Zmluva na školenia bezpečnostných administrátorov pri správe prevádzkovaných bezpečnostných produktov a aplikácií

uzatvorená podľa ustanovení § 261 ods. 2 a § 269 ods. 2 Obchodného zákonníka v znení neskorších predpisov

Číslo zmluvy objednávateľa: 2022/143

Zmluvné strany

1. **Poskytovateľ:**
   Obchodné meno:
   Sídlo:
   Zastúpený:
   IČO:
   IČ pre DPH:
   DIČ:
   Zapísaný:
   Právna forma:
   Označenie registra:
   Číslo zápisu:
   Bankové spojenie:
   IBAN:

   (ďalej len „poskytovateľ“)

2. **Objednávateľ :**

Názov:	**Slovenská republika zastúpená Ministerstvom financií Slovenskej republiky**
Sídlo:	Štefanovičova 5, P.O.BOX 82, 817 82 Bratislava 15, Slovenská republika
Zastúpený:	Veronika Gmiterko, MBA, generálna tajomníčka služobného úradu
IČO:	00151742
IČ pre DPH:	nie je platiteľom DPH
Bankové spojenie:	Štátna pokladnica, Radlinského 32,810 05 Bratislava 15
IBAN:	SK5981800000007000001400

(ďalej len „objednávateľ“ alebo „MF SR“)

Preambula

Podkladom pre uzatvorenie Zmluvy na školenia bezpečnostných administrátorov pri správe prevádzkovaných bezpečnostných produktov a aplikácií (ďalej len „Zmluva“) je úspešná ponuka poskytovateľa predložená v rámci Výzvy na predkladanie ponúk zverejnenej MF SR, ako verejným obstarávateľom, dňa DD.MM.RRRR v rámci verejného obstarávania k tejto zákazke, zadávanej podľa § 117 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej iba „zákon o verejnom obstarávaní“).

Článok 1
Účel Zmluvy

1.1. Účelom zmluvy je adekvátne, odborne a technicky vyškoliť vecne príslušných zamestnancov objednávateľa, ktorí budú vykonávať bezpečnostný dohľad pri správe bezpečnostných produktov a aplikácií prevádzkovaných objednávateľom.

Článok 2
Predmet Zmluvy

2.1. Predmetom Zmluvy je záväzok poskytovateľa riadne a včas poskytnúť objednávateľovi školenia bezpečnostných administrátorov - zamestnancov odboru informačnej a kybernetickej bezpečnosti MF SR (ďalej aj „zamestnanci objednávateľa“ alebo „účastníci školenia“), pri správe objednávateľom prevádzkovaných bezpečnostných produktov a aplikácií (ďalej len „bezpečnostné školenia“), a to v oblastiach:

2.1.1 vybudovanie Security Operation Centre (SOC) teamu,

2.1.2 riešenie bezpečnostných incidentov,

2.1.3 forenzná analýza,

2.1.4 zabezpečenie systémov Windows,

2.1.5 zabezpečenie systémov Linux,

2.1.6 penetračné testovanie webových aplikácií,

2.1.7 penetračné testovanie interného prostredia.

2.2. Podrobný obsah, rozsah a požiadavky na bezpečnostné školenia v oblastiach podľa bodu 2.1. tejto Zmluvy sú bližšie špecifikované v Prílohe č.1 tejto Zmluvy.

2.3. Za riadne a včas poskytnuté bezpečnostné školenia v rozsahu (oblastiach) podľa bodu 2.1 tohto článku sa objednávateľ zaväzuje zaplatiť cenu podľa článku 4 bod 4.1 a 4.2 tejto Zmluvy.

Článok 3
Lehota a spôsob poskytovania bezpečnostných školení

3.1. Bezpečnostné školenia sa poskytovateľ zaväzuje realizovať skupinovo pre tých účastníkov školenia, ktorých určí objednávateľ.

3.2. V lehote do 7 pracovných dní odo dňa nadobudnutia účinnosti Zmluvy je poskytovateľ povinný predložiť objednávateľovi na schválenie:

3.2.1. návrh časového harmonogramu bezpečnostných školení vypracovaný podľa Prílohy č.1 tejto Zmluvy. Návrh časového harmonogramu bude vypracovaný tak, aby bezpečnostné školenie mohlo začať najneskôr do 40 dní odo dňa schválenia časového harmonogramu objednávateľom a skončilo do uplynutia 9-tich mesiacov odo dňa, v ktorom bolo realizované prvé školenie.

3.3. Poskytovateľ je povinný zohľadniť pripomienky objednávateľa k návrhu časového harmonogramu bezpečnostných školení a bezodkladne ich do predmetných návrhov zapracovať.

3.4. Časový harmonogram bezpečnostných školení je pre poskytovateľa záväzný po jeho písomnom schválení zo strany objednávateľa. Zmeny schváleného časového harmonogramu bezpečnostných školení je možné robiť len na základe písomnej (e-mail) požiadavky objednávateľa alebo po vzájomnej dohode zmluvných strán.

3.5. Bezpečnostné školenia budú prebiehať prezenčne v priestoroch sídla objednávateľa, a to v pracovných dňoch podľa schváleného časového harmonogramu vypracovaného poskytovateľom. Jeden pracovný deň tvorí 8 hodín, spravidla v čase medzi 8:00 – 16:00, pokiaľ sa objednávateľ s poskytovateľom nedohodne inak. V čase, kedy prezenčné vzdelávanie neumožní epidemiologická (mimoriadna) situácia vyhlásená vládou SR, je možné školenie realizovať online po dohode s Objednávateľom. V takom prípade sa zmluvné strany zaväzujú, ak to bude nevyhnutné, bezodkladne schváliť nový časový harmonogram tak, aby celková lehota na realizáciu školení v trvaní 9 mesiacov ostala zachovaná.

3.6. V prípade, ak ktorákoľvek zmluvná strana zruší deň, kedy má prebiehať bezpečnostné školenie, je povinná písomne to oznámiť druhej zmluvnej strane v lehote nie kratšej ako 24 hodín pred začatím bezpečnostného školenia.

3.7. Účasť na bezpečnostnom školení bude vykazovaná formou prezenčných listín podpísaných účastníkmi bezpečnostného školenia, pripravených poskytovateľom.

3.8. Poskytovateľ bude objednávateľa informovať o účasti účastníkov bezpečnostných školení spôsobom písomne odsúhlaseným medzi poskytovateľom a objednávateľom.

Článok 4
Cena, platobné a preberacie podmienky

4.1. Cena za predmet Zmluvy podľa článku 2 tejto Zmluvy je stanovená dohodou zmluvných strán v súlade s platným zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov a v súlade s výsledkom verejného obstarávania k tejto zákazke, a to nasledovne:

Tabuľka č. 1

Typ školenia (a)	Cena za 1 deň bezpečnostného školenia v EUR bez DPH* (b)	Aktuálne platná sadzba DPH v % (c)	Cena za 1 deň bezpečnostného školenia v EUR s DPH* (d)	Počet dní (1 deň = 8 hodín) (e)	Cena za jednotlivé typy bezpečnostného školenia v EUR s DPH (f) = (d) x (e)	Cena za predmet Zmluvy v EUR s DPH* (g)
Vybudovanie SOC teamu		**20**		**5**		
Riešenie bezpečnostných incidentov		**20**		**5**		
Forenzná analýza		**20**		**8**		
Zabezpečenie systémov Windows		**20**		**5**		
Zabezpečenie systémov Linux		**20**		**4**		
Penetračné testovanie webových aplikácií		**20**		**5**		
Penetračné testovanie interného prostredia		**20**		**5**		

**Cena za 1 deň bezpečnostného školenia v EUR bez DPH, v EUR s DPH a Maximálna cena za predmet Zmluvy v EUR s DPH sú uvedené v súlade s ponukou poskytovateľa ako úspešného uchádzača v rámci Výzvy na predkladanie ponúk k predmetu tejto zákazky.*

4.2. Zmluvné strany berú na vedomie, že cena za 1 deň bezpečnostného školenia v EUR s DPH uvedená v Tabuľke č. 1 pre jednotlivé typy bezpečnostných školení je pevná a nie je ju možné zmeniť počas trvania tejto Zmluvy ani formou písomného dodatku k Zmluve. Celková cena za predmet Zmluvy v EUR s DPH, t. j. finančný limit Zmluvy, počas celej doby jej platnosti, je stanovený v súlade s Tabuľkou č. 1 vo výške ..... EUR s DPH, ktorý môže byť zmenený iba v súlade s platným zákonom o verejnom obstarávaní na základe písomného dodatku k Zmluve.

4.3. Do ceny predmetu tejto Zmluvy sú zahrnuté všetky náklady, ktoré poskytovateľovi vzniknú pri plnení predmetu tejto Zmluvy alebo v súvislosti s jej plnením.

