MOCRX046RR5Z

Velitelství informačních a kybernetických sil

Kounicova 156/65, Brno, PSČ 662 10, datová schránka hjyaavk

Počet listů: 41

Rámcová dohoda o provedení vzdělávacích kurzů v oblasti IT
Sp. zn. SpMO 357625/2024-1980/4

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

[redacted]

(dále jen „objednatel“)

Poskytovatel:	**GOPAS, a.s.**
zapsaná v obchodním rejstříku	u Městského soudu v Praze oddíl B, vložka 7753
Sídlo:	Kodaňská 1441/46, Praha 10, 101 00
IČ:	63911035
DIČ:	CZ63911035

[redacted]

(dále jen „poskytovatel“).

Smluvní strany se dohodly, že jejich závazkový vztah se řídí ve smyslu ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „OZ“) a uzavírají na veřejnou zakázku, zadanou v ET NEN pod č. N006/24/V00016033 tuto rámcovou dohodu (dále jen „smlouva“).

II.

Účel smlouvy

Účelem smlouvy je pořízením vzdělávacích kurzů k odbornému rozvoji znalostí příslušníků kybernetických sil a k zabezpečení plnění výstavby schopností středisek kybernetických sil.

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 **2 361 465 Kč** bez DPH (slovy: dvamiliony třistašedesátjednatisíc čtyřistašedesátpět korun českých), tj. **2 857 372,65 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 podle přílohy č. 2 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 na dobu **2 let od dne účinnosti této** smlouvy **dle čl. 10, odst. 12** smlouvy, a to ode dne podpisu rámcové dohody posledním z účastníků smlouvy.

[redacted]

4. Poskytovatel je povinen zabezpečit, aby kurzy, které na sebe v jednotlivých oblastech odborně navazují, byly realizovány 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 je objednatel 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 straznickym@army.cz úkonem s označením „Výzva k poskytnutí plnění“.

[redacted]

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 nebo anglickém 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 poskytovatel 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. Zástupce objednatele poskytne potřebnou součinnost poskytovateli pro plnění předmětu smlouvy.

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.

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 každé poskytnuté výzvě k poskytnutí plnění na základě daňového dokladu – faktury (dále jen „faktura“). Příslušná faktura bude objednateli doručena vždy nejpozději do 15. dne následujícího kalendářního měsíce. Faktura bude vyhotovena v českém.

3. Na faktuře bude uvedena tato adresa objednatele:

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

[redacted]

- 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

[redacted]

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 dodavatele 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 Ministerstvo obrany při zasílání úplaty vždy postupovat zvláštním způsobem zajištění daně podle § 109a tohoto zákona. Smluvní strany berou na vědomí a souhlasí, že takovém případě bude platba dodavateli za předmět smlouvy snížena o daň z přidané hodnoty, která bude odvedena Ministerstvem obrany na účet správce daně místně příslušného dodavateli. Dodavatel obdrží úhradu za předmět smlouvy ve výši částky odpovídající základu daně a nebude nárokovat úhradu ve výši daně z přidané hodnoty odvedené na účet jemu místně příslušnému správci daně.

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.

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.

4. Smluvní strany se dohodly, že smlouva nemusí být ze strany objednatele naplněna. Plnění smlouvy bude probíhat na základě skutečných potřeb objednatele.

X.

Závěrečná ujednání

1. Smlouva je vyhotovena ve dvou výtiscích o 5 listech se 3 přílohami o 16 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 objednatele, 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. Poskytovatel se zavazuje, že po celou dobu plnění bude dbát o dodržování důstojných pracovních podmínek svých zaměstnanců, resp. všech osob, které se na plnění předmětu smlouvy o dílo podílejí, dodržování pracovněprávních práv a povinností, mj. pravidel odměňování, pracovní doby a doby odpočinku, bezpečnosti a ochrany zdraví při práci (zejména před případným škodlivým působením chemikálií, elektrických zařízení nebo povětrnostních podmínek), zejména:

- plnění zakázky budou zajišťovat zaměstnanci s řádně uzavřenými pracovními smlouvami;
- ve vztahu k zaměstnancům bude důsledně dodržovat pracovněprávní práva a povinnosti vyplývající z obecně závazných právních předpisů a smluv, zejména vytvářet slušné a důstojné pracovní podmínky, dbát na bezpečnost a o ochranu zdraví zaměstnanců při práci, poskytovat vhodné a dostatečné pracovní pomůcky a ochranné prostředky, dodržovat pravidla pro stanovování pracovní doby a doby odpočinku mezi směnami, placené přesčasy, zajistit vedení zaměstnanců v příslušných registrech (např. v registru pojištěnců České správy sociálního zabezpečení), zajistit u zaměstnanců příslušná povolení k pobytu v České republice;

- zaměstnancům bude poskytovat pracovněprávní odměnu v souladu s právní úpravou odměňování v pracovněprávních vztazích včetně výplaty ve výplatním termínu a rovněž odpovídající odměnu (příplatek) za případnou práci přesčas, práci ve svátek atp.;
- bude oznamovat zadavateli, že vůči poskytovateli či jeho poddodavateli bylo orgánem veřejné moci (např. Státním úřadem inspekce práce či oblastními inspektoráty, Krajskou hygienickou stanicí) zahájeno řízení pro porušení právních předpisů, jichž se dotýká ujednání v tomto prohlášení, a k němuž došlo při plnění smlouvy nebo v souvislosti s ní, a to nejpozději do 10 dnů ode dne doručení oznámení o zahájení řízení;
- bude předávat objednateli kopii pravomocného rozhodnutí, jímž se řízení dle předchozího bodu končí, a to nejpozději do 10 dnů ode dne nabytí právní moci tohoto rozhodnutí.
- k výše uvedenému smluvně zaváže všechny případné poddodavatele.

