazy; - anonymní funkce, first-class funkce, rekurze, closures, ... - Map, reduce, filter; - zkrácené logické výrazy. **Tvorba skriptů v Pythonu** - psaní skriptů. **Standardní knihovna, zajímavé moduly a balíčky** - přehled modulů a balíčků standardní knihovny; - repozitář PyPi; - nástroje pip, ensurepip. **CPython a jeho alternativy** - hlavní vlastnosti CPythonu - Virtuální prostředí s virtualenv, venv, … - PyPy, Jython, IronPython, … - Python ve WWW prohlížeči, Brython, ... - nástroje pro distribuci programu jako Pyinstaller, cx_Freeze, … **Datové formáty, perzistentní úložiště, databáze** - práce s formáty Python pickle, JSON; - Key-value databáze shelve. **Testování** - základní technologie testování; - modul pytest. **Aplikace s GUI** - návrh jednoduché aplikace s GUI; - widget knihovny jako GTk+, wxWidgets, QT a Python.

Délka trvání kurzu: minimálně 5 dní/40 standartních hodin.

Požadavky na školitele: certifikát jako školitele Python II.

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na dodavatele:

- dodavatel doloží certifikát školitele od Python II;
- zabezpečení výukových a studijních materiálu v online formě s možností stažení pro účastníky školení;
- poskytnutí výukových a studijních materiálu v elektronické podobě z důvodu kontroly ze strany objednatele;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

[redacted]

Příloha 2 k Sp. zn. SpMO 16819/2022-1980 - část 1.
Počet listů: 1

CENOVÝ ROZKLAD

Název veřejné zakázky:	**Soubor vzdělávacích kurzů v oblasti IT - část 1.**
Zadavatel:	Česká republika – Ministerstvo obrany zastoupená VÚ 1980 Brno, Tychonova 1, 160 00 Praha 6 – Hradčany, IČ: 60162694, DIČ: CZ60162694
Identifikační údaje účastníka:	
Obchodní firma/název:	**GOPAS, a.s.**
Údaje o zápisu:	Vedená Městským soudem v Praze, oddíl B, vložka 7753
Sídlo	Kodaňská 1441/46, 101 00, Praha 10
IČ:	63911035
Zastoupená:	[redacted]
Kontaktní osoba:	[redacted]
Kontaktní telefon:	
Kontaktní e-mail:	[redacted]
Bankovní spojení a číslo účtu:	Raiffeisenbank a.s., 1111028/5500
Adresa pro doručování:	Kodaňská 1441/46, 101 00, Praha 10

Nabídková cena

P.č.	Název školení	Předpo. počet osob	Cena za školení 1 osoby v Kč bez DPH	Cena za školení 1 osoby v Kč vč. DPH	Cena za školení požadovaných o počtu osob v Kč bez DPH	Cena za školení požadovaných o počtu osob v Kč vč. DPH
1.	Kurz Praktické hekování	4	[redacted]			
2.	Kurz Middle praktické hekování	3				
3.	Kurz Pokročilé praktické hekování	3				

4.	Kurz Základy bezpečnosti a zabezpečení sítí	2	[redacted]			
5.	Kurz Úvod do programování v Python	2				
6.	Kurz Pokročilé techniky v Python	2				
7.	Kurz Bezpečnost a hacking android aplikací	5				
8.	Kurz Pokročilé práce v nástroji IBM Security	4				
9.	Kurz Skriptování v PowerShell a PowerShell Core základy	4				
10.	Kurz Ochrana sítí	4				
11.	Kurz Kryptografie a šifrování	2				

Prohlášení o nabídkové ceně:

- nabídková cena je stanovena jako celková nabídková cena za uvedený rozsah předpokládaného plnění;
- nabídková cena obsahuje ocenění všech plnění poskytovatele nutných k řádnému splnění veřejné zakázky, tj. zahrnuje ocenění veškerých činností, dodávek a souvisejících výkonů nutných k naplnění účelu a cíle smlouvy - veřejné zakázky, tj. i ocenění činností, dodávek a souvisejících výkonů, které nejsou v nabídce výslovně uvedeny.

Čestné prohlášení o zpracování nabídky:

- účastník, osoba jemu blízká, ani žádný jeho zaměstnanec, ani poddodavatel účastníka, osoba jemu blízká, ani žádný jeho zaměstnanec se nepodílel na zpracování zadávací dokumentace shora uvedené veřejné zakázky;
- účastník nezpracoval nabídku v součinnosti s jiným poskytovatelem, který podal nabídku.

[redacted]

Příloha 3 k RD Sp. zn. SpMO 16819/2022-1980 - část 1.
Počet listů: 1

VÝZVA K POSKYTNUTÍ PLNĚNÍ č. XX/2022

ve smyslu čl. VI. a násl. Rámcové dohody č. **SpMO 16819/2022-1980 - část 1.**

Objednatel:

ČR - MINISTERSTVO OBRANY

se sídlem Tychonova 1, 160 01 Praha 6,
[redacted]
Identifikační číslo: 60162694
DIČ: CZ60162694
Bankovní spojení: Česká národní banka
Číslo bankovního účtu: 404881/0710

Poskytovatel:

GOPAS, a.s.
se sídlem Kodaňská 1441/46, 101 00, Praha 10
jejímž jménem jedná Ing. Petr Daniel, předseda správní rady
Identifikační číslo: 63911035
DIČ: CZ63911035
Bankovní spojení: Raiffeisenbank a.s.
Číslo bankovního účtu: 1111028/5500

V souladu s výše uvedenou rámcovou dohodou Vás tímto vyzýváme k provedení níže uvedeného plnění:

P.č.	Specifikace dílčího plnění - název kurzu	Počet účastníků	Cena za posluchače bez DPH	Cena kurzu bez DPH	Den zahájení dílčího plnění	Den ukončení dílčího plnění	Poznámka
1.							
Úhrnem cena kurzu bez DPH				**XX,XX- Kč**			
Úhrnem cena kurzu včetně 21% DPH				**XX,XX,- Kč**			

Brno dne:

[redacted]

Praha dne:

Ing. Petr Daniel, předseda správní rady

Podpis zástupce poskytovatele

[redacted]

Příloha 4 k RD Sp. zn. SpMO 16819/2022-1980 - část 1.
Počet listů: 1

AKCEPTAČNÍ PROTOKOL

ve smyslu ustanovení čl. VI. odst. 4 rámcové dohody č. 16819/2022-1980 - část 1.

Měsíc: …….

P.č.	Název provedeného školení	Skutečný počet účastníků	Převzetí kompletní dokumentace	Převzetí certifikátu	Poznámka
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

V ……..

_____
Podpis zástupce objednatele

V ……..

_____
Podpis zástupce poskytovatele