4.4. Úhradu ceny za poskytnuté bezpečnostné školenie uskutoční objednávateľ na základe faktúry, vystavenej poskytovateľom za riadne poskytnuté plnenie v súlade s bodom 4.7.

4.5. Poskytovateľ do 10 pracovných dní po ukončení všetkých bezpečnostných školení (oblastiach) v rozsahu podľa článku 2 bod 2.1. a 2.2. tejto Zmluvy predloží na schválenie objednávateľovi v dvoch vyhotoveniach akceptačný protokol podpísaný kontaktnou osobou poskytovateľa. Akceptačný protokol bude obsahovať prehľad o poskytnutých bezpečnostných školeniach.

4.6. Prílohou akceptačného protokolu bude jeden originál prezenčných listín podpísaných príslušnými účastníkmi bezpečnostného školenia za každý absolvovaný deň bezpečnostného školenia. V lehote do 5 pracovných dní od doručenia akceptačného protokolu objednávateľovi, objednávateľ doručí poskytovateľovi podpísaný akceptačný protokol v jednom vyhotovení. Podpisom akceptačného protokolu objednávateľom, objednávateľ odsúhlasí vecnú správnosť údajov v ňom uvedených. V prípade nesúhlasu objednávateľa s vecnou správnosťou údajov uvedených v akceptačnom protokole, objednávateľ akceptačný protokol do 5 pracovných dní odo dňa jeho doručenia objednávateľovi vráti poskytovateľovi na prepracovanie. Prepracovaný/doplnený akceptačný protokol sa poskytovateľ zaväzuje objednávateľovi doručiť do 3 pracovných dní.

4.7. Deň podpisu akceptačného protokolu objednávateľom sa považuje za deň poskytnutia služieb a poskytovateľovi vzniká právo vystaviť faktúru. Faktúra musí obsahovať náležitosti podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov v platnom znení. Zároveň poskytovateľ uvedie na faktúre aj číslo a názov tejto Zmluvy, obdobie poskytovania bezpečnostných školení a fakturovaný počet dní bezpečnostných školení.

4.8. V prípade, ak poskytovateľ nebol v čase uzatvorenia tejto Zmluvy platcom DPH a stane sa ním počas trvania tejto Zmluvy, nemá nárok na zvýšenie ceny o DPH. Uvedená skutočnosť nebude mať vplyv na finančný limit Zmluvy podľa bodu 4.2 tohto článku.

4.9. Faktúra je splatná do 30 dní od dátumu jej doručenia do sídla objednávateľa. Faktúry sú objednávateľovi doručované výlučne:

1. elektronicky e-mailom vo formáte PDF na adresu elektronickej pošty: podatelna@mfsr.sk. Jeden e-mail môže obsahovať maximálne 1 PDF faktúru, maximálna veľkosť e-mailu je 10 MB. Faktúra vo formáte PDF musí byť pripojená ako príloha k e-mailu. Prílohy k faktúre (dodací list, súpis prác, akceptačný protokol atď.) sa nesmú odosielať ako samostatný súbor, ale musia byť súčasťou faktúry (t. j. prílohou musí byť len jediný PDF súbor, ktorý bude obsahovať všetky strany faktúry, vrátane všetkých jej príloh). Ďalšie prílohy (JPG, GIF, atď.) e-mailu budú zamietnuté z dôvodu dodržiavania pravidiel kybernetickej bezpečnosti,

alebo

2. hodnoverne elektronicky prostredníctvom elektronickej schránky ministerstva zriadenej na portáli Slovensko.sk. Adresa elektronickej schránky - UPVS ID: ico://sk/00151742. Jedna správa môže obsahovať maximálne jednu faktúru. Prílohy k faktúre (dodací list, súpis prác, akceptačný protokol atď.) sa nesmú odosielať ako samostatný súbor, musia byť súčasťou faktúry (t. j. prílohou musí byť len jediný PDF súbor, ktorý bude obsahovať všetky strany faktúry, vrátane všetkých jej príloh). Správa môže byť len vo formáte PDF, TXT, PNG, XML. Maximálna veľkosť všetkých objektov vložených do správy nemôže presiahnuť 33 MB.

4.10. Ak objednávateľ zistí na faktúre formálne alebo vecné chyby, alebo v prípade, ak vyhotovená faktúra nebude obsahovať všetky náležitosti daňového dokladu je objednávateľ oprávnený takto doručenú faktúru vrátiť poskytovateľovi v lehote splatnosti faktúry s uvedením zistených nedostatkov. V prípade vrátenia faktúry sa objednávateľ s jej úhradou nedostáva do omeškania a poskytovateľ je povinný takúto faktúru bezodkladne opraviť. Zmluvné strany sa dohodli na splatnosti opravenej faktúry v lehote 30 dní od doručenia opravenej faktúry do podateľne objednávateľa.

4.11. Faktúra sa považuje za uhradenú dňom pripísania sumy uvedenej na faktúre na účet poskytovateľa.

4.12. Zmluvné strany sa zaväzujú, že všetky finančné záväzky, vrátane zmluvných pokút, sankcií a náhrady škody si budú uhrádzať na bankové účty uvedené v záhlaví tejto Zmluvy alebo na bankové účty preukázateľne písomne oznámené druhej zmluvnej strane.

4.13. Poskytovateľ berie na vedomie, že ak si nesplnil svoju oznamovaciu povinnosť podľa § 6 zákona č. 222/2004 Z. z. o dani z pridanej hodnoty a neoznámil Finančnému riaditeľstvu SR svoj bankový účet uvedený v identifikačných údajoch poskytovateľa, objednávateľ nie je povinný poskytovateľovi uhradiť faktúru a to až do dňa splnenia oznamovacej povinnosti. Do doby splnenia oznamovacej povinnosti nie je objednávateľ v omeškaní s úhradou faktúry. Poskytovateľ je povinný oznámiť objednávateľovi akúkoľvek zmenu, doplnenie alebo zrušenie týkajúce sa bankového účtu uvedeného v identifikačných údajoch poskytovateľa.

Článok 5
Povinnosti poskytovateľa a objednávateľa

5.1. Poskytovateľ sa zaväzuje zabezpečiť účastníkom bezpečnostných školení potrebné študijné materiály riadne a včas, ktorých cena je zahrnutá v cene za predmet Zmluvy podľa bodu 4.1 a 4.2 tejto Zmluvy. Poskytnuté študijné materiály si objednávateľ bezodplatne ponechá.

5.2. Poskytovateľ sa zaväzuje zabezpečiť riadne a včasné plnenie predmetu Zmluvy podľa požiadaviek objednávateľa lektormi, prostredníctvom ktorých deklaroval splnenie požiadaviek stanovených objednávateľom v rámci podmienok účasti stanovených vo verejnom obstarávaní v rámci Výzvy na predkladanie ponúk k predmetu tejto zákazky. Požiadavky na požadované vzdelanie a odbornú prax lektorov sú uvedené v Prílohe č. 2 tejto Zmluvy.

5.3. V prípade, ak poskytovateľ prostredníctvom lektora alebo lektorov riadne neplní svoje zmluvné povinnosti, objednávateľ má právo ho písomne upozorniť, aby vykonal nápravu a zabezpečil riadne plnenie predmetných zmluvných povinností v čase uvedenom v písomnom upozornení. V prípade, ak poskytovateľ nevykoná nápravu v stanovenom čase, zaväzuje sa, na základe opätovného písomného upozornenia objednávateľa, poskytnúť bezodkladne, a to najneskôr v lehote do 3 pracovných dní objednávateľovi iného lektora alebo lektorov, ktorí spĺňajú požiadavky stanovené objednávateľom v rámci podmienok účasti stanovených vo verejnom obstarávaní v rámci Výzvy na predkladanie ponúk k predmetu tejto zákazky v Prílohe č. 2 tejto Zmluvy.

5.4. V prípade, ak nebude môcť poskytovateľ plniť predmet Zmluvy prostredníctvom schváleného lektora, poskytovateľ je povinný o tejto skutočnosti bez zbytočného odkladu, najneskôr do 3 pracovných dní odkedy nastane skutočnosť zakladajúca dôvod nemožnosti plnenia, písomne informovať objednávateľa a vyžiadať si jeho súhlas. Pri zmene/doplnení nového lektora, musí tento lektor spĺňať požiadavky určené verejným obstarávateľom na lektorov v podmienkach účasti stanovených vo verejnom obstarávaní v rámci Výzvy na predkladanie ponúk k predmetu tejto zákazky. Žiadosť o súhlas pri zmene/doplnení lektora predloží poskytovateľ v písomnej forme na adresu objednávateľa alebo e-mailom elektronicky spolu s dokladmi preukazujúcimi splnenie minimálnych požiadaviek na lektorov pred ich zaradením do bezpečnostného školenia na schválenie objednávateľom. Po kladnom písomnom stanovisku objednávateľa môže príslušný lektor začať vykonávať lektorskú činnosť v rámci plnenia tejto Zmluvy.