14. Nedílnou součástí smlouvy jsou přílohy:

Příloha 1	Specifikace předmětu smlouvy (14 listů)
Příloha 2	Cenový rozklad (1 list)
Příloha 3	Výzva k poskytnutí plnění (1 list)

V Brně dne

Za objednatele:

brigádní generál Ing. Radek Haratek, M.S.
velitel

Ing. Radek Haratek , M.S.
Digitálně podepsal Ing. Radek Haratek , M.S.
Datum: 2024.08.28 07:15:09 +02'00'

Razítko a podpis

V Praze dne

Za poskytovatele:

Ing. Petr Daniel

GOPAS POCITACOVA.SKOLA.CZ
Digitálně podepsal Ing. Petr Daniel
Datum: 2024.08.23 09:36:19 +02'00'

Razítko a podpis

Velitelství informačních a kybernetických sil
Kounicova 156/65, Brno, PSČ 662 10, datová schránka hjyaavk

Příloha 1 k RD Sp. zn. SpMO 357625/2024-1980/4
Počet listů: 2

Specifikace předmětu smlouvy

1. Pokročilé metody forenzní analýzy

Minimální náplň školení v teoretické i praktické výuce

- 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
- 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

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).
Předpokládaný počet vyškolených osob: 1 osoba.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;

- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

2. Windows server a řešení problémů

Minimální náplň školení v teoretické i praktické výuce

- Windows Server 2022/2019/2016 – autentizace Kerberos a jeho nastavení
- Úvod do bezpečnostní a autentizační infrastruktury Windows a LSASS
- Ukládání hesel, heší, přihlašování čipovou kartou, cache a Single-Sign-On (SSO)
- Lokální vs. doménové účty, útoky na hesla a jejich šifrované komunikace přes síť
- Princip počítačových účtů, účty SYSTEM, Network Service, Local Service, NT SERVICE, IISAppPool
- Ověřovací protokoly Basic, Kerberos, LM, NTLM, NTLMv2, Schannel a EAP/TLS a PKINIT
- Optimalizace zabezpečení pro NTLM a Kerberos, implementace AES, omezení NTLM
- Kerberos SPN, použití a definice pro DNS aliasy a servisní účty, managed service accounts
- Synchronizace času
- Privilege Attribute Certificate (PAC), členství ve skupinách a jejich omezení, velikosti tiketů a access tokenu
- Kerberos unconstrained delegation, constrained delegation, protocol transition
- Podmínky pro delegaci, řešení potíží delegace
- Použití a nastavení Kerberos ověřování a delegace pro služby Remote Desktop Services a Terminal Services, SQL Server, SharePoint, System Center, Exchange a UAG
- Porovnání verzí operačních systémů a jejich podpory a schopností týkajících se ověřování
- Active Directory atributy uživatelských účtů týkající se ověřování
- Auditování a řešení potíží a bezpečnostních incidentů
- Příhlašování certifikáty na SSL/TLS služby - Schannel
- Přihlašování čipovou kartou (smart card) - PKINIT
- Zásady použití a vydávání čipových karet (smart card)
- Optimalizace ověřování v komplikovaných prostředí multiforest multidomain vztahů důvěry
- Závislost ověřování na parametrech síťových linek

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

3. Základní nástroje a principy útoků na počítačové sítě

Minimální náplň školení v teoretické i praktické výuce

- Penetrační testování
- Opakování TCP/IP
- Odchytávání dat v síťovém analyzéru
- Vyhledávání informací z Internetových zdrojů
- Spouštění procesů pod službami a plánovanými úlohami

Analýza prostředí a první útoky

- Analýza prostředí náchylných k sociálnímu inženýrství
- Skenování síťových služeb pomocí skenování otevřených portů a bannerů
- Analýza používaných operačních systémů
- Princip a aplikování ARP poisioningu pomocí nástrojů pro Microsoft Windows i Linux

Hesla a jejich prolamování

- Principy ukládání hesel v operačních systémech
- Přenos hesel při síťovém ověřování
- Downgrade ověřovacích metod
- Útoky 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

Bezdrátové sítě

- Druhy rámců používaných v bezdrátových sítích
- Analýza bezdrátových sítí v dosahu
- Zneužití 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

Pokročilejší útoky

- 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 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 8 osob.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

4. Certifikace Ethical Hacker

Minimální náplň školení v teoretické i praktické výuce

- Techniky, strategie a nástroje použité při hackingu
- Hacking webových serverů webových stránek aplikaci a dalších
- Skenování sítě
- Zjištění zranitelnosti a její enumerace
- Pochopení techniky social engineering a jak se bránit
- Techniky SQL injection
- Kryptografie
- Techniky a nástroje sloužící k auditu sítě
- Pochopení znalosti techniky DoS, DDoD včetně nástrojů na odhalení tohoto typu útoku

- Hackování bezdrátových sítí
- Hackování mobilních platforem na bázi systému OS Android
- Hackování IoT
- Využití prostředí v cloudu k útokům a ochraně proti nim
- Certifikační zkouška CEH v aktuální verze.

