**Agentura komunikačních a informačních systémů**
**Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk**

Čj. MO 264723/2025-3255 Počet stran: 10
SpMO 37783/2024-3255 Přílohy: 5

# RÁMCOVÁ DOHODA
## č. 25106000291
## Kurzy SANS

## I. Smluvní strany

**Česká republika – Ministerstvo obrany**
Sídlo: Tychonova 221/1, 160 00 Praha 6 - Hradčany
IČ: 601 626 94
DIČ: CZ 601 626 94
[redacted]

(dále jen „**objednatel**“)

a

The Escal Institute of Advanced Technologies, Inc.
Sídlo: 11200 Rockville Pike, Suite 200, 20852, Maryland, Spojené státy americké
IČ: 252 67 77
DIČ: CZ681636906
[redacted]

(dále jen „**poskytovatel**“)
(objednatel a poskytovatel dále společně také „**smluvní strany**“ jednotlivě „**smluvní strana**“)

podle ust. § 1746 odst. 2, ustanovením § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**občanský zákoník**“) a ustanovení zákona č. 121/2000 Sb., autorský zákon, v platném znění (dále jen „**autorský zákon**“), uzavírají na základě výsledku nadlimitního zadávacího řízení pro veřejnou zakázku „**Kurzy SANS**“ zadanou v elektronickém nástroji NEN pod systémovým číslem N006/24/V00029855 na základě ust. § 130 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění tuto rámcovou dohodu (dále jen „**Rámcová dohoda**“).

## II. Účel Rámcové dohody

2.1. Účelem Rámcové dohody je zabezpečení vysoce odborně připravených příslušníků InKys pro včasné a soustavné přijímání příslušných nápravných a preventivních opatření pro potřeby výkonu služební činnosti na daném služebním místě.

2.2. Stanovit rámcové podmínky mezi objednatelem a poskytovatelem, na jejichž základě bude poskytovatel uzavírat s objednatelem tzv. Realizační smlouvu (dále také jen „**Realizační smlouva**“ nebo „**Realizační smlouvy**“) v souladu s touto Rámcovou dohodou, tj. formou písemného návrhu objednatele na uzavření Realizační smlouvy dle přílohy č. 2 Rámcové dohody a písemného přijetí návrhu smlouvy poskytovatelem, tj. podpisem návrhu Realizační smlouvy poskytovatelem.

## III. Předmět Rámcové dohody

3.1. Předmětem Rámcové dohody je závazek poskytovatele poskytnout objednateli službu, a to **školení v oblasti IT**, které spadá pod správu zabezpečení v působnosti komunikačních a informačních systémů resortu Ministerstva obrany ČR, a to v rozsahu, kvalitě a za podmínek dle Rámcové dohody a jednotlivých Realizačních smluv. Kurzy poskytnou základní dovednosti a techniky v oblasti zabezpečení informací, obranné síťové architektury, analýze malware, digitální forenzní analýze a reakci na bezpečnostní incidenty. Dále rozšíření znalostí v oblasti open-source inteligence a manažerských dovednostech bezpečnostních lídrů (dále také jen „**služba**“). Bližší popis služby je uveden v příloze č. 1 Cenová kalkulace a specifikace služby Rámcové dohody.

3.2. Služba bude realizována podle potřeb objednatele formou dílčích plnění na základě uzavřených Realizačních smluv k poskytnutí plnění.

3.3. Závazek objednatele za řádně poskytnutou službu uhradit poskytovateli řádně a včas smluvenou cenu.

## IV. Cena

4.1. Maximální celková cena za službu je **8 468 332,16 Kč bez DPH a** zaokrouhleno **ve výši 10 246 681,93 Kč s DPH** (slovy Deset miliónů dvě stě čtyřicet šest tisíc šest set osmdesát jedna korun českých devadesát tři haléřů), (dále jen „**Finanční objem**“). Finanční objem představuje maximální cenu za souhrnné plnění dle Rámcové dohody

a jednotlivých Realizačních smluv a zahrnuje veškeré náklady poskytovatele související s plněním Rámcové dohody a jednotlivých Realizačních smluv.

4.2. Cena jednotlivých položek služby je stanovena v příloze č. 1 Cenová kalkulace a specifikace služby Rámcové dohody.

4.3. Cena za poskytnuté dílčí plnění služby bude stanovena dle formy kurzu (prezenční/ on – line) a skutečného počtu účastníků vyplývající z dílčí Realizační smlouvy dle ceny kurzu dle přílohy č. 1 Cenová kalkulace a specifikace služby Rámcové dohody.

4.4. Objednatel není povinen Finanční objem vyčerpat.

4.5. Cenu je možné zvýšit pouze z důvodů zvýšení DPH, a to na základě písemného dodatku ve smyslu čl. XII. odst. 12.8. Rámcové dohody.

## V. Doba platnosti Rámcové dohody

5.1. Rámcová dohoda se uzavírá na dobu určitou do 31. prosince 2025.

## VI. Lhůta a místo plnění

6.1. Poskytovatel se zavazuje službu poskytnout v průběhu roku 2025 dle podmínek stanovených Rámcovou dohodou a příslušnou Realizační smlouvou.