5.5. Objednávateľ je povinný, okrem iných povinností uvedených v tejto Zmluve, poskytnúť poskytovateľovi primeranú súčinnosť na realizovanie predmetu tejto Zmluvy, a to najmä:

a) odovzdať poskytovateľovi riadne a včas potrebné informácie, akými sú najmä zoznamy účastníkov bezpečnostných školení;
b) zabezpečiť pre lektorov poskytovateľa vstup do priestorov sídla objednávateľa v rozsahu nevyhnutnom na plnenie tejto Zmluvy;
c) schváliť bezodkladne zmenu/doplnenie lektorov podľa bodu 5.4 tohto článku Zmluvy.

Článok 6
Zmluvné sankcie a náhrada škody

6.1. V prípade, ak objednávateľ zruší bezpečnostné školenie v lehote kratšej ako 24 hodín pred jeho začatím (bod 3.7. Zmluvy), má poskytovateľ nárok na zaplatenie objednávateľom zrušeného dňa bezpečnostného školenia vo výške 50 % z celkovej sumy za príslušný školiaci deň.

6.2. V prípade porušenia povinnosti poskytovateľa podľa bodu 5.3, 10.2, 10.3, a 10.6 tejto Zmluvy, má objednávateľ nárok na zaplatenie zmluvnej pokuty vo výške 2 500,00 EUR za každé jednotlivé porušenie povinnosti poskytovateľa. Poskytovateľ berie na vedomie, že nárok na zaplatenie zmluvnej pokuty vzniká samotným porušením zmluvnej povinnosti poskytovateľa.

6.3. Objednávateľ má právo uplatniť si u poskytovateľa zmluvnú pokutu vo výške 1 000,- eur za každý deň existencie dôvodu vzniku práva na odstúpenie od Zmluvy v zmysle § 15 ods. 1 zákona č. 315/2016 Z. z. o registri partnerov verejného sektora v platnom znení.

6.4. V prípade neuhradenia faktúry v lehote splatnosti má poskytovateľ v súlade s § 369a Obchodného zákonníka nárok na úrok z omeškania v sadzbe podľa nariadenia vlády SR č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka.

6.5. Zmluvné pokuty dohodnuté v Zmluve nevylučujú vymáhanie náhrady škody, ktorá vznikla porušením povinností zmluvných strán v plnej výške, v súlade s ustanoveniami Obchodného zákonníka za splnenia podmienky, že spôsobená škoda prevyšuje sumu zmluvnej pokuty.

6.6. Poskytovateľ má nárok na náhradu škody spôsobenej omeškaním so splnením peňažného záväzku objednávateľa, len ak táto škoda nie je krytá úrokmi z omeškania alebo paušálnou náhradou nákladov spojených s uplatnením pohľadávky alebo ich súčtom.

6.7. Dohodnuté zmluvné pokuty a sankcie uhradí povinná strana strane oprávnenej do 30 dní odo dňa ich uplatnenia.

Článok 7
Dôverné informácie

7.1. Poskytovateľ berie na vedomie, že všetky informácie o objednávateľovi, o jeho zamestnancoch, interných postupoch objednávateľa, know-how a ďalších skutočnostiach týkajúcich sa objednávateľa a jeho činnosti, o ktorých sa dozvedel pri plnení predmetu tejto Zmluvy alebo v súvislosti s ním a ktoré nie sú verejne dostupné a známe (všetko spoločne ďalej len „dôverné informácie“), sú predmetom ochrany dôverných údajov podľa príslušných ustanovení Obchodného zákonníka a predmetom ochrany osobných údajov podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“).

7.2. Poskytovateľ sa týmto zaväzuje, že nesprístupní žiadne dôverné informácie akejkoľvek tretej osobe a ani ich nebude akýmkoľvek spôsobom bez právneho dôvodu alebo v rozpore s touto Zmluvou alebo pokynmi objednávateľa zhromažďovať, zbierať, uchovávať, rozširovať, sprístupňovať, spracovávať, využívať či združovať s inými informáciami. Poskytovateľ sa ďalej zaväzuje, že všetky dôverné informácie, s ktorými sa dostane do styku nad rámec tejto Zmluvy, bez zbytočného odkladu odovzdá objednávateľovi a v období, keď bude s dôvernými informáciami sám nakladať, zabezpečí ich dostatočnú ochranu pred ich akoukoľvek stratou, odcudzením, zničením, neoprávneným prístupom, náhodným či iným poškodením, či iným neoprávneným využívaním alebo spracovaním. Po skončení platnosti tejto Zmluvy je poskytovateľ povinný všetky dôverné informácie, ich kópie, resp. záznamy získané na nosičoch dát, či iných médiách bez odkladu vrátiť objednávateľovi alebo ich zničiť. Poskytovateľ si v žiadnom prípade nemôže tieto informácie ponechať alebo ich používať mimo rámec výkonu činností podľa tejto Zmluvy. Táto povinnosť i povinnosť mlčanlivosti trvá i po skončení platnosti tejto Zmluvy.

7.3. Poskytovateľ sa zaväzuje, že ak sa v súvislosti so spoluprácou s objednávateľom, a to v procese prípravy, realizácie a dodania predmetu tejto Zmluvy zamestnanci Poskytovateľa dostanú do styku s osobnými údajmi zamestnancov Objednávateľa, ktorý je prevádzkovateľom osobných údajov v zmysle Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb

pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „GDPR") a zákona č. 18/2018 Z. z. o ochrane osobných údajov, budú zachovávať mlčanlivosť o týchto osobných údajoch. Táto povinnosť mlčanlivosti pretrváva aj po skončení zmluvného vzťahu s objednávateľom. Za porušenie mlčanlivosti sa nepovažuje poskytnutie informácií o osobných údajoch na základe povinnosti uloženej v zmysle všeobecne záväzných právnych predpisov orgánmi, ktoré sú na vyžiadanie takýchto informácií oprávnené a slúžia nevyhnutne na plnenie úloh súdu a orgánov činných v trestnom konaní a ani vo vzťahu k Úradu na ochranu osobných údajov pri plnení jeho úloh. Pred poskytnutím takýchto informácií musí poskytovateľ informovať objednávateľa o vyžiadaní informácie a o rozsahu informácií, ktoré boli vyžiadané. Poskytovateľ zodpovedá za porušenie mlčanlivosti o osobných údajoch a to aj za dodržanie mlčanlivosti svojimi zamestnancami a inými osobami, ktoré použil v procese realizácie zmluvného vzťahu s objednávateľom, ako aj po skončení tohto zmluvného vzťahu.

7.4. Poskytovateľ sa zaväzuje, že v prípade porušenia ktorejkoľvek z povinností uvedených v tomto článku, je povinný nahradiť objednávateľovi škodu a/alebo ujmu, ktorá mu tým vznikne.

7.5. Dôvernými informáciami nie sú informácie, ktoré sa bez porušenia Zmluvy a zákonov platných na území Slovenskej republiky stali verejne známymi, informácie získané oprávnene inak ako od druhej zmluvnej strany a informácie, ktorých používanie upravujú osobitné predpisy, napr. informácie, ktoré je objednávateľ povinný sprístupniť alebo zverejniť podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o slobodnom prístupe k informáciám").

7.6. Poskytovateľ berie na vedomie, že spracúvanie osobných údajov objednávateľom, ktoré poskytovateľ uviedol v tejto Zmluve, je zákonné, vykonávané v súlade so zákonom o ochrane osobných údajov a GDPR, dobrými mravmi a na relevantnom právnom základe. Všeobecná informácia o ochrane osobných údajov je zverejnená na webovej stránke objednávateľa (http://www.finance.gov.sk/Default.aspx?CatID=11765).

Článok 8
Doručovanie a vzájomná komunikácia

8.1. S poukázaním na príslušné články tejto Zmluvy, ktoré upravujú otázky vzájomnej komunikácie medzi zmluvnými stranami, akékoľvek oznámenia, žiadosti, upomienky, výzvy, informácie alebo iné povinnosti, ktoré majú byť vykonané v súlade s touto Zmluvou, musia mať písomnú formu v listinnej podobe s prihliadnutím na znenie bodu 8.3 tohto článku. Takéto zásielky budú považované za riadne doručené druhej zmluvnej strane, ak budú prijaté zmluvnou stranou, ktorej boli adresované na kontaktné adresy objednávateľa a poskytovateľa podľa bodu 8.4 tejto Zmluvy. Odosielateľ akejkoľvek písomnej správy môže požadovať písomné potvrdenie príjemcu. Za deň doručenia zásielky zmluvnej strane, ktorej bola adresovaná sa považuje takisto deň,

a) v ktorom ju táto zmluvná strana odmietla prijať,

b) ktorým márne uplynula odberná lehota pre jej vyzdvihnutie si na pošte alebo

c) v ktorý bola na nej zamestnancom pošty vyznačená poznámka, že "adresát sa odsťahoval", "adresát je neznámy" alebo iná poznámka, ktorá podľa poštového poriadku znamená nedoručiteľnosť zásielky.