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 7 osob.

Další požadavky na poskytovatele:

- **zabezpečení vykonání certifikační zkoušky s doložení certifikátu o splnění;**
- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

5. Active directory – zabezpečení, útoky a penetrační testování

Minimální náplň školení v teoretické i praktické výuce

- Active directory – zabezpečení, útoky a penetrační testování.
- Krádež přihlašovacích údajů a laterální pohyb posíti, Pass-the-Hash, Pass-the-Ticket, Silver Ticket, Overpass-the-Hash, DCSync
- Hádáni hesel, (útoky hrubou silou a další techniky)
- MITM útoky, NBNS/LLMNR Spoofing, NTLM Relay, Kerberoasting
- Offline útoky na Active Directory, dešifrování DPAPI a DPAPI-NG
- Útoky na autentizaci pomocí čipových karet
- Dosažení persistence, Skeleton Key, Golden Ticket útok
- Detekce pomocí Microsoft ATA

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;

- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

6. Pokročilý hacking prakticky

Minimální náplň školení v teoretické i praktické výuce

Systémové útoky

- Zneužívání nejčastějších chyb v administraci ke kompletní kompromitaci sítě
- Proč nevinné přesměrování lokálních zdrojů v RDP může vést k ovládnutí sítě
- RDP MitM a session recording
- 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, Pass The Ticket
- NTLM Relay
- Responder a podvrh legitimních cílů
- Golden Ticket prakticky
- DMA útoky

Malware

- Princip komunikace
- Jak zneužít nejčastější cesty spuštění malwaru k infiltraci prostředí
- Možnosti ovládání a sledování obětí
- Skrývání malware
- Wmi filtry
- Využívání více úrovní streamů
- Opomíjená nastavení office
- Skrývání v registrech
- Neobvyklé metody spouštění kódu

- Využívání skrytých kanálů a tuneling v jiných protokolech
- Automatizace prostupu prostředím
- Infekce obsahu při MitM útocích
- Asynchronní komunikace
- Skrývání malwaru pomocí Application Compatibility Toolkitu a tvorba shimů

USB Hid útoky

- 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

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 3 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

7. OSINT (využití v praxi)

Minimální náplň školení v teoretické i praktické výuce

- Open Source Intelligence (OSINT)
- Potenciál a disciplíny OSINTu
- Mindset OSINT vyšetřovatele
- Právní znalosti pro legální OSINT vyšetřování
- Procesní bezpečnost vyšetřování (OPSEC)
- Sock puppets
- Vlastní virtuální zařízení pro vyšetřování
- Vlastní Android emulátor pro vyšetřování

- Search engine
- Google hacking
- Vyšetřování metadat, obrázků a fotografií, videí, emailů, uživatelských jmen, lidí, zdrojových kódů, webů, domén, telefonních čísel, dokumentů a IP adres.
- Social Media Intelligence (SOCMIT)
- Human Intelligence (HUMINT)
- Geospatial Intelligence (GEOINT)
- Český OSINT
- Základy a principy vyšetřování na darkwebu
- Praktické tipy pro vlastní bezpečnost
- Praktická část
- Případové studie (ukázky praktického vyšetřování)
- Ukázka základních metodologických nástrojů v procesu vyšetřování
- Vlastní vyšetřování a ověření získaných znalostí

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 3 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

8. Metody a praktické příklady útoků na uživatele webových aplikací

Minimální náplň školení v teoretické i praktické výuce

- Metody a praktické příklady útoků na uživatele webových aplikací.
- Zranitelnosti webových aplikací, techniky útoků a obrana proti těmto útokům.
- HTTP protokol
- Použití nástroje Burp Suite
- Web Parameter Tampering / Hidden Fields
- Enumerace uživatelů
- Útoky na autentizaci / Guessing

- Captcha – použití a chyby
- Citlivé údaje v URL
- Session Stealing, Prediction, Fixation, Donation, Expiration
- Insufficient logout
- Logout action availability
- Cross-Site Request Forgery (CSRF)
- CSRF a metody GET / POST
- Možnosti obrany před CSRF
- HTTP verb tampering
- Krademe kliknutí pomocí clickjackingu
- Vyplňujeme a odesíláme formuláře pomocí clickjackingu
- Možnosti obrany před clickjackingem
- Cross-Site Scripting (XSS)
- Perzistentní XSS
- Reflektovaný XSS
- DOM based XSS
- Blind XSS
- Self XSS
- Bypass kódu
- Protokoly javascript, vbsctipt, data
- XSS a nastavení Content-Type
- Cross-Site Flashing
- Použití nástroje BeEF
- Obrana před XSS
- Too long cookie value
- Přznak HttpOnly
- Cross-Site Tracing
- Reflected HTTP Request Header
- Open Redirect
- HTTP Response Splitting (CRLF injection)
- HTTPResponse Smuggling
- File Download via Open redirect
- Content Spoofing
- Cross-Site Messaging