6.2. Místem plnění služby:

- v případě provedení kurzu ve školícím středisku poskytovatele na adrese poskytovatele:

  - Nizozemsko, Amsterdam, Amsterdam Marriott Hotel, Stadhouderskade 12;
  - Dánsko, Copenhagen, Copenhagen Marriott Hotel, Kalvebod Brygge 5, 1560;
  - Francie, Paris, Crowne Plaza Paris – Republique, 10 Pl. de la République, 75011;
  - Francie, Paris, Paris Marriott Opera Ambassador Hotel, 16 Bd Haussmann, 75009;
  - Francie, Paris, Hyatt Regency Paris Étoile, 3 Pl. du Général Kœnig, 75017;
  - Spojené království, London, De Vere Grand Connaught Rooms, 61-65 Great Queen St;
  - Spojené království, London, ETC Venues Monument, 8 Eastcheap, EC3M 1AE;
  - Estonsko, Tallinn, Hilton Tallinn Park, F. R. Kreutzwaldi 23, 10147;
  - Německo, Munich, Munich Marriott Hotel, Berliner Strasse 93, Bavaria;
  - Norsko, Oslo, Radisson Blu Plaza Oslo, Sonja Henies plass 3;
  - Česká republika, Prague, Vienna House By Wyndham Andels Prague, Stroupežnického 21, 150 00 Praha 5-Smíchov;
  - US, Hyatt Centric Fisherman's Wharf San Francisco, 555 North Point Street, San Francisco, CA 94133;
  - US, The Westin Alexandria Old Town, 400 Courthouse Square, Alexandria, VA 22314;

- US, Hilton New Orleans Riverside, Two Poydras St., New Orleans, LA 70130;
- US, Alma San Diego, 1047 5th Avenue, San Diego, CA 92101;
- US, The Westin Crystal City, 1800 Richmond Highway, Arlington, VA 22202;
- US, Hilton Baltimore Inner Harbor, 401 West Pratt Street, Baltimore, MD 21201;
- US, Marriott San Antonio Airport, 77 NE Interstate 410 Loop, San Antonio, TX 78216;
- US, Hyatt Regency Orlando, 9801 International Drive, Orlando, FL 32819;
- US, The Drake, a Hilton Hotel, 140 East Walton Place, Chicago, IL 60611-1501 4;
- US, Manchester Grand Hyatt, 1 Market Place, San Diego, CA 92101;
- US, Nashville Marriott at Vanderbilt University, 2555 West End Avenue, Nashville, TN 37203;
- US, Hyatt Regency Coral Gables, 50 Alhambra Plaza, Coral Gables, FL 33134;
- US, The Royal Sonesta Harbor Court Baltimore, 550 Light Street, Baltimore, MD 21202;
- US, Embassy Suites by Hilton Denver Downtown, 1420 Stout Street, Denver, CO 80202;
- US, Washington Hilton, 1919 Connecticut Avenue, N.W., Washington D.C. 20009;
- US, Hilton Anaheim, 777 W Convention Way, Anaheim, CA 92802;
- US, Huntsville Marriott at the Space & Rocket Center, 5 Tranquility Base, Huntsville, AL 35805;
- US, Hilton Boston Park Plaza, 50 Park Plaza, Boston, MA 02116;
- US, Hilton Virginia Beach Oceanfront, 3001 Atlantic Avenue, Virginia Beach, VA, 23451;
- US, Caesars Palace, 3570 Las Vegas Blvd South, Las Vegas, NV 89109;
- US, DoubleTree by Hilton McLean Tysons, 1960 Chain Bridge Road, McLean, VA 22102;
- US, The Westin Alexandria Old Town, 400 Courthouse Square, Alexandria, VA 22314;
- US, Hilton Dallas Lincoln Center, 5410 Lyndon B. Johnson Freeway, Dallas, TX 75240;
- US, Salt Lake Marriott Downtown at City Creek, 75 South West Temple, Salt Lake City, UT;
- US, Palmer House Hilton, 17 East Monroe Street, Chicago, IL 60603;

- v případě provedení kurzu formou on-line, poskytovatel uvede do příslušné Realizační smlouvy k danému kurzu příslušný internetový odkaz k přístupu do školící platformy poskytovatele.

6.3. Poskytovatel je povinen poskytnout objednateli školení nejpozději ve lhůtě uvedené v Realizační smlouvě k plnění dle čl. VII. Rámcové dohody.

## VII. Podmínky poskytování služby

7.1. Pověřený zástupce kupujícího pro řešení technicko - organizačních záležitostí dle čl. I. této Rámcové dohody (dále jen" **zástupce objednatele za VÚ 1980**") zašle poskytovateli neprodleně po uzavření této Rámcové dohody na e-mail poskytovatele [redacted] žádost o harmonogram kurzů pro 1. čtvrtletí roku 2025 s tím, že v žádosti uvede název kurzu, formu kurzu (prezenční/on – line), počet účastníků a časové období od – do pro předpokládaný termín kurzů. Poskytovatel do 10 pracovních dnů od doručení návrhu zašle zástupci objednatele za VÚ 1980 harmonogram vyžádaných kurzů. Pro další kurzy je zástupce objednatele za VÚ 1980 povinen požádat poskytovatele o harmonogram výše uvedeným způsobem vždy 14 dní před nadcházejícím čtvrtletím.

7.2. Harmonogram musí být odsouhlasen mezi zástupcem objednatele za VÚ 1980 a poskytovatelem. Změna v harmonogramu školení je možná pouze při odsouhlasení změny oběma stranami a je závazná pro další plnění Rámcové dohody.

7.3. Zástupce objednatele za VÚ 1980, neprodleně po odsouhlasení harmonogramu, zašle e-mailem objednávku k plnění dle přílohy č. 5 této Rámcové dohody osobě pověřené ve věcech smluvních dle čl. I. této Rámcové dohody (dále jen „**zástupce objednatele ve věcech smluvních**"). K objednávce k plnění bude přiložen odsouhlasený harmonogram.