8.2. Každá komunikácia týkajúca sa platnosti alebo účinnosti Zmluvy, jej zániku či zmeny musí byť listinná a doručovaná výhradne poštovým podnikom ako doporučená zásielka, kuriérom alebo osobne.

8.3. Informácie uvedené v bode 8.1, týkajúce sa vzájomnej komunikácie, ktoré nezakladajú vznik, zmenu alebo zánik tejto Zmluvy, sa môžu považovať za doručené druhej zmluvnej strane aj po ich zaslaní elektronicky na e-mailové adresy uvedené v bode 8.4, resp. osobám v zmysle bodu 8.5, prípadne iným osobám dohodnutým obidvomi zmluvnými stranami. V prípade požiadavky odosielateľa na potvrdenie prijatia takýchto informácií, sa informácia považuje za doručenú až zaslaním potvrdenia o jej prijatí odosielateľovi zo strany príjemcu. Tieto informácie si strany zašlú formou šifrovania dát, ak o to ktorákoľvek strana požiada.

8.4. Kontaktné údaje pre komunikáciu sú:

(a) v prípade objednávateľa:
Meno: Mgr. Stanislav Schubert
Adresa: Ministerstvo financií SR, Štefanovičova 5, P.O.BOX 82, 817 82 Bratislava 15
Tel: +421 915 794 490
E-mail: stanislav.schubert@mfsr.sk

(b) v prípade poskytovateľa:
Meno:
Adresa:
Tel:
E-mail

8.5. Objednávateľ a poskytovateľ sa zaväzujú písomne si navzájom oznámiť kontaktné osoby a ich kontaktné údaje pre komunikáciu pre potreby realizácie Zmluvy, a to do 5 pracovných dní odo dňa účinnosti tejto Zmluvy.

8.6. Objednávateľ a poskytovateľ sa zaväzujú bezodkladne písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu svojich kontaktných údajov uvedených v Zmluve alebo vyplývajúcich zo Zmluvy, pre budúce doručovanie.

Článok 9
Doba trvania Zmluvy a ukončenie Zmluvy

9.1. Táto Zmluva sa uzatvára na dobu určitú do ukončenia realizácie bezpečnostných školení podľa bodu 3.2.1 tejto Zmluvy.

9.2. Táto Zmluva nadobúda platnosť dňom jej podpísania zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv (ďalej len „register“). Zmluva je povinne zverejňovanou Zmluvou v zmysle § 5a zákona o slobodnom prístupe k informáciám v platnom znení. Zmluvné strany berú na vedomie a súhlasia, že Zmluva vrátane všetkých jej príloh, resp. aj jej prípadných dodatkov, budú zverejnené v registri bezodkladne po jej, resp. ich podpísaní oboma zmluvnými stranami. Register je verejný zoznam povinne zverejňovaných zmlúv, ktorý vedie Úrad vlády Slovenskej republiky v elektronickej podobe.

9.3. Zmluvné strany sa dohodli, že túto Zmluvu je možné ukončiť:

9.3.1. odstúpením v prípade podstatného porušenia tejto Zmluvy. Odstúpením od tejto Zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce zo Zmluvy. Odstúpenie od Zmluvy sa nedotýka nároku oprávnenej zmluvnej strany na náhradu škody vzniknutej porušením tejto Zmluvy povinnou zmluvnou stranou a na zaplatenie zmluvnej pokuty. Odstúpenie od Zmluvy je účinné dňom doručenia oznámenia o odstúpení od Zmluvy druhej zmluvnej strane alebo iným dňom nasledujúcim po jej doručení, ktorý je uvedený v oznámení o odstúpení;

9.3.2. výpoveďou zo strany objednávateľa. Zmluvu je možné vypovedať zo strany objednávateľa kedykoľvek (i) bez uvedenia dôvodu v trojmesačnej výpovednej lehote, alebo (ii) s uvedením výpovedného dôvodu v jednomesačnej výpovednej lehote. Výpovedným dôvodom je porušenie povinností poskytovateľa vyplývajúcich z článku 3, 4 a 5 tejto Zmluvy. Zmluvné strany sa dohodli, že výpovedná lehota začína plynúť od prvého dňa kalendárneho mesiaca nasledujúceho po kalendárnom mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane;

9.3.3. výpoveďou zo strany poskytovateľa. Poskytovateľ je oprávnený vypovedať túto Zmluvu v prípade preukázateľného porušenia povinností objednávateľa vyplývajúcich z článku 4 a 5 tejto Zmluvy v trojmesačnej výpovednej lehote. Zmluvné strany sa dohodli, že výpovedná lehota začína plynúť od prvého dňa kalendárneho mesiaca, nasledujúceho po kalendárnom mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane;

9.3.4. písomnou dohodou zmluvných strán.

9.4. Zmluvné strany sa dohodli, že za podstatné porušenie Zmluvy budú považovať najmä opakované porušenie zmluvných povinností poskytovateľa, upravených v článku 3, 4 a 5 Zmluvy, porušenie zmluvných povinností poskytovateľa podľa čl. 10 Zmluvy, opakované neodôvodnené rušenie jednotlivých bezpečnostných školení, nedostatočný počet lektorov, nedodržiavanie školení podľa Prílohy č.1 tejto Zmluvy a preukázateľné neposkytovanie súčinnosti zmluvných strán pri plnení Zmluvy.

9.5. Podmienky tejto Zmluvy, ktoré svojou povahou presahujú dobu jej platnosti, zostávajú v platnosti v celom rozsahu a sú účinné až do okamihu ich splnenia a platia aj pre prípadných nástupcov a postupníkov zmluvných strán.

Článok 10
Osobitné ustanovenia

10.1. Poskytovateľ má právo za podmienok dohodnutých v tejto Zmluve uzatvárať subdodávateľské Zmluvy. Tým nie je dotknutá zodpovednosť poskytovateľa za plnenie Zmluvy v súlade s § 41 ods. 8 zákona o verejnom obstarávaní a poskytovateľ je povinný odovzdávať objednávateľovi plnenia sám, na svoju zodpovednosť, v dohodnutom čase a v dohodnutej kvalite. Zoznam subdodávateľov známych pri podpise Zmluvy spolu s ich identifikačnými údajmi v rozsahu: (i) meno a priezvisko alebo obchodné meno, resp. názov, (ii) adresa pobytu alebo sídlo, (iii) IČO alebo dátum narodenia, ak nebolo pridelené IČO, ako aj údajmi o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia, tvorí neoddeliteľnú súčasť tejto Zmluvy ako Príloha č. 3.

10.2. Poskytovateľ je oprávnený zmeniť a/alebo doplniť subdodávateľa počas trvania Zmluvy. Poskytovateľ je povinný bezodkladne, ako sa dozvedel o potrebe vykonať zmenu, predložiť objednávateľovi písomné oznámenie o zmene a/alebo doplnení subdodávateľa, vrátane aktualizovaného zoznamu subdodávateľov poskytovateľa, ktorý bude obsahovať údaje o subdodávateľoch v rozsahu podľa bodu 10.1 tohto článku, resp. Prílohy č. 3 Zmluvy. Zmenený/doplnený subdodávateľ musí spĺňať podmienky účasti týkajúce sa osobného postavenia podľa § 32 ods. 1 písm. e) a f) zákona o verejnom obstarávaní a nesmie u neho existovať dôvod na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7 zákona o verejnom obstarávaní.

10.3. Poskytovateľ vyhlasuje, že je ku dňu podpísania tejto zmluvy zapísaný v registri partnerov verejného sektora v zmysle zákona č. 315/2016 Z. z. o registri partnerov verejného sektora (ďalej len „zákon o RPVS“) a tiež každý jemu známy subdodávateľ v ktoromkoľvek rade, ktorý je partnerom verejného sektora je zapísaný v registri partnerov verejného sektora. Ďalej poskytovateľ vyhlasuje, že ku dňu podpísania tejto Zmluvy má ako partner verejného sektora alebo má osoba, ktorá plní povinnosti oprávnenej osoby pre poskytovateľa v zmysle zákona o RPVS (ďalej len „oprávnená osoba“), splnené všetky povinnosti, ktoré pre poskytovateľa ako partnera verejného sektora alebo pre oprávnenú osobu vyplývajú zo zákona o RPVS. Zmluvné strany sa dohodli, že ak sa vyhlásenia podľa tohto bodu ukážu ako nepravdivé, objednávateľ nie je v omeškaní s plnením podľa tejto zmluvy až do splnenia povinnosti poskytovateľa, resp. oprávnenej osoby. V prípade nesplnenia povinnosti podľa prvej a druhej vety tohto bodu alebo ak bol poskytovateľ vymazaný z registra partnerov verejného sektora, berie poskytovateľ na vedomie, že objednávateľ má právo v zmysle § 19 ods. 3 zákona o RPVS od tejto Zmluvy odstúpiť.