- Únik dat refererm
- Únik dat při redirektu
- Útoky na CORS
- JavaScript Hijacking
- Problémy callbacků
- WWW-Authenticate attack
- Post & Back Attack
- Cross-site WebSocket hijacking
- Útoky na local storage
- Útoky na websockety
- Cache Poisoning
- HTTP Parameter Pollution
- Host Header Injection
- Path Relative StyleSheet Import (PRSSI)
- Zneužití uživatele pro napadení intranetu
- Reflected File Download
- CSV injection
- HTTP Response hlavičky pro bezpečný web

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 6 osob.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

9. Windows - práce s balíčkem SysInternals - základní

Minimální náplň školení v teoretické i praktické výuce

- Koncepty a nástroje Windows;
- Systémová architektura;
- K čemu je databáze registry a jak s ní pracovat;
- Co jsou procesy a různé mechanismy jako např. scheduling vláken, handles, access token;
- WMI;

- Drivers;
- IO subsystém, File Systém.

Délka trvání kurzu: minimálně 5 dní/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 1 osoba

Požadavky na školitele: certifikát jako školitel Windows.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

10. Metody a praktické příklady útoků na webové aplikace

Minimální náplň školení v teoretické i praktické výuce

- Metody a praktické příklady útoků na webové aplikace.
- Zranitelnosti webových aplikací, techniky útoků a obrana proti těmto útokům.
- Web Crawling / Spidering
- Hledání neveřejných zdrojů
- Repozitáře
- Open Directory listing
- Enumerace souborů , IIS Tilde File Enumerate
- HTTP metody
- Heartbleed, Poodle, BEAST, CRIME, BREACH
- Chybějící / Nedostatečná autorizace
- Přímý přístup k objektům
- Únik dat při redirektu
- Forced Browsing
- SQL injection (Union-Based, Boolean-Based, Error-Based, Time-Based, Stacked)
- DNS exfiltration
- Multibyte SQL injection
- SQL injection via binary hash
- Local File Disclosure via SQL injection

- Command execute via SQL injection
- SQL Truncation
- Hashovací algoritmy
- Solení
- Crackování hashů
- Brute Force / Dictionary attack / Rainbow tables
- Denial of Services via XML
- Local File Disclosure via XML
- Command Execution via XML
- XML injection
- LDAP injection
- XPATH injection
- Nezabezpečený upload
- Nezabezpečený download
- Local File Disclosure
- Remote File Inclusion (RFI)
- Local File Inclusion (LFI)
- LFI via file upload
- LFI via session storage
- LFI via environment
- LFI via log
- LFI via phpinfo
- Function Injection
- PHP Object Injection
- Code Execution
- Command Execution
- WebDav a zneužití HTTP metod
- PHP-CGI vulnerability
- SSI Injection
- Zneužití webserveru jako proxy
- HTTP request smuggling
- Privilege escalation / autorization bypass skrz cookie
- HTTP Request hlavičky
- Host Header Injection

- Napadení Session Storage
- Local Session Injection
- Session Puzzling
- ZIP bomby a DoS
- Útoky na sdílených serverech
- Server-Side Request Forgery (SSRF)
- Zranitelnost Shellshock

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 5 osob.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

11. Certifikece penetračního testování

Minimální náplň školení v teoretické i praktické výuce

Průzkum cíle

- OSINT
- Fyzický průzkum a vytipování slabých míst ve fyzickém zabezpečení
- Hardware útoky
- Headless device deployment a management

Skenování a enumerace

- Efektivní využívání nmapu ale i komponent v OS
- DNS extraction
- Průzkum prostředí pomocí pasivní analýzy okolního i vlastního provozu v síti
- Zjišťování topologie sítě a cílových segmentů

Malware deployment

- social engineering
- USB útoky
- Obfuscation

- Covert channel

Pentesting Active Directory

- Kerberos hacking
- Kerberoasting
- NTLM Relay
- Golden Ticket
- Secret data extraction
- Lateral movement

Pivoting

- Identifikace filtrování komunikace
- Základní pivoting
- Double pivoting
- Manuální postup

Exploitace

- Reverse engineering
- Fuzzing
- Buffer overflow
- Payload execution

Privilege escalation

- Analýza konfigurace systémů
- Identifikace aplikací a chyb v konfiguraci
- Zneužívání nalezených chyb

Web Pentesting

- Enumerace web serveru
- Mapování aplikace
- Exploitace vstupu pomocí injektáže - SQL Injection, Function injection, Object injection
- Local file inclusion
- Remote file inclusion
- Local session poisoning
- Session management
- Remote Code Execution

- Command Execution
- CSRF
- XSS

IoT Hacking

- Firmware extraction
- Key extraction
- Analýza komunikace

OT Hacking

- Prostup z IT do OT
- Analýza komunikace
- PLC, Mod Bus

Délka trvání kurzu: minimálně 5 dní/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 1 osoba.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

12. <u>IBM SOAR (Resilient) základní</u>

Minimální náplň školení v teoretické i praktické výuce

- Celkový popis, použití a funkce IBM SOAR
- Architektura, zapojení a základní konfigurace a integrace s IBM SIEM
- Uživatelské rozhraní (GUI)
- Administrace (uživatele, role …)
- Vytváření playbooku
- Použití API
- Vytvoření incidentů, jejich fází a úkolů
- Automatizace emailů jako vstupu
- Tvorba reportů a dashbordů
- Tvorba scriptů a pravidel
- Použití aplikací (App Exchange)