7.4. Zástupce objednatele ve věcech smluvních zpracuje Realizační smlouvu dle přílohy č. 2 této Rámcové dohody za daný kurz dle zaslané objednávky k plnění a odešle prostřednictvím NEN poskytovateli k podpisu.

7.5. Poskytovatel je povinen podepsat doručenou Realizační smlouvu bez zbytečného odkladu po jejím doručení objednatelem poskytovateli a zaslat ji zpět poskytovateli způsobem dle předchozího odstavce.

7.6. Poskytovatel se zavazuje k nakládání s poskytnutými osobními údaji mj. v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, v platném znění (nařízení GDPR).

7.7. Dopravu účastníků školení do místa plnění služby je povinen zabezpečit objednatel na vlastní náklady.

7.8. V případě poskytnutí služby **prezenční formou** je poskytovatel povinen zabezpečit adekvátní prostory pro provedení školení, vybavení těchto prostor potřebnou technikou (výpočetní technika apod.), programovým vybavením a didaktickými pomůckami, které umožní seznámení všech účastníků školení s tématem školení včetně praktických cvičení. Prostory musí umožnit pořizování poznámek v průběhu výkladu i při praktických cvičeních.

7.9. Poskytovatel je povinen provést školení v českém nebo anglickém jazyce a zabezpečit pro dané školení studijní materiály (dále jen „**materiály**") pro všechny účastníky školení v elektronické podobě. Materiály v elektronické podobě budou poskytovatelem všem účastníkům školení natrvalo předány ještě před jeho samotným zahájením školení (prostřednictvím zástupce objednatele za VÚ 1980), přičemž poskytovatel tímto uděluje objednateli bezúplatnou licenci k užití materiálů ve smyslu ust. § 2358 a násl. občanského zákoníku a ust. § 12 a násl. autorského zákona. U materiálů, které nejsou

dílem poskytovatele ve smyslu Autorského zákona a materiálů, u nichž poskytovatel z jakéhokoliv důvodu nevykonává autorské právo, či je jeho autorské právo omezeno právem třetí osoby, je poskytovatel povinen zabezpečit poskytnutí licence podle tohoto odstavce smlouvy osobou, která takové právo vykonává.

7.10. Poskytovatel vydá **certifikát / doklad o absolvování školení pro účastníky**, kteří školení absolvovali. Tento certifikát / doklad předá nebo zašle účastníkům na konci školení.

7.11. Po poskytnutí služby (provedení školení) je poskytovatel povinen vyhotovit Protokol o provedeném školení (dále jen „**Protokol**“) dle přílohy č. 3 této Rámcové dohody a Prezenční listinu dle přílohy č. 4 této Rámcové dohody a zaslat je zástupci objednatele za VÚ 1980. Zástupce objednatele za VÚ 1980 ověří, že údaje v Protokolu a Prezenční listině odpovídají podmínkám Rámcové dohody a příslušné Realizační smlouvě a podepsaný Protokol odešle zpět poskytovateli. Poskytovatel odsouhlasený a podepsaný Protokol přiloží k vystavené faktuře k proplacení a celé odešle Objednateli dle článku VIII. této Rámcové dohody.

7.12. Pověřený zástupce objednatele za VÚ 1980 je oprávněn kontrolovat, zda poskytovatel plní své povinnosti stanovené touto Rámcovou dohodou a příslušnou Realizační smlouvou. V případě zjištění vad v plnění je oprávněn požadovat po poskytovateli jejich neprodlené odstranění, případně je oprávněn určit poskytovateli lhůtu pro jejich odstranění a poskytovatel je povinen zjištěné vady plnění odstranit.

7.13. Poskytovatel umožní pověřenému zástupci objednatele za VÚ 1980 provádět kontrolu školení. Za tímto účelem je poskytovatel povinen předložit pověřenému zástupci objednatele veškerou dokumentaci související s prováděním školení, vyžádanou pověřeným zástupcem objednatele. Poskytovatel je povinen, v případě zjištění vad pověřeným zástupcem objednatele, tyto vady odstranit neprodleně, nebo v objednatelem určené lhůtě.

7.14. V případě, že poskytovatel poskytne jakoukoliv část služby (provede školení) v termínu, který neodpovídá podmínkám této Rámcové dohody a/nebo příslušné Realizační smlouvy, nemá nárok na zaplacení ceny školení, ani na náhradu škody, či ušlého zisku, které mu v souvislosti s přípravou a provedením školení vznikly. Objednatel není v takovém případě povinen učnit jakékoliv jednání k zabezpečení účasti účastníků školení, ani jiné jednání, k nimž je dle této smlouvy povinen v případě řádného poskytnutí služby.

7.15. Smluvní strany jsou oprávněny školení zrušit minimálně 3 pracovní dny před plánovaným konáním v případě vzniku krizové situace, kterou daná smluvní strana nemohla předvídat ani ji zabránit, zejména v důsledku vyhlášení krizového stavu dle zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů, v platném znění, nebo v případě vzniku opatření pro zvládání epidemie onemocnění COVID-19 dle zákona č. 94/2021 Sb. o mimořádných opatřeních při epidemii onemocnění COVID-19 a o změně některých souvisejících zákonů, v platném znění, nebo obdobných epidemií, dále pak z rozhodnutí k mimořádným a preventivním opatřením hlavní hygieničky Ministerstva obrany České republiky. Poskytovateli v takovém případě nevzniká nárok na náhradu škody nebo případných nákladů, nebude-li sjednán náhradní termín a školení nebude realizováno.