10.4. Poskytovateľ zodpovedá za správnosť a úplnosť údajov zapísaných v registri partnerov verejného sektora, identifikáciu konečného užívateľa výhod a overovanie identifikácie konečného užívateľa výhod v zmysle § 11 zákona o registri partnerov verejného sektora. Kým poskytovateľ nevykoná overenie identifikácie konečného užívateľa výhod, objednávateľ nie je povinný plniť zo Zmluvy a nedostane sa pritom do omeškania. Objednávateľ má právo odstúpiť od tejto Zmluvy z dôvodov, uvedených v § 15 ods. 1 zákona o registri partnerov verejného sektora. Objednávateľ nie je v omeškaní a nie je povinný plniť čo mu ukladá Zmluva, ak nastanú dôvody podľa § 15 ods. 2 zákona o RPVS.

10.5. Poskytovateľ je povinný zákazníkovi oznámiť zmenu v osobe, resp. osobách, ktoré sú v registri partnerov verejného sektora zapísané ako konečí užívatelia výhod alebo výmaz poskytovateľa z registra partnerov verejného sektora najneskôr do 5 dní odo dňa vykonania zmeny alebo výmazu v registri partnerov verejného sektora.

10.6. Prípadné vyčiarknutie subdodávateľa z registra partnerov verejného sektora počas trvania tejto Zmluvy je Poskytovateľ povinný bezodkladne oznámiť Objednávateľovi. Poskytovateľ má oznamovaciu povinnosť voči Objednávateľovi bezodkladne od momentu, kedy sa túto skutočnosť preukázateľne dozvedel.

10.7. Po dobu omeškania poskytovateľa ako partnera verejného sektora alebo oprávnenej osoby s plnením niektorej povinnosti podľa zákona o RPVS, objednávateľ nie je v omeškaní s plnením podľa tejto Zmluvy až do splnenia povinnosti poskytovateľa, resp. oprávnenej osoby.

10.8. Poskytovateľ je povinný dodržiavať zákazy, obmedzenia a povinnosti vyplývajúce zo zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o nelegálnej práci"), najmä je však povinný postupovať tak, aby plnenie podľa tejto Zmluvy neposkytoval prostredníctvom fyzickej osoby, ktorá je nelegálne zamestnaná.

10.9. Za porušenie zákona o nelegálnej práci poskytovateľ zodpovedá v plnom rozsahu a znáša prípadné škody, ktoré v dôsledku porušenia zákona o nelegálnej práci pri plnení tejto Zmluvy objednávateľovi vzniknú.

10.10. Objednávateľ v súlade s § 6 ods. 7 zákona č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, za účelom zaistenia bezpečnosti a ochrany zdravia pri práci, oboznámi všetkých lektorov plniacich predmet tejto Zmluvy pred začatím vykonávania lektorskej činnosť o miestnych prevádzkových pomeroch objednávateľa a z oboznámenia vypracuje záznam o oboznámení. Poskytovateľ je povinný zabezpečiť účasť lektorov na oboznámení podľa predchádzajúcej vety a zabezpečiť pre objednávateľa podpísanie záznamu o oboznámení všetkými lektormi plniacimi predmet tejto Zmluvy.

10.11. Formálna zmena spočívajúca v údajoch týkajúcich sa zmluvných strán (obchodné meno/názov, sídlo, štatutárny orgán, zmena v kontaktných údajoch, alebo iná zmena, ktorá má vo vzťahu k tejto zmluve iba deklaratórny účinok) alebo zmena v subjekte Poskytovateľa, ku ktorej dôjde na základe všeobecne záväzného právneho predpisu, nie je zmenou, ktorá pre svoju platnosť vyžaduje zmenu tejto zmluvy. To znamená, že takúto zmenu oznámi jedna zmluvná strana druhej zmluvnej strane bezodkladne spôsobom dohodnutým v článku 8 zmluvy a premietne sa do tejto zmluvy pri najbližšom písomnom dodatku. Súčasťou oznámenia sú doklady, z ktorých zmena vyplýva, najmä výpis z obchodného registra alebo iného registra, odkaz na príslušný právny predpis a podobne. Oznámenie musí byť podpísané štatutárnym zástupcom Poskytovateľa.

10.12. Žiadna zo zmluvných strán nebude zodpovedná za nedodržanie záväzkov, pokiaľ toto nedodržanie vznikne v dôsledku vonkajších udalostí, ktoré nemohli byť ovplyvnené zmluvnými stranami alebo nimi predvídané. Pre účely tejto zmluvy sa za vyššiu moc považujú skutočnosti od zmluvných strán nezávislé a zmluvnými stranami objektívne neovplyvniteľné, napr.: vojna, mobilizácia, povstanie, generálny štrajk, živelné pohromy, zlá epidemiologická situácia alebo núdzový stav vyhlásený vládou SR a pod. Lehoty uvedené v tejto zmluve alebo zákone sa na čas trvania skutočnosti označenej ako vyššia moc dočasne pozastavujú, s presným označením ich začiatku a charakteru. Po skončení trvania skutočnosti označenej ako vyššia moc plynú pozastavené lehoty plynule ďalej s tým, že nadväzujú na časť lehôt už uplynulých pred ich pozastavením v dôsledku vyššej moci.

Článok 11
Protikorupčná doložka

11.1. Pri plnení tejto Zmluvy sa poskytovateľ zaväzuje zaviesť a vykonávať všetky nevyhnutné a vhodné postupy a opatrenia vedúce k zabráneniu protispoločenskej činnosti, vrátane korupcie.

11.2. Poskytovateľ vyhlasuje, že podľa jeho vedomostí žiaden z jeho predstaviteľov, zástupcov, zamestnancov alebo iných osôb konajúcich v jeho mene pri poskytovaní plnenia predmetu Zmluvy neponúka a ani nebude priamo alebo nepriamo ponúkať, dávať, vyžadovať ani prijímať finančné prostriedky alebo akékoľvek oceniteľné hodnoty alebo poskytovať akékoľvek výhody, dary, alebo pohostenia zamestnancovi objednávateľa, za účelom ovplyvňovania konania takejto osoby v jej funkcii

s využitím odmeňovania alebo navádzania k nekorektnému výkonu príslušnej funkcie alebo činnosti akoukoľvek osobou, za účelom získania alebo udržania výhody pri podnikateľskej činnosti.

11.3. Poskytovateľ sa zaväzuje okamžite oznámiť primeranou formou zástupcovi objednávateľa akékoľvek podozrenie na porušenie akéhokoľvek ustanovenia tohto článku Zmluvy a byť plne súčinný pri dôkladnom vyšetrení podozrenia.

11.4. V prípade porušenia ktoréhokoľvek z vyššie uvedených ustanovení tohto článku Zmluvy poskytovateľom je objednávateľ oprávnený, aj bez predchádzajúceho upozornenia, odstúpiť od Zmluvy a to s okamžitou platnosťou bez toho, aby poskytovateľovi vznikol akýkoľvek nárok zo zodpovednosti za odstúpenie objednávateľa od Zmluvy.

11.5. Poskytovateľ sa zaväzuje, že ak bude preukázané protispoločenské konanie a/alebo porušenie protikorupčného správania, odškodní poskytovateľ v maximálne možnom rozsahu podľa platných právnych predpisov za akúkoľvek stratu, ujmu, poškodenie alebo nahradí náklady vzniknuté v priamej príčinnej súvislosti s porušením tohto článku Zmluvy.

Článok 12
Záverečné ustanovenia

12.1. Zmluvné vzťahy neupravené touto Zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka v platnom znení. Zmluva je uzavretá a vykladá sa v súlade s právnym poriadkom Slovenskej republiky.

12.2. Zmluvné strany sa zaväzujú, že vyvinú maximálnu snahu o riešenie všetkých sporov vyplývajúcich alebo súvisiacich so Zmluvou zmierlivou cestou. Pokiaľ zmierlivé riešenie sporu nebude možné, spor rozhodnú príslušné súdy Slovenskej republiky.

12.3. Ak sa niektoré z ustanovení Zmluvy stane nevynútiteľným alebo neplatným podľa platných právnych predpisov, bude toto ustanovenie neúčinné len do tej miery, do akej je nevynútiteľné, či neplatné. Pokiaľ nastane takáto situácia, zmluvné strany nahradia toto nevynútiteľné či neplatné ustanovenie iným ustanovením, ktoré sa mu svojim obsahom bude čo najviac približovať. Ďalšie ustanovenia Zmluvy zostávajú naďalej záväzné a v plnej platnosti a účinnosti.

12.4. Zmluvné strany nie sú oprávnené na prevod svojich práv a záväzkov, ktoré zo Zmluvy vyplývajú, na tretiu osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.

12.5. Žiadna zo zmluvných strán nie je oprávnená postúpiť Zmluvu ako celok alebo akúkoľvek jej časť bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.

12.6. Akékoľvek zmeny alebo doplnky tejto Zmluvy je možné vykonať iba písomným dodatkom k tejto Zmluve.

12.7. Každý dodatok k Zmluve musí byť uzavretý v súlade s platným a účinným zákonom o verejnom obstarávaní.

12.8. Neoddeliteľnou súčasťou tejto Zmluvy je:

12.8.1. Príloha č.1 – Opis predmetu zákazky,

12.8.2. Príloha č.2 – Požiadavky na vzdelanie a/alebo odbornú kvalifikáciu osôb a odbornú prax lektorov

12.8.3. Príloha č.3 – Zoznam subdodávateľov pri podpise Zmluvy,

12.8.4. Príloha č.4 – Povinnosti zmluvných strán pri dodržiavaní bezpečnostnej politiky objednávateľa.

12.9. Zmluvné strany vyhlasujú, že si Zmluvu prečítali, jej obsahu porozumeli, zmluvné prejavy sú im dostatočne zrozumiteľné a určité, ich zmluvná voľnosť nie je ničím obmedzená a právny úkon je urobený v písomnej forme, na znak čoho Zmluvu podpísali.

12.10. Zmluva je vyhotovená v štyroch rovnopisoch, z ktorých objednávateľ dostane tri rovnopisy a poskytovateľ jeden rovnopis.

V Bratislave dňa:

Za objednávateľa:

_____

Veronika Gmiterko, MBA
generálna tajomníčka služobného úradu
Ministerstvo financií SR

V Bratislave dňa:

Za poskytovateľa:

_____

Príloha č. 1 Opis predmetu zákazky

Všeobecné požiadavky na školenia bezpečnostných administrátorov pri správe prevádzkovaných bezpečnostných produktov a aplikácií

Školenia v oblastiach:

- Vybudovanie SOC teamu
- Riešenie bezpečnostných incidentov
- Forenzná analýza
- Zabezpečenie systémov Windows
- Zabezpečenie systémov Linux
- Penetračné testovanie webových aplikácií
- Penetračné testovanie interného prostredia

Školenia	Popis	Časový rozsah
Vybudovanie SOC teamu	• Vybudovanie reakčného tímu • Definovanie hlavného reakčného tímu • Systémové nástroje • Identifikácia (zadefinovanie incidentu, detekcia a reakcia na prípadnú vnútornú hrozbu) • Ukladanie (Stratégia dokumentácie: video a audio, ukladanie a karanténa, izolácia od prevereného prostredia) • Vyradenie z prevádzky (Posúdenie, či je ohrozené zálohovanie, úplná prestavba operačného systému, zmena architektúry) • Vylepšenia (monitorovanie systému, očakávanie zvýšenia počtu útokov) • Špecifické akcie na reakcie na rôzne incidenty (špionáž, zneužitie) • Uskladnenie záznamu z incidentu (Formuláre, právna prípustnosť) • Monitoring incidentov (zmena procesov na základe skúseností)	5 dní
Riešenie bezpečnostných incidentov	Riešenie bezpečnostných incidentov minimálne v rozsahu: • prijímanie opatrení na ochranu systémov a sietí postihnutých alebo ohrozených rušivou činnosťou • poskytnutie riešení a poskytnutie stratégií na základe príslušných odborných rád alebo výstrah • pátranie po činnosti narušiteľov na iných častiach siete filtrovanie prevádzky na sieti • systémy prestavby • systémy zaplátania alebo opráv • vypracovanie iných stratégií reakcie alebo stratégií dočasných opravných balíčkov (workarounds). • Reakcie na bezpečnostné incidenty na mieste	5 dní

	• Podpora reakcie na bezpečnostné incidenty • Koordinácia reakcií na bezpečnostné incidenty • Analýza bezpečnostného incidentu • Zhromažďovanie dôkazov	
Forenzná analýza	Forenzné analýzy v rozsahu: 1. forenzný proces a analýza - 0,5 dňa 2. Forenzná akvizícia a právny/legálny vstup - 1 deň a. Forenzná akvizícia desktopov, serverov, úložných zariadení, virtualizácie, Cloud-u 3. Forenzná analýza artefaktov Windows - 1,5 dňa a. dôkaz o vykonaní b. dôkaz o otvorení c. dôkaz o prístupe 4. Forenzná analýza linuxových artefaktov - 0,5 dňa a. dôkaz o vykonaní b. dôkaz o otvorení c. dôkaz o prístupe 5. Forenzná analýza aktívnych zariadení - 0,5 dňa 6. Forenzná analýza pamäte - 1 deň 7. Forenzná analýza sieťovej komunikácie - 1 deň 8. Úvodná analýza škodlivého softvéru - 2 dni	8 dní
Zabezpečenie systémov Windows	Zabezpečenie a OnPrem a cloudových riešení Windows - AD, podporné služby, O365 a pod • komplexné zabezpečenie O365 v súlade s odporúčaniami MS a best practices - 1 deň • komplexné zabezpečenie Azure v súlade s odporúčaniami MS a best practices - 1 deň • Komplexné zabezpečenie Windows Active Directory v súlade s odporúčaniami Center for Information Security úroveň 2 - 3 dni	5 dní
Zabezpečenie systémov Linux	Zabezpečenia systémov na platforme Linux: • Architektúra a bezpečnostné prvky Linuxu - 0,5 dňa • Hardening Linuxu podľa CIS Lvl2 - 3 dni • Reakcia na incidenty s Linuxom - 0,5 dňa	4 dni
Penetračné testovanie webových aplikácií	Penetračné testovanie webových aplikácií v rozsahu OWASP - Úvod a ciele : • Realizovať odhalenie a prieskum vyhľadávača na účely úniku informácií • Vypočítať aplikácie na webovom serveri • Preskúmať komentáre a metadáta webových stránok kvôli úniku informácií • Identifikovať vstupné body aplikácií Testovanie riadenia konfigurácie a nasadenia - nesprávna konfigurácia zabezpečenia • Testovanie konfigurácie siete/infraštruktúry	5 dní

	• Testovanie konfigurácie aplikačnej platformy • Testovanie manipulácie s príponami súborov pre citlivé informácie • Preskúmanie citlivých informácii v starých, záložných a nereferencovaných súborov • Testovanie zabezpečenia HTTP Strict Transport Testovanie správy identít: • Test definícií rolí • Testovanie procesu registrácie používateľa • Testovanie procesu poskytovania/vytvárania účtov • Testovanie výčtu účtov a hádateľného používateľského účtu • Testovanie slabej alebo nevykonávanej politiky pre používateľské mená Testovanie overovania: • Testovanie poverení prenášaných cez šifrovaný kanál • Testovanie predvolených poverení • Testovanie funkčnosti zapamätania hesla • Testovanie politiky hesiel T • Testovanie bezpečnostnej otázky/odpovede Testovanie autorizácie: • Testovanie prechádzania adresárov/obsahu súborov • Testovanie obchádzania autorizačnej schémy • Testovanie zvýšenia oprávnení • Testovanie nezabezpečených priamych odkazov na objekty Testovanie správy relácií: • Testovanie obchádzania schémy správy relácií • Testovanie na falšovanie krížových požiadaviek na stránky (CSRF) • Testovanie funkčnosti odhlásenia • Testovanie časového limitu relácie Testovanie overovania vstupov: • Analýza chybových kódov • Analýza sledovania zásobníka OWASP Top 10 :	

	• Injekcie • Nefunkčné overovanie a správa relácií • Odhalenie citlivých údajov • Externé entity XML (XXE) • Nefunkčné riadenie prístupu • Nesprávna konfigurácia zabezpečenia • Cross Site Scripting – XSS • Nezabezpečená deserializácia • Používanie komponentu so známymi zraniteľnosťami • Nedostatočné zaznamenávanie a monitorovanie Testovanie na strane klienta/bezpečný kód HTML5: • Testovanie vykonávania JavaScriptu • Testovanie HTML a CSS Injection • Testovanie presmerovania URL na strane klienta • Testovanie manipulácie so zdrojmi na strane klienta • Testovanie zdieľania zdrojov medzi pôvodcami / Cross Origin Resource Sharing • Testovanie Clickjacking • Testovanie lokálneho úložiska	
Penetračné testovanie interného prostredia	Penetračné testovanie interného prostredia v rozsahu • Proces etického hackingu - 0,5 dňa • Skenovanie siete a enumerácia - 1 deň • Skenovanie a analýza zraniteľností - 0,5 dňa • Využívanie - používanie a modifikácia verejných exploitov - 1 deň • Post exploitačné techniky a C2 - 1 deň • Útoky na Active directory - 1 deň	5 dní

Školenia pre penetračné testovanie webových aplikácií a interného prostredia minimálne v rozsahu :

- Rozpoznávanie (Používanie Whois dopredného a spätného vyhľadávania, ARIN, RIPE a APNIC. Získanie systému názvov domén, Zhromažďovanie údajov z pracovných ponúk, webových stránok a vládnych databáz, Identifikácia verejne kompromitovaných účtov, Malta).
- Skenovanie (Lokalizácia a útok na súkromné a firemné siete Wi-Fi, Identifikácia a použitia proprietárnych bezdrôtových systémov. Skenovanie portov: Tradičné, skryté a slepé skenovanie. Aktívne a pasívne metódy fingerprintingu, systémov, Definovanie filtrovania firewallových pravidiel.