- Automatizace na Incident response
- Konfigurace autentizace do SOAR IBM (LDAP, SAML, MFA)

Délka trvání kurzu: minimálně 3 dny/24 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 5 osob.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

13. IBM SOAR (Resilient) pokročilý

Minimální náplň školení v teoretické i praktické výuce

- Kompletní Instalace IBM SOAR a jeho integrování s SIEM
- Použití s MITRE Framework a GDPR nástroje
- Design playbooků
- Administrace - Metrics systems
- OVA administrace

Délka trvání kurzu: minimálně 2 dny/16 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 5 osob.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

14. IBM QRadar SIEM Foundations

Minimální náplň školení v teoretické i praktické výuce

- Základy IBM SIEM (QRadar)
- QRadar Architektura, GUI, zdroje logů (log sources), zdroje flows, Network insights
- QRadar Tvorba vlastních pravidel (Custom Rule), Engine (CRE)
- QRadar aplikace (Use Case Manager)
- QRadar Assety

- QRadar pársování logů
- Práce s Offenses
- QRadar vyhledávání a filtrování, použtí Query jazyka (AQL)
- QRadar Vytváření reportů a dashboardů
- QRadar Administrace

Délka trvání kurzu: minimálně 3 dny/24 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 4 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

15. CISSP

Minimální náplň školení v teoretické i praktické výuce

- CISSP (Ceritified Information System Security Professional) - včetně zkoušky
- Systémy řízení rizik a bezpečnosti (security and risk management)
- Organizační a technické zabezpečení aktiv (asset security)
- Bezpečnostní technologie a zranitelnosti systémů (security engineering)
- Zabezpečení komunikací obecně a síťových komunikací (communication and network security)
- Správa identit a přihlašovacích účtů, bezpečné přihlašování a ověřování uživatelů a řízení přístupu (identity and access management)
- Hodnocení účinnosti bezpečnostních opatření a jejich testování (security assessment and testing)
- Provozní otázky v řízení bezpečnosti, řízení incidentů a kontinuity (security oprations)
- Bezpečnostní požadavky na vývoj software (software development security)

Délka trvání kurzu: minimálně 2 dny

Předpokládaný počet vyškolených osob: 1 osoba.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;

- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

16. Kurz ISO/IEC Foundation

Minimální náplň školení v teoretické i praktické výuce

- Náhledem do normy ISO 27001 (revize 2022) i souvislostmi s požadavky na ochranu osobních údajů, možnostmi integrace s normou ISO 9001.
- Vysvětlení praktických i formálních požadavků na řízení informační bezpečnosti.
- Návod na zavedení normy ISO 27001 do organizace.

Délka trvání kurzu: minimálně 1 den / 8 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

17. Řízení IT služeb (IT service management)

Minimální náplň školení v teoretické i praktické výuce

- Řízení životního cyklu IT služeb,
- Řízení hodnoty, kterou informační technologie poskytují.
- Obdržené Informace musí odpovídat ITIL 4 Foundation
- Příprava na zkoušku ITIL 4 Foundation.
- Certifikační zkouška ITIL 4 Foundation.

Délka trvání kurzu: minimálně 3 dnů/24 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 3 osoby.

Další požadavky na poskytovatele:

- **zabezpečení vykonání certifikační zkoušky s doložení certifikátu o splnění;**
- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;

- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

18. Windows Server 2022/2019/2016 – Správa bezpečnosti

Minimální náplň kurzu

- Správa Windows Server 2022/2019/2016 a jeho zabezpečení
- Uživatelské a servisní účty, logon session, access token, SID a SID history
- Ověřování uživatelů, autentizace pomocí NTLM, Kerberos, SSL certifikátů a čipových karet
- Auditování a sledování přístupu a ověřování
- Multiuživatelské prostředí, identity procesů, identity služeb a IIS AppPoolIdentity, SYSTEM, Network Service a Local Service
- Trust, forest trust, trust účty, selective trust a komplexní prostředí, migrace uživatelů
- NTFS a Share oprávnění, Access Based Enumeration (ABE)
- User Account Control (UAC)
- Lokální skupiny, delegace oprávnění pro správu serverů a stanic, delegace v Active Directory
- Group Policy a Security Policy, software restrictions, password policies
- Windows Firewall a jeho centrální správa přes Group Policy
- DAC - Dynamic Access Control
- Active Directory Certificate Services (AD CS), PKI a správa certifikátů a privátních klíčů
- Přístup do sítě a šifrování IPSec a 802.1x
- TLS/SSL certifikáty a jejich aplikace pro IIS, RDP apod.
- Šifrování BitLocker a EFS a jejich rozdíly, aplikace a zálohování klíčů

Délka trvání kurzu: minimálně 5 dnů/ 40 hodin

Předpokládaný počet vyškolených osob: 1 osoba.