7.16. Smluvní strany se dohodly a souhlasí s tím, že služby podle této Rámcové dohody jsou určeny k využití v rámci zákonem stanovené činnosti objednatele a rovněž tak

k zajištění výkonu státní správy a dalších činností stanovených právním řádem České republiky.

## VIII. Platební a fakturační podmínky

8.1. Nárok na úhradu ceny za službu poskytovateli vzniká prvním dnem měsíce následujícího po měsíci, v němž byla služba poskytnuta v rozsahu a kvalitě dle této Rámcové dohody a příslušné Realizační smlouvy, na základě poskytovatelem vystaveného daňového dokladu (dále jen „**faktura**“), a to na bankovní účet uvedený na faktuře.

8.2. Po vzniku práva na úhradu ceny doručí poskytovatel objednateli souhrnnou fakturu za službu poskytnutou v daném kalendářním měsíci elektronicky do datové schránky ID [redacted]ce (Ministerstvo obrany), případně na e-mail: [redacted] to do 15. dne měsíce následujícího po měsíci, v němž byla služba poskytnuta. Poskytovatel je povinen doručit objednateli fakturu v některém z následujících formátů: **ISDOC, PDF/A,** UBL 2.1 ISO/IEC, UN/CEFACT Cil, JPEG, PNG, TIF. Velikost jedné zprávy může být maximálně 20 MB a může obsahovat vždy pouze jednu fakturu s příslušnými přílohami. V případě, že nelze použít elektronickou komunikaci, je poskytovatel oprávněn zaslat fakturu v listinné podobě na adresu pro doručování korespondence.

8.3. Faktura musí obsahovat náležitosti stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění (dále jen „**zákon o DPH**“), a ustanovením § 435 Občanského zákoníku. Dále musí faktura obsahovat zejména tyto údaje:

- číslo Rámcové dohody a příslušné Realizační smlouvy;
- rozpis cen po jednotlivých položkách zboží;
- přesnou fakturační adresu kupujícího:

Odběratel

[redacted]

8.4. K faktuře musí být připojen Protokol dle přílohy č. 3 Rámcové dohody, podepsaný pověřenou osobou objednatele a Prezenční listinu dle přílohy č. 4 s podpisy účastníků školení.

8.5. Objednatel neposkytuje zálohové platby.

8.6. Splatnost faktur je stanovena v délce třiceti (30) dnů ode dne doručení faktury objednateli. Je-li na faktuře uvedena odlišná doba splatnosti, platí ujednání dle věty předchozí. Bude-li faktura doručena objednateli v období od 15. prosince příslušného kalendářního roku do 15. ledna roku následujícího, prodlužuje se splatnost takové faktury o 30 dnů.

8.7. Faktura se považuje za uhrazenou okamžikem odepsání fakturované částky z účtu objednatele ve prospěch poskytovatele.

8.8. Objednatel je oprávněn fakturu vrátit před uplynutím lhůty splatnosti, neobsahuje-li požadované náležitosti nebo doklad uvedený v Rámcové dohodě, obsahuje nesprávné

cenové údaje, nebo má jiné závady v obsahu. Při vrácení faktury objednatel uvede důvod jejího vrácení a poskytovatel vystaví fakturu novou. Oprávněným vrácením faktury přestává běžet původní lhůta splatnosti a běží znovu ode dne doručení nové faktury objednateli. Poskytovatel je povinen novou fakturu doručit objednateli do 10 dnů ode dne doručení oprávněně vrácené faktury poskytovateli.

8.9. Pokud budou u poskytovatele shledány důvody k naplnění institutu ručení za daň podle § 109 Zákona o DPH, bude objednatel při zasílání ceny vždy postupovat zvláštním způsobem zajištění daně podle § 109a zákona o DPH. Smluvní strany berou na vědomí a souhlasí, že v takovém případě bude platba poskytovateli za předmět smlouvy snížena o daň z přidané hodnoty, která bude odvedena objednatelem na účet správce daně místně příslušného poskytovateli. Poskytovatel obdrží úhradu za poskytnuté služby ve výši částky odpovídající základu daně a nebude nárokovat úhradu ve výši daně z přidané hodnoty odvedené na účet jemu místně příslušnému správci daně.

## IX. Práva a povinnosti smluvních stran

9.1. Poskytovatel se zavazuje respektovat a dodržovat pokyny objednatele.

9.2. Objednatel se zavazuje poskytnout poskytovateli maximální součinnost pro řádnou realizaci služby.

## X. Smluvní pokuta

10.1. Za nesplnění závazku z Rámcové dohody a Realizačních smluv se sjednávají následující smluvní pokuty:

10.2. V případě nedodržení lhůt a rozsahu poskytování služby dle podmínek Rámcové dohody a příslušné Realizační smlouvy je poskytovatel povinen zaplatit smluvní pokutu ve výši 0,5 % z ceny za školení, s jehož poskytnutím je v prodlení vč. DPH zaokrouhlené na celé koruny dolů za každý den prodlení s poskytnutím služby. Objednatel uplatní nárok na smluvní pokutu a její výši u poskytovatele písemnou výzvou. Poskytovatel je povinen zaplatit uplatněnou smluvní pokutu bankovním převodem na bankovní účet objednatele do 30 dnů od doručení této výzvy objednatelem poskytovateli.