Vyhľadávanie zraniteľností pomocou programu Nessus a iných nástrojov, Distribúcia skenovania pomocou cloudových agentov s cieľom vyhnúť sa zaradeniu na čiernu listinu)

- Vyhýbanie sa systému detekcie prienikov (IDS) (zmarenie IDS na úrovni aplikácie: Využitie bohatej syntaxe počítačového jazyka (rich computer language syntax), Taktika vyhýbania sa sieťovým útokom IDS, Obchádzanie IDS/IPS pomocou techník obfuscate TCP)
- Vyčíslenie cieľov služby Windows Active Directory (Vyčíslenie Windows Active Directory domén pomocou BloodHound, SharpView, príkazy a ovládanie systému Windows pomocou PowerShell Empire, pripojenie operačného systému z Linux do systému Windows, obrana proti útokom SMB pomocou pokročilých sieťových funkcií systému Windows)
- Útoky na fyzickú vrstvu (využívanie odkrytých USB portov, jednoduché odcudzenie identity v sieti za účelom obnovenia prihlasovacích údajov, krádež knižníc hesiel s nástrojmi na obnovenie systému za studena)
- Zhromažďovanie a analýza paketov (Bettercap, Active Sniffing, LLMNR poisoning, WPAD útoky, DNS cache poisoning: Presmerovanie internetovej prevádzky, Používanie a zneužívanie Netcatu vrátane zadných vrátok a sneaky relays, varianty spoofingu IP, vyhýbanie sa šifrovaniu a útoky na staršie verzie)
- Útoky na operačný systém na úrovni aplikácií (Buffer overflow in depth, Metasploit exploitation framework, AV and application whitelist bypass techniques)
- Netcat (prenos súborov, vytváranie zadných dverí a shell dusting, Netcat relays)
- Obídenie zabezpečenia koncového bodu (Detekcia obídenia pomocou veilu, magic unicorn, spustenie PowerShellu ako nástroja útoku, vyhnutie sa AV pomocou Ghostwritingu, rekonfigurácia nástroja útoku pomocou natívnych binárnych súborov)
- Prelomenie hesla (prelomenie hesla pomocou "" John the Ripper "", Útoky Hashcat Mask, Moderné útoky na systém Windows Pass-the-Hash)
- Útoky na webové aplikácie (Account collection, SQL Injection: Manipulácia s back-endovými databázami, klonovanie relácií: únos relácií iných používateľov, Cross-site scripts)
- Útoky na odmietnutie služby (distribuované odmietnutie služby: Pulse Zombies and Reflected Attacks, Local Denial of Service)
- Udržiavanie prístupu (zadné vrátka: Používanie Poison Ivy, VNC, Ghost RAT a ďalšie, Trojan Horse Backdoors, Rootkits: Nahradenie binárnych spustiteľných súborov podlými variantmi, rootkity na úrovni jadra: útok na srdce operačného systému (Rooty, Avatar a Alureon))
- Skrývanie ciest (skrývanie súborov a adresárov, úprava logov v systémoch Windows a Unix, úprava záznamov v denníku: UTMP, WTMP, história shellu atď., skryté kanály cez HTTP, ICMP, TCP a iné protokoly, analýza útoku z pamäte).
- Praktická analýza (Nmap Port Scanner, Nessus Vulnerability Scanner, Network Mapping, Netcat: File Transfer, Backdoors and Relays, Privilege Escalation)

Každé školenie musí obsahovať:

- Prezentáciu vo forme PowerPoint
- Podrobnú dokumentáciu
- Testovacie prostredie na virtualizačnej platforme, ktoré je použiteľné aj po ukončení školenia a obnoviteľné do pôvodného stavu
- Návod, resp. pracovný zošit pre jednotlivé cvičenia
- Podklady pre školiteľa, aby bolo možné dané školenia opakovať aj s iným trénerom.
- Vytvorenie praktického tréningového scenára pre každý Playbook v rozsahu minimálne 4 hodín

Ďalšie požiadavka na Školenia:

- vytvorenie a dokumentácie procesov a Playbook-ov riešenia bezpečnostných incidentov minimálne pre :
    - Ransowmare útok
        - Vytvorenie praktických scenárov na virtualizačnej platforme pre Rasnomware (napríklad Case study Conti)"
    - Malware spreading
    - Data Breach
    - DDOS útok
    - Business Email Compromise
    - vytvorenie Playbook-ov pre ohodnocovanie zraniteľností externé
    - vytvorenie Playbook-ov pre ohodnocovanie zraniteľností interné
    - vytvorenie Playbook-ov pre zachytávanie digitálnych stôp
        - sieť
        - pracovné stanice
        - notebooky
        - mobilné zariadenia
        - servery
    - Vytvorenie Playbook-ov pre základnú forenznú analýzu
    - Pre každý Playbook vytvorenie praktického tréningového scenára v rozsahu minimálne 4 hodín
- virtualizačné prostredie
- Step by step Guide pre (môže byt súčasť dodávaných Playbook-ov) :
    - Rozpoznávanie (Používanie Whois dopredného a spätného vyhľadávania, ARIN, RIPE a APNIC, získanie systému názvov domén, zhromažďovanie údajov z pracovných ponúk, webových stránok a vládnych databáz, identifikácia verejne kompromitovaných účtov, Malta).
    - Skenovanie (Lokalizácia a útok na súkromné a firemné siete Wi-Fi, identifikácia a použitia proprietárnych bezdrôtových systémov. Skenovanie portov: Tradičné, skryté a slepé skenovanie, Aktívne a pasívne metódy fingerprintingu, systémov, Definovanie filtrovania firewallových pravidiel, Vyhľadávanie zraniteľností pomocou programu Nessus a iných nástrojov, Distribúcia skenovania pomocou cloudových agentov s cieľom vyhnúť sa zaradeniu na čiernu listinu)
    - Vyhýbanie sa systému detekcie prienikov (IDS) (zmarenie IDS na úrovni aplikácie: Využitie bohatej syntaxe počítačového jazyka (rich computer language syntax), Taktika vyhýbania sa sieťovým útokom IDS, Obchádzanie IDS/IPS pomocou techník obfuskacie TCP)
    - Vyčíslenie cieľov služby Windows Active Directory (Vyčíslenie Windows Active Directory domén pomocou BloodHound, SharpView, príkazy a ovládanie systému Windows pomocou PowerShell Empire, Pripojenie operačného systému z Linux do systému Windows, obrana proti útokom SMB pomocou pokročilých sieťových funkcií systému Windows)
    - Útoky na fyzickú vrstvu (využívanie odkrytých USB portov, jednoduché odcudzenie identity v sieti za účelom obnovenia prihlasovacích údajov, krádež knižníc hesiel s nástrojmi na obnovenie systému za studena)
    - Zhromažďovanie a analýza paketov (Bettercap, Active Sniffing, LLMNR poisoning, WPAD útoky, DNS Cache poisoning: Presmerovanie internetovej prevádzky, používanie a zneužívanie Netcatu vrátane zadných vrátok a Sneaky Relays, varianty spoofingu IP, vyhýbanie sa šifrovaniu a útoky na staršie verzie)
    - Útoky na operačný systém na úrovni aplikácií (Buffer Overflow in Depth, Metasploit exploitation framework, AV and application whitelist bypass techniques)
    - Netcat (prenos súborov, vytváranie zadných dverí a shell dusting, Netcat relays)
    - Obídenie zabezpečenia koncového bodu (detekcia obídenia pomocou veilu, magic unicorn, spustenie PowerShellu ako nástroja útoku, Vyhnutie sa AV pomocou Ghostwritingu, rekonfigurácia nástroja útoku pomocou natívnych binárnych súborov)

- Prelomenie hesla (Prelomenie hesla pomocou "" John the Ripper "", Útoky Hashcat Mask, Moderné útoky na systém Windows Pass-the-Hash)
- Útoky na webové aplikácie (Account collection, SQL Injection: Manipulácia s back-endovými databázami, klonovanie relácií: Únos relácií iných používateľov, Cross-site scripts)
- Útoky na odmietnutie služby (distribuované odmietnutie služby: Pulse Zombies and Reflected Attacks, Local Denial of Service)
- Udržiavanie prístupu (zadné vrátka: Používanie Poison Ivy, VNC, Ghost RAT a ďalšie, Trojan Horse Backdoors, Rootkits: Nahradenie binárnych spustiteľných súborov podlými variantmi, Rootkity na úrovni jadra: Útok na srdce operačného systému (Rooty, Avatar a Alureon))
- Skrývanie ciest (skrývanie súborov a adresárov, Úprava logov v systémoch Windows a Unix, úprava záznamov v denníku: UTMP, WTMP, história Shell-u atď., skryté kanály cez HTTP, ICMP, TCP a iné protokoly, analýza útoku z pamäte).
- Praktická analýza (Nmap Port Scanner, Nessus Vulnerability Scanner, Network Mapping, Netcat: File Transfer, Backdoors and Relays, Privilege Escalation)

- Prezentácia
- Podrobná dokumentácia

Dodané materiály budú použité len v rezorte Ministerstva financií SR a organizáciách patriacich pod rezort MF SR.

Príloha č. 2 Požiadavky na vzdelania a/alebo odbornú kvalifikáciu osôb a odbornú prax lektorov

- Skúsenosti minimálne 2 roky v oblasti ohodnocovania zraniteľnosti alebo penetračného testovania (požiadavku musí spĺňať minimálne jeden lektor).
- Skúsenosti minimálne 5 rokov v oblasti návrhu alebo posudzovania informačných systémov alebo infraštruktúr, riešenia bezpečnostných incidentov alebo bezpečnostných auditov (požiadavku musí spĺňať minimálne jeden lektor).
- Držiteľ certifikátu OSCP alebo GPEN alebo GXPN alebo OSCE (požiadavku musí spĺňať minimálne jeden lektor).
- Držiteľ certifikátu CISSP alebo CISA (požiadavku musí spĺňať minimálne jeden lektor).
- Minimálne jedna nájdená a publikovaná bezpečnostná zraniteľnosť, ktorá má pridelené CVE (požiadavku musí spĺňať minimálne jeden lektor).

Príloha č. 3

Zoznam subdodávateľov pri podpise Zmluvy

P. č.	Meno a priezvisko / Obchodné meno	Adresa pobytu / Sídlo	Dátum narodenia / IČO	Údaje o osobe oprávnenej konať za subdodávateľa
1.				
2.				
3.				
4.				
5.				

Príloha č. 4

Povinnosti zmluvných strán pri dodržiavaní bezpečnostnej politiky objednávateľa

Preambula

Táto príloha Zmluvy vychádza z ustanovení platného Interného riadiaceho aktu MF SR č. 10/2014 Smernica o prístupe tretích strán na Ministerstve financií Slovenskej republiky. Ustanovenia tejto prílohy sa použijú pre účely tejto Zmluvy primerane s prihliadnutím na predmet Zmluvy a práva a povinnosti zmluvných strán v Zmluve upravené.

1. Na účely tejto Zmluvy sa rozumie:

a) treťou stranou

1. poskytovateľ a jeho subdodávatelia,
2. externí spolupracovníci,
3. fyzické osoby.

b) aktívom objekt, subjekt, štruktúra, vzťah alebo proces, ktorého narušením môže MF SR utrpieť stratu; aktíva môžu byť hmotné a nehmotné: budovy, hardvér, softvér, nosiče informácií, na nich uložené informácie, komunikačná technika, kancelárska technika, dokumenty v papierovej a elektronickej podobe, dodávateľská podpora, dôležité osoby potrebné na prevádzku organizácie, identifikačné prostriedky, bezpečnostné prostriedky, peniaze, dobré meno, kredit a pod.,

c) bezpečnostným incidentom každá situácia alebo stav, ktorý priamo ohrozuje bezpečnosť a/alebo funkčnosť aktíva. Bezpečnostný incident (ďalej len „BI“) môže byť vyvolaný náhodným faktorom, neúmyselným činom, úmyselným útokom alebo podvodom, najmä je to situácia alebo stav:

1. ktorý je v rozpore so všeobecne záväznými právnymi predpismi, schválenými dokumentmi bezpečnostnej politiky alebo inými internými riadiacimi aktmi ministerstva, ktoré sa týkajú informačného systému, napríklad ak sa niekto pokúša zisťovať informácie o informačnom systéme a prístupových heslách,
2. pri ktorom sú čiastočne alebo úplne nefunkčné systémy (technické zariadenia), hrozí ich zničenie (napríklad ohňom, vodou a i.) alebo je narušená dostupnosť, dôvernosť alebo integrita údajov,
3. pri ktorom je v informačnom systéme alebo v jeho časti prítomné škodlivé programové vybavenie (napr. vírová nákaza, neautorizovaný softvér) a systémová „diera“,
4. pri ktorom je zrejmé alebo existuje podozrenie z vydierania, únosu, spravodajských aktivít alebo iného kriminálneho činu vrátane teroristického útoku.

d) oprávneným zamestnancom zamestnanec MF SR a tretej strany poverený výkonom určených úloh vyplývajúcich z činností spojených s naplnením účelu Zmluvy (napr. projektový manažér).

2. Bezpečnostné povinnosti poskytovateľa

2.1 Zamestnanci tretej strany sú pri vstupe do objektu MF SR a odchode z objektu MF SR povinní riadiť sa pokynmi strážnej služby.

2.2 Do objektu MF SR môžu zamestnanci tretej strany vstupovať a z neho odchádzať len k tomu určenými vchodmi pre osoby na Štefanovičovej alebo Kyčerského ulici.

2.3. Tretia strana sa zaväzuje, že

2.3.1. pred začatím činností spojených s naplnením účelu Zmluvy oznámi MF SR personálne obsadenie svojho tímu, ktorý bude vykonávať činnosti spojené s naplnením účelu Zmluvy,

2.3.2. bude bezodkladne informovať MF SR o všetkých personálnych zmenách vo svojom tíme, ktorý vykonáva činnosti spojené s naplnením účelu Zmluvy,

2.3.3. oboznámi svojich zamestnancov, resp. tretie osoby realizujúce činnosti spojené s naplnením účelu Zmluvy pre MF SR s bezpečnostnými požiadavkami v rozsahu tejto Zmluvy,

2.3.4. oboznámi svojich zamestnancov resp. tretie osoby realizujúce činnosti spojené s naplnením účelu Zmluvy pre MF SR a následne zabezpečí od týchto zamestnancov dodržiavanie povinnosti:

- ochrany údajov a záväzku mlčanlivosti o údajoch, s ktorými prišli počas výkonu prác pre MF SR do styku a to aj po ukončení pracovného, resp. služobného pomeru,
- zachovávať mlčanlivosť o osobných údajoch, s ktorými počas práce pre MF SR prídu do styku, ako aj zákaz ich využitia pre osobnú potrebu, bez súhlasu MF SR ich nesmie zverejniť, nikomu poskytnúť ani sprístupniť, pričom povinnosť mlčanlivosti trvá aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, zmluvného pomeru alebo obdobného pracovného vzťahu k tretej strane; povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, zdokumentovať všetky zásahy do IKT MF SR podľa pokynov oprávneného zamestnanca za MF SR,
- rešpektovať operatívne pokyny zamestnancov s pridelenými bezpečnostnými rolami na MF SR a oprávnených zamestnancov počas výkonu práce pre MF SR,
- rešpektovať autorské práva k materiálom poskytnutým MF SR,
- vrátiť MF SR všetky poskytnuté materiály a údaje, vrátane elektronických a zlikvidovať všetky ich kópie, ak to nebude zmluvne dohodnuté inak,
- poskytnúť potrebnú súčinnosť audítorovi vykonávajúcemu audit IS, ak tento súvisí s výkonom práce na Zmluve pre MF SR.

2.4 V prípade nevyhnutnosti prístupu tretích strán k projektom obsahujúcim utajované skutočnosti sa postupuje podľa ustanovení zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

2.5 Každý zamestnanec tretej strany resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu Zmluvy pre MF SR je povinný zistenie bezpečnostného incidentu alebo podozrenie na bezpečnostný incident bezodkladne nahlásiť na určené kontaktné miesto, ktorým je Help Desk (tel. číslo: +421 2 5958 2400, kl.: 2400, resp. email: helpdesk@mfsr.sk).

2.6 Každý zamestnanec tretej strany, resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu Zmluvy pre MF SR, sú povinní pri vyšetrovaní bezpečnostných incidentov zamestnancom alebo zamestnancami MF SR poskytnúť potrebnú súčinnosť.

2.7 Po vzniku bezpečnostného incidentu nesmie zamestnanec tretej strany, resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu Zmluvy pre MF SR, vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov bezpečnostného incidentu.