Požadavky na školitele: certifikát jako školitel Windows.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;

- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

19. Pokročilá správa verzovacího systému

Minimální náplň školení v teoretické i praktické výuce

- Git jako DVCS
- Instalace Git
- Git repository – commit, undo, historie
- Git a větvení/merge
- Git tagy, remotes
- Stashing
- Rewriting history
- Interactive
- Searching

Délka trvání kurzu: minimálně 3 dny/24 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 1 osoba.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem,

20. Softwarový aplikační rámec - nastavení použití

Minimální náplň školení v teoretické i praktické výuce

Úvod do Springu

- Java Configuration & Spring context
- Anotace @Configuration, @Bean, @Import
- Bean scope (singleton, prototype, ...)

- Vytvoření Spring contextu, spuštění Spring aplikace a získání Spring Bean
- Spring profiles
- External properties

Dependency Injection pomocí anotací

- Component scanning
- Autowiring pomocí @Autowired
- @Component, @Service, @Controller anotace
- Java Configuration vs. anotace vs. XML konfigurace (legacy)
- Lifecycle annotations: @PostConstruct, @PreDestroy
- Spring Bean Lifecycle
- Spring Bean Proxies

Aspect Oriented Programming

- Jaké problémy řeší AOP?
- Implementace Spring AOP a z ní vyplývající omezení / implementační vlastnosti
- Anotace, které jsou postavené na AOP

Data Access & JDBC + Spring & JPA (Hibernate)

- JdbcTemplate
- JPA & Spring (Boot)
- Spring Data JPA (JpaRepository interface)
- Životní cyklus entity

Databázové transakce

- @Transactional
- Transaction management & Spring
- Šíření transakcí, commit, rollback

Spring Boot

- Tvorba webové Spring Boot aplikace
- Spring Boot starters
- Auto configuration
- Změna konfigurace pomocí properties, yaml, parametrů z příkazové řádky
- Packaging Spring Boot aplikace do Docker image
- Spring Boot Actuator & integrace na Prometheus

Testování Spring aplikace

- Spring a TDD (Test Driven Development)
- Spring 5 & integrační testy s JUnit 5

- @ActiveProfiles, @Sql
- Testování Spring Boot aplikací
- Testcontainers

Spring MVC a tvorba REST aplikací

- Úvod do REST architektury
- @RestController, @GetMapping, @PostMapping
- Exception handling pomocí @ExceptionHandler a @ControllerAdvice
- OpenAPI (Swagger)
- Třívrstvá architektura
- DTO (Data Transfer Object) & MapStruct
- Bean Validation

Spring Security

- Obecně k bezpečnosti webových aplikací
- Konfigurace Spring Security
- Konfigurace certifikátů u Spring Boot aplikací
- Autorizace na úrovni URL a metod

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

21. Architektura softwarových systémů

Minimální náplň školení v teoretické i praktické výuce

Úvod do problematiky vývoje softwaru

- Dopad použité metodiky tvorby SW (iterační, nebo agilní)
- Základní disciplíny vývoje SW a v nich vytvářené artefakty
- Co je to softwarová architektura

Konceptuální modelování

- Úvod do Clean Architecture

- Použití doménového modelu tříd v architektuře
- Použití Use Case Modelu v architektuře

Architekturní vzory

- Klasifikace, principy, jazyk vzorů, metavzory
- Vzory v návrhu a jejich aplikace v architektuře
- GRASP vzory
- Seznámení s některými GoF design patterns

Enterprise Application Architecture Patterns

- Kategorie a principy strukturálních vzorů
- Domain Logic Patterns (Transaction Script, Domain Model, Table Module, Service Layer)
- ORM - Object-Relational Mapping Patterns (Data Gateway, Row Data Gateway, Active Record, Data Mapper, Unit of Work, Identity Field, Foreign Key Mapping, Embeded Value, Class Table Inheritens)
- Sesion State Patterns (Client Session State, Server Session State)
- WEB Presentation Patterns (Model – View – Controler, Page Controller)
- Distribution Patterns (Remote Facade, Data Transfer Object)
- Graphical User Interface (GUI) Patterns

Délka trvání kurzu: minimálně 2 dny/16 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

22. Základy grafického editoru

Minimální náplň školení v teoretické i praktické výuce

- Základní pojmy – rastrová vs. vektorová grafika, rozlišení
- Popis prostředí programu Adobe Photoshop
- Různé obrazové formáty
- Využití klávesových zkratek pro urychlení workflow

- Nástroje pro výběry (geometrické výběry, laso, kouzelná hůlka, rychlý výběr)
- Uložení a editace okraje výběru. Automatické zpřesnění výběru u složitých částí (vlasy, zvíře, strom) a odstranění nežádoucího lemu kolem vybrané části.
- Lokální úpravy pomocí selekcí
- Využití vrstev v nedestruktivní editaci grafiky
- Vrstvy úprav
- Využití masek a maskování při úpravách fotografií v kolážích
- Generativní výplň
- Správa barev, barevné modely RGB a CMYK
- Použití a tvorba barevných přechodů
- Efekty vrstev např. s textem a jinými tvary
- Transformace obsahu (posun, otáčení, zkosení, perspektiva, deformace)
- Jasové a barevné úpravy fotografií
- Přesnější práce s histogramem pomocí Křivky
- Režimy prolnutí vrstev
- Způsoby převodů do černobílé fotografie
- Úpravy digitálních negativů RAW pomocí vestavěné aplikace
- Nadpisový a odstavcový text
- Seznámení s řadou běžných filtrů
- Retušovací nástroje (klonovací razítko, záplata, bodový retušovací štětec)
- Retušování v perspektivě
- Retušování portrétu (červené oči, bělení zubů, zkapalnění)
- Přebarvení části obrázku (změna barvy auta), kolorování černobílých fotografií
- Nástroje pro kreslení