10.3. Smluvní pokutu je poskytovatel povinen zaplatit bez ohledu na to, vznikla-li objednateli škoda. Náhrada škody je vymahatelná samostatně v plné výši vedle smluvní pokuty.

10.4. Povinnost k zaplacení smluvní pokuty vzniká pouze v případě zaviněného porušení povinnosti, ke které se smluvní pokuta váže, povinnou smluvní stranou.

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

## XI. Zánik smluvního vztahu

11.1. Smluvní strany se dohodly na tom, že Rámcová dohoda a/nebo Realizační smlouva zaniká vedle ostatních případů stanovených občanským zákoníkem také jednostrannou výpovědí Rámcové dohody a/nebo Realizační smlouvy bez výpovědní doby ze strany

objednatele pro její podstatné porušení poskytovatelem, dále v případě, že poskytovatel uvedl v nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek realizace veřejné zakázky, na jejímž základě byla Rámcová dohoda a/nebo Realizační smlouva uzavřena.

11.2. Objednatel je oprávněn vypovědět Rámcovou dohodu bez výpovědní doby v případě, že výše zůstatku Finančního objemu znemožňuje objednateli nákup služby.

11.3. Podstatným porušením povinnosti ze strany poskytovatele se rozumí:

a) prodlení poskytovatele s plněním služby dle Rámcové dohody a příslušné Realizační smlouvy delší 10 dnů;

b) prodlení poskytovatele s odstraněním vad školení po dobu delší než 10 (deset) pracovních dnů ode dne ohlášení vady objednatelem poskytovateli, případně od uplynutí lhůty, kterou objednatel poskytovateli pro odstranění vady určil;

c) realizace plnění služeb poskytovatelem, které je v rozporu s ustanoveními této Rámcové dohody/ Realizační smlouvy a ani po písemném upozornění objednatelem nesjedná poskytovatel nápravu v náhradním termínu;

d) opakované porušení povinností poskytovatele vyplývající z této Rámcové dohody a/nebo Realizační smlouvy, přičemž opakovaným porušením se rozumí nejméně třetí porušení jakékoliv povinnosti.

## XII. Závěrečná ustanovení

12.1. Všechny právní vztahy, které vzniknou při realizaci závazků vyplývajících z Rámcové dohody a Realizační smlouvy, se řídí právním řádem České republiky, bez přihlédnutí k jeho kolizním normám.

12.2. Smluvní strany se dohodly, že si bezodkladně sdělí skutečnosti, které se týkají změn některého ze základních identifikačních údajů, včetně právního nástupnictví a veškeré informace relevantní z pohledu plnění Rámcové dohody a Realizační smlouvy. Změna údajů obsažených v čl. I a kontaktní údaje Objednatele či Poskytovatele (včetně změny osob pověřených) Rámcové dohody a Realizační smlouvy se nepovažuje za změnu, kterou je třeba činit dodatkem k Rámcové dohodě, nebo Realizační smlouvě; smluvní strana, u které ke změně došlo, je povinna tuto změnu oznámit písemně datovou zprávou druhé smluvní straně bez zbytečného odkladu. Účinnost změny nastává okamžikem doručení oznámení o změně příslušné smluvní straně.

12.3. Poskytovatel není oprávněn v průběhu plnění svého závazku podle Rámcové dohody a Realizační smlouvy a ani po jeho splnění bez písemného souhlasu objednatele poskytovat jakékoli informace, se kterými se seznámil v souvislosti s plněním svého závazku a podkladovými materiály v listinné či elektronické podobě, které mu byly poskytnuty v souvislosti s plněním závazku podle Rámcové dohody, třetím osobám (mimo subdodavatele). Poskytnuté informace jsou ve smyslu § 1730 občanského zákoníku důvěrné.

12.4. Poskytovatel podpisem Rámcové dohody uděluje podle zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění, souhlas objednateli, jako správci údajů, se zpracováním jeho osobních a dalších údajů v Rámcové dohodě a Realizační smlouvě uvedených pro účely naplnění práv a povinností vyplývajících z Rámcové dohody a Realizační smlouvy, a to po dobu jejich platnosti a dobu stanovenou pro archivaci příslušnými právními předpisy.

12.5. Poskytovatel uzavřením této Rámcové dohody výslovně souhlasí, aby tato Rámcová dohoda a jednotlivé Realizační smlouvy (včetně všech jejich změn a dodatků) byly zveřejněny v souladu s příslušnými právními předpisy, zejména v registru smluv postupem dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, v platném znění (dále jen „zákon o registru smluv“).

12.6. Smluvní strany jsou oprávněny postoupit jakoukoliv pohledávku nebo závazek vyplývající z Rámcové dohody a Realizační smlouvy pouze s předchozím písemným souhlasem druhé smluvní strany.

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

12.8. Rámcové dohoda a Realizační smlouva může být měněna či doplňována vzájemně odsouhlasenými a podepsanými písemnými a vzestupně očíslovanými dodatky, které se stávají její nedílnou součástí.

12.9. V případě, že nastane rozpor mezi Rámcovou dohodou a jejími přílohami, budou přednostně aplikována ustanovení Rámcové dohody.

12.10. Rámcová dohoda nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv postupem dle zákona o registru smluv.

12.11. Smluvní strany prohlašují, že si Rámcovou dohodu před jejím podpisem přečetly, že byla sepsána podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, že nebyla uzavřena za nápadně nevýhodných podmínek ani v tísni, na důkaz čehož připojují níže své podpisy.

Nedílnou součástí Rámcové dohody jsou 4 přílohy:

příloha č. 1 – Cenová kalkulace a specifikace služby
příloha č. 2 – Realizační smlouva
příloha č. 3 - Protokol o provedeném školení
příloha č. 4 – Prezenční listina
příloha č. 5 – Objednávka plnění

V_____dne_____ V_____dne_____

**Objednatel:**
[redacted]

**Poskytovatel:** Signature Not Verified
[redacted]

…….. ……

ředitel
podepsáno elektronicky

**General Counsel**
podepsáno elektronicky

**Agentura komunikačních a informačních systémů**
**Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk**

Příloha č. 1 k čj. MO 264723/2025-3255
Počet stran: 16

# Cenová kalkulace a specifikace služby – Kurzy SANS

**Prezenční forma**

| *Kurzy SANS* | *Cena v Kč bez DPH za 1 účastníka školení* | *Předpokládaný počet účastníků* | *Cena v Kč bez DPH za předpokládaný počet účastníků* | *Výše DPH v Kč 21% za předpokládaný počet účastníků* | *Cena v Kč s DPH předpokládaný počet účastníků* |
|---|---|---|---|---|---|
| Základy zabezpečení – síť, koncové body, cloud | | | | | |
| Otevřené zdroje (OSINT) | | | | | |
| Pokročilé zabezpečení | | | | | |
| Monitoring sítí a detekce hrozeb | | | | | |
| Zabezpečení Windows | | | | | |
| SIEM taktická analýza | | | | | |
| Penetrační testování | | | | | |
| Pokročilé penetrační testování | | | | | |
| Třídění, akvizice | | | | | |
| Forenzní analýza Windows | | | | | |
| Pokročilá reakce na incidenty, vyhledávání hrozeb | | | | | |
| Ransomware pro odpovídače incidentů | | | | | |
| Pokročilá síťová forenzní analýza – hledání hrozeb, analýza, reakce | | | | | |
| Kybernetické hrozby | | | | | |
| Hloubková forenzní analýza mobilního zařízení | | | | | |
| Malware reverzní inženýrství – pokročilá analýza kódu | | | | | |
| Základy vedení bezpečnosti pro manažery | | | | | |

| | |
|---|---|
| **Celková nabídková cena v Kč bez DPH** | |
| **Celková nabídková cena v Kč s DPH 21 %** | |

**On – line výuka**

| *Kurzy SANS* | *Cena v Kč bez DPH za 1 účastníka školení* | *Předpokládaný počet účastníků* | *Cena v Kč bez DPH za předpokládaný počet účastníků* | *Výše DPH v Kč 21% za předpokládaný počet účastníků* | *Cena v Kč s DPH předpokládaný počet účastníků* |
|---|---|---|---|---|---|
| Základy zabezpečení – síť, koncové body, cloud | | | | | |
| Otevřené zdroje (OSINT) | | | | | |
| Pokročilé zabezpečení | | | | | |
| Monitoring sítí a detekce hrozeb | | | | | |
| Zabezpečení Windows | | | | | |
| SIEM taktická analýza | | | | | |
| Penetrační testování | | | | | |
| Pokročilé penetrační testování | | | | | |
| Třídění, akvizice | | | | | |
| Forenzní analýza Windows | | | | | |
| Pokročilá reakce na incidenty, vyhledávání hrozeb | | | | | |
| Ransomware pro odpovídače incidentů | | | | | |
| Pokročilá síťová forenzní analýza – hledání hrozeb, analýza, reakce | | | | | |
| Kybernetické hrozby | | | | | |
| Hloubková forenzní analýza mobilního zařízení | | | | | |
| Malware reverzní inženýrství – pokročilá analýza kódu | | | | | |
| Základy vedení bezpečnosti pro manažery | | | | | |

| | |
|---|---|
| **Celková nabídková cena v Kč bez DPH** | |
| **Celková nabídková cena v Kč s DPH 21 %** | |

**Základy zabezpečení – síť, koncové body, cloud**

Minimální náplň školení v teoretické i praktické výuce:

- Vytvoření rámce základních znalostí v oblasti fungování počítačové a informační bezpečnosti. Tento rámec má sloužit k efektivnímu zabezpečení informačních systémů v organizaci.
- Praktická práce v bezpečnostního programu, který má sloužit k detekci, reakci a prevenci zabezpečení sítě v organizaci.
- Rozbor metodiky pro správu identit a přístupů (IAM), včetně aspektů silného ověřování (Multi-Factor Authentication).
- Představení a shrnutí silných, slabých stránek a rozdílů třech největších poskytovatelů cloudu na světě (Amazon, Microsoft a Google), včetně konceptů multi-cloudu a následného využití.
- Ukázka nástrojů Wireshark a tcpdump ke sledování síťové komunikace.
- Prakticky identifikovat viditelná slabá místa systému pomocí různých nástrojů a po objevení zranitelností nakonfigurovat systém tak, aby byl bezpečnější (realistická a praktická aplikace schopného programu pro správu zranitelností).
- Použití nástroje příkazového řádku Windows, Linux a macOS k analýze systému, který hledá vysoce rizikové indikátory kompromitace, a také koncepty základního skriptování pro automatizaci nepřetržitého monitorování.
- Vytvořit mapu viditelnosti sítě, kterou lze použít k ověření prostoru pro útok a určení nejlepší metodologie pro omezení prostoru pro útoky prostřednictvím posílení zabezpečení a správy konfigurace.
- Praktická výuka týkající se protokolů a analýzy paketů.
- Základy virtualizace a cloudu.
- Shrnutí informací týkajíc se zabezpečení bezdrátových sítí.
- Hloubková obrana při zabezpečení sítí.
- Praktická výuka při správném nastavování autentizace a zabezpečení hesel, ukázka všech možností.
- Praktická výuka a vysvětlení všech možností při správě identit a přístupů.
- Představení bezpečnostního rámce zahrnující informace o ovládacích prvcích Center for Internet Security (CIS) (vytvořené, aby pomohly organizacím upřednostnit nejkritičtější rizika, kterým čelí). Dále rámce kybernetické bezpečnosti NIST (standardy, pokyny a osvědčené postupy, které mohou pomoci při řízení celkového rizika kybernetické bezpečnosti); a znalostní báze MITRE ATT&CK (taktika a techniky protivníka).
- Prevence ztráty dat - metodika, která lze využít k implementaci vhodné funkce prevence ztráty dat.
- Zabezpečení mobilních zařízení.
- Správa zranitelností a reakce na ně zahrnující hodnocení zranitelnosti, útoky a škodlivý software, zabezpečení webových aplikací, bezpečnostní operace a správa protokolů, digitální forenzní analýza a reakce na incidenty.