Délka trvání kurzu: minimálně 2 dny / 16 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 6 osoby

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

23. Základní skriptování v jazyce PowerShell

Minimální náplň školení v teoretické i praktické výuce

- Verze PowerShellu a PowerShell Core na různých operačních systémech a jejich požadavky
- Ovládání příkazové řádky a vývojového prostředí PowerShell_ISE, náhled na integraci ve Visual Studio
- Spouštění zabudovaných EXE programů, cmdlet a volání .NET statických metod
- Syntaxe intepretru příkazového řádku (command line parsing)
- Syntaxe intepretru ve vývojářském režimu (expression parsing)
- Základní elementy příkazové roury (pipe) a její možnosti
- Úvod do typů proměnných, objektů a jejich vlastností (properties) a metod (methods)
- Běžné zabudované cmdlety pro správu operačního systému a cloudu jako jsou Get-, Set-, New-, Move- a další
- Získání nápovědy, alisy, komentáře
- Koncept PSDrive, práce se soubory, registry a certifikáty
- Spouštění skriptů 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
- Práce s CMI a WMI, generování náhodných čísel, stahování a zpracování webových stránek a přístup na webové služby (web service)
- Práce s textovými soubory, CSV/TSV soubory, INI a XML soubory, vstup a výstup z/do souborů
- Základní elementy jazyka if, while, do, for, foreach apod.
- Základy vytváření složitějších funkcí a modulů
- Zpracování chyb a výjimek (try, catch, finally)

Délka trvání kurzu: minimálně 5 dnů/ 40 hodin

Předpokládaný počet vyškolených osob: 2 osoby

Požadavky na školitele: certifikát jako školitel Powershell.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;

- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

24. <u>Pokročilé skriptování v jazyce PowerShell</u>

Minimální náplň školení v teoretické i praktické výuce

- Pokročilé skriptování v jazyce powerShell,
- Item, podmínky, cykly, operátory
- Pokročilá práce s pipeline
- Filtrování objektů a základní a pokročilé
- Parametry funkcí (ByValue, ByPropertyName)
- Práce s proměnnými, jejich použití a datové typy
- Pole, vícerozměrná pole, ArrayList
- Třídy - Vlastní třídy (Class)
- Funkce, parametry, Trap, Try – Catch – Finally
- Ošetření chyb - Error handling
- Pipe Filter
- Kódové moduly
- NuGet provider
- Pokročilá témata WMI, CIM, WMI – Eventing
- WMI Temporary Event Subscriptions
- WMI Permanent Event Subscriptions
- PSProvider, PSDrive pro Active directory, MS SQL a SharePoint
- Paralelní úlohy a jejich plánování
- Pokročilý Remoting
- Runspaces, JEA
- Soubory csv, XML, JSOM a vlastní formátování
- Pokročilá správa Active Directory
- Úvod do System.DirectoryServices.Protocols
- Síťové skripty a jejich konfigurace, Hyper-V & PowerCli, PKI, naplánované úlohy
- Nasazení DSC konfigurace
- Použití DSC on nanoServer
- DSC Core
- Pokročilé využití .NET framework a jeho statických tříd a metod

- System.Data.SqlClient.SqlConnection
- COM objekty pro automatizaci New-object –comobject
- Exchange EWS
- Pokročilá správa Sharepoint
- GUI a vytváření grafických aplikace a uživatelského rozhraní
- Optimalizace výkonu skriptů

Délka trvání kurzu: minimálně 5 dnů/40 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 3 osoby.

Požadavky na školitele: certifikát jako školitel Powershell.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

25. Virtualizace v Linuxu

Minimální náplň školení v teoretické i praktické výuce

- Úvod do virtualizačních technologií v prostředí Linux
- Systém OpenVZ
- Systém XEN
- Systém Qemu
- Systém KVM
- Knihovna libvirt
- Nástroje virsh, virt-install, virt-manager

Délka trvání kurzu: minimálně 3 dny/24 standardních hodin (60 min.).

Předpokládaný počet vyškolených osob: 2 osoby.

Další požadavky na poskytovatele:

- poskytovatel doloží kompetentnost a odbornou praxi školitele v délce trvání nejméně jeden rok, kterou získal praktické zkušenosti, např. profesní životopis, certifikát;
- poskytnutí výukových a studijních materiálu v elektronické podobě;
- zajištění prezenční listiny s obsahem všech náležitostí kurzu, která bude podepsána účastníky a školitelem;

Velitelství informačních a kybernetických sil
Kounicova 156/65, Brno, PSČ 662 10, datová schránka hjyaavk

Příloha 2 k RD Sp. zn. SpMO 357625/2024-1980/4
Počet listů: 1

CENOVÝ ROZKLAD

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 požadovaného počtu osob v Kč bez DPH	Cena za školení požadovaného počtu osob v Kč vč. DPH
1.	**Bezpečnost**					
2.	Pokročilé metody forenzní analýzy	1	53,200 Kč	64,372.00 Kč	53,200.00 Kč	64,372.00 Kč
3.	Windows server a řešení problémů	2	32,775 Kč	39,657.75 Kč	65,550.00 Kč	79,315.50 Kč
4.	Základní nástroje a principy útoků na počítačové sítě	8	31,050 Kč	37,570.50 Kč	248,400.00 Kč	300,564.00 Kč
5.	Certifikace Ethical Hacker	7	58,410 Kč	70,676.10 Kč	408,870.00 Kč	494,732.70 Kč
6.	Active directory – zabezpečení, útoky a penetrační testování	2	27,075 Kč	32,760.75 Kč	54,150.00 Kč	65,521.50 Kč
7.	Pokročilý hacking v praxi	3	31,500 Kč	38,115.00 Kč	94,500.00 Kč	114,345.00 Kč
8.	OSINT (využití v praxi)	3	29,450 Kč	35,634.50 Kč	88,350.00 Kč	106,903.50 Kč
9.	Metody a praktické příklady útoků na uživatele webových aplikací	6	27,900 Kč	33,759.00 Kč	167,400.00 Kč	202,554.00 Kč
10.	Windows - práce s balíčkem SysInternals - základní	1	28,500 Kč	34,485.00 Kč	28,500.00 Kč	34,485.00 Kč
11.	Metody a praktické příklady útoků na webové aplikace	5	27,900 Kč	33,759.00 Kč	139,500.00 Kč	168,795.00 Kč
12.	Certifikace penetračního testování	1	65,000 Kč	78,650.00 Kč	65,000.00 Kč	78,650.00 Kč
	IBM					
13.	Kurz IBM SOAR (Resilient) Fundamentals Training	5	38,500 Kč	46,585.00 Kč	192,500.00 Kč	232,925.00 Kč
14.	Kurz IBM SOAR (Resilient) Advanced Training	5	22,110 Kč	26,753.10 Kč	110,550.00 Kč	133,765.50 Kč
15.	Kurz IBM QRadar SIEM Foundations	4	40,200 Kč	48,642.00 Kč	160,800.00 Kč	194,568.00 Kč

	Management					
16.	CISSP	1	77,710 Kč	94,029.10 Kč	77,710.00 Kč	94,029.10 Kč
17.	Kurz ISO/IEC Foundation	2	6,900 Kč	8,349.00 Kč	13,800.00 Kč	16,698.00 Kč
18.	Řízení IT služeb (IT service management)	3	23,655 Kč	28,622.55 Kč	70,965.00 Kč	85,867.65 Kč
	Microsoft					
19.	Windows Server 2019/2016 – Správa bezpečnosti	1	27,075 Kč	32,760.75 Kč	27,075.00 Kč	32,760.75 Kč
	Programování					
20.	Pokročilá správa verzovacího systému	1	14,400 Kč	17,424.00 Kč	14,400.00 Kč	17,424.00 Kč
21.	Softwarový aplikační rámec - nastavení použití	2	34,200 Kč	41,382.00 Kč	68,400.00 Kč	82,764.00 Kč
22.	Architektura softwarových systémů	2	14,580 Kč	17,641.80 Kč	29,160.00 Kč	35,283.60 Kč
23.	Základy grafického editoru	6	5,510 Kč	6,667.10 Kč	33,060.00 Kč	40,002.60 Kč
24.	Základní skriptování v jazyce PowerShell	2	21,375 Kč	25,863.75 Kč	42,750.00 Kč	51,727.50 Kč
25.	Pokročilé skriptování v jazyce PowerShell	3	27,075 Kč	32,760.75 Kč	81,225.00 Kč	98,282.25 Kč
26.	Virtualizace v Linuxu	2	12,825 Kč	15,518.25 Kč	25,650.00 Kč	31,036.50 Kč

Velitelství informačních a kybernetických sil

Kounicova 156/65, Brno, PSČ 662 10, datová schránka hjyaavk

Příloha 3 k RD Sp. zn. SpMO 357625/2024-1980/4
Počet listů: 1

VÝZVA K POSKYTNUTÍ PLNĚNÍ č. XX/2024
ve smyslu čl. VI. a násl. Rámcové dohody Sp.zn. SpMO 357625/2024-1980/4

Objednatel:

ČR - MINISTERSTVO OBRANY

se sídlem Tychonova 1, 160 01 Praha 6,
jejímž jménem jedná velitel VÚ 1980 Brno
brigádní generál Ing. Radek Haratek, M.S
Identifikační číslo: 60162694
DIČ: CZ60162694
Bankovní spojení: Česká národní banka
Číslo bankovního účtu: 404881/0710

Poskytovatel:

XXXXXXXXX.
se sídlem XXXXXXXXXXXXX
jejímž jménem jedná XXXXXXXXX
Identifikační číslo: XXXXXXXXX
DIČ: XXXXXXXXXX
Bankovní spojení: XXXXXXXXXX
Číslo bankovního účtu: XXXXXXXX

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:

brigádní generál Ing. Radek Haratek, M.S

velitel

_____

Podpis zástupce objednatele

XXXXX dne: *XXXXXXXXXX,*

jednatel

_____

Podpis zástupce poskytovatele