- Shrnutí informací týkající se technologie zabezpečení dat – kryptografie, kryptografické algoritmy a nasazení, aplikace kryptografie, zařízení pro zabezpečení sítě, zabezpečení koncových bodů.
- Poskytnutí informačního rámce týkající se zabezpečení Windows a Azure - infrastruktury zabezpečení systému windows, windows jako služba, řízení přístupu k systému, vynucování bezpečnostní politiky, Microsoft Cloud Computing, Automatizace, protokolování a auditování,
- Praktická výuka v oblasti zabezpečení Linuxu, AWS a Macu - základy Linuxu, vylepšení zabezpečení Linuxu a infrastruktura.
- Min. 18 praktických laboratorních úloh

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU

Další požadavky na poskytovatele:

- poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky TCP IP, vstupy do virtuálních laboratoří);
- Osvědčení o absolvování kurzu

**Otevřené zdroje (OSINT)**

Minimální náplň školení v teoretické i praktické výuce:

- Provádění OSINT vyšetřování a zároveň procvičování operační bezpečnosti OPSEC.
- Správné techniky vyhledání informací na internetu, včetně některých obtížně dohledatelných a smazaných informací.
- Ukázka a praktické procvičení efektivního vyhledávání informací na dark webu.
- Výuka metod efektivního shromažďování a využívání dat ze sociálních sítí a médií.
- Teoretická i praktická výuka vedená k porozumění a správnému používání nástrojů pro rozpoznávání a porovnávání obličejů.
- Praktické procvičení metod pro rychlé a snadné třídění velkých datových sad s cílem zjistit co obsahují.
- Teoretická i praktická výuka vedená k rychlé identifikaci škodlivých nástrojů či dokumentů, jejichž cílem je prozradit vaši polohu.
- Praktická cvičení založených na skutečných scénářích jak pro státní sektor, tak soukromý. Účastník kurzu si dostatečně procvičí všechny vyučované techniky.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky OSINT a OPSEC, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Pokročilé zabezpečení**

Minimální náplň školení v teoretické i praktické výuce:

- Výuka zaměřená na oblast obrany síťové architektury, penetračního testování, bezpečnostních operací, digitální forenzní analýzy a reakce na incidenty a analýzy malware.
- Praktická výuka v oblasti bezpečného nastavení jednotlivých komponentů sítě.
- Praktické procvičení různých metod pro posouzení zranitelnosti a penetračního testování za účelem nalezení slabých míst v síti.
- Ukázka analytických metod pro detekci pokročilých útoků na síť a indikátorů kompromitace v různých systémech. Následné praktické procvičení účastníků kurzu.
- Školení efektivní a rychlé reakce na incident pomocí šestistupňového procesu reakce na incidenty.
- Teoretická i praktická výuka v oblasti analýzy malware, od plně automatizovaných technik až po manuální analýzu statických vlastností.
- Praktická výuka za použití reálných nástrojů (např. směrovače Cisco, Covenant, Metasploit, Nessus, Nmap, Procmon, Snort, SOF-ELK, TShark, Wireshark atd.) v každé z těchto oblastí je nutné demonstrovat (aktivní obranu, útoky proti síťovým zařízením, sbírka digitálních artefaktů, forenzní záchranu dat a interaktivní behaviorální analýzu malwaru.
- Praktická výuka v oblastech detekce, narušení a vytvoření podpisu Snort, agregace a korelace protokolů, ručního obrácení kódu, síťové forenzní analýzy, prohledávání sítě, analýzy paketů a protokolů, prolomení hesla, analýzy časové osy, systémové exploatace a post-expolitační pivoting, posouzení ohrožení zabezpečení, skenování a útoků na webové aplikace.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky síťová architektura a penetrační testování, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Monitoring sítí a detekce hrozeb**

Minimální náplň školení v teoretické i praktické výuce:

- Technické znalosti v oblasti hloubkového monitoringu sítě a detekci hrozeb.
- Praktické školení v oblasti spolehlivé obrany tradiční i cloudové sítě.
- Podrobné seznámení s teorií protokolů TCP/IP a nejpoužívanějšími aplikačními protokoly (DNS a http).
- Praktické procvičení monitoringu síťového provozu a identifikace hrozeb.
- Praktická ukázka a procvičení metod proaktivního vyhledávání hrozeb v síti.
- Teoretická výuka a praktické procvičení v oblasti rekonstrukce síťového útoku.
- Shrnutí a porovnání výhod a nevýhod spojených s používáním různých nástrojů pro monitorování sítě.
- Vytvoření rámce možností detekce hrozeb nultého dne.
- Praktické provádění síťové forenzní analýzy za účelem identifikace TTP a nalezení aktivních hrozeb.
- Praktické cvičení zaměřené na zvládání různých nástrojů, včetně tcpdump, Wireshark, Snort, Suricata, Zeek, tshark, SiLK a NetFlow/IPFIX.
- Praktické procvičení ve virtuální laboratoři.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky TCP/IP, DNS, http, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu

**Zabezpečení Windows**

Minimální náplň školení v teoretické i praktické výuce:

- Teoretická i praktická výuka v oblasti zabezpečení Windows za použití bezpečnostního skriptování v PowerShellu.
- Vysvětlení metody psaní skriptů a jejich bezpečného spouštění v PowerShellu pro automatizaci zabezpečení Windows a Active Directory v síti.
- Procvičení metod ochrany v síti před malwarem typu ransomware.

- Praktická výuka v možnostech zabezpečení Windows Serveru a Windows 10/11 proti zkušeným útočníkům.
- Teoretická i praktická výuka v oblastech vzdáleného spuštění příkazu PowerShellu, PowerShell Core s OpenSSH, PowerShell Enough Správce (JEA), Skripty PowerShellu pro nahrazení Microsoft LAPS, ověřování certifikátů PowerShellu, například pomocí YubiKeys, posílení zabezpečení protokolů TLS, RDP a SMB v PowerShellu.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky zabezpečení Windows a Active Directory, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**SIEM taktická analýza**

Minimální náplň školení v teoretické i praktické výuce:

- Teoretická i praktická výuka v oblasti školení metod a procesů pro vylepšení stávajících řešení protokolování.
- Podrobný popis a vysvětlení všeho, co obsahují protokoly.
- Trénink praktických zkušeností ve virtuálních laboratořích k podrobnému prozkoumání SOF-ELK a SIEM k analýze dat ve velkém měřítku.
- Praktické vyzkoušení opensourcového zásobníku Elasticsearch, Logstash a Kibana (ELK) spolu s dalšími opensourcovými projekty, které poskytují architekturu a proces SIEM (Security Information and Event Management).
- Shrnutí metod, jak ukládat a zpracovávat velké množství dat.
- Praktická výuka aktivní aplikace technik nepřetržitého monitorování a analýzy za využití moderních útoků na kybernetické hrozby. Testovací prostředí by mělo zahrnovat přehrání zachycených dat o útocích, tak aby bylo možné poskytnout výsledky a vizualizace z reálného světa.
- Praktické procvičení integrace a psaní vlastních skriptů pro SIEM.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky SIEM, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu

**Penetrační testování**

Minimální náplň školení v teoretické i praktické výuce:

- Výuka zaměřená na komplexním pokrytím nástrojů, technik a metod pro síťové, webové a jiné aplikace v souvislosti s penetračním testováním.
- Teoretická i praktická výuka zaměřená na plánování penetračních testů, stanovení rozsahu, průzkum a skenování s vysokým hodnotovým výstupem.
- Teoretická výuka zaměřená na komplexní náhled na penetrační testování a know-how v oblasti etického hackingu.
- Praktická výuka zaměřená na provádění podrobného průzkumu, zjištění informací o cíli a infrastruktuře pomocí blogů, vyhledávačů, sociálních sítí a dalších internetových stránek.
- Vyzkoušení nejlepších nástrojů ke skenování sítí. Podrobný rozbor výstupů ze skenů.
- Shrnutí nejlepších sad nástrojů pro penetrační testování, které jsou dnes k dispozici a různých metod k jejich využití.
- Hloubková analýza post-exploatace a útoků na hesla.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky penetrační testování, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Pokročilé penetrační testování**

Minimální náplň školení v teoretické i praktické výuce:
Teoretická a praktická výuka zaměřená na dovednosti a znalosti v oblasti reverzního inženýrství aplikací za účelem zjištění zranitelností.
Znalost v oblasti zabezpečení aplikací, analýzy záplat pro jednodenní exploity, provádění pokročilého fuzzingu a psaní exploitů.

Praktická výuka v oblasti psaní komplexních exploitů proti operačním systémům Windows a Linux.
Praktická výuka v oblasti efektivního využití různých debuggery a plug-inů ke zlepšení průzkumu zranitelností.
Metody odhalení zranitelnosti nultého dne v programech běžících na moderních operačních systémech s plnými opravami.
Využití pokročilé funkce IDA Pro a psaní vlastních skriptů IDAPython.
Využití aplikace Fuzz s uzavřeným zdrojovým kódem.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky penetrační testování, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Třídění, akvizice**

Minimální náplň školení v teoretické i praktické výuce:

- Teoretická i praktická výuka digitální forenzní akvizice.
- Identifikace různých médií pro ukládání dat.
- Shromažďování dat a uchovávání forenzně správným způsobem tyto data bez ohledu na to, jak a kde mohou být uložena.
- Digitální akvizici z počítačů, přenosných zařízení, sítí a cloudu.
- Efektivní získávání dat z PC, Microsoft Surface a tabletů, Zařízení Apple, Mac a Macbook, paměti RAM (Random Access Memory), smartphonů a přenosných mobilních zařízení, cloudových úložišť a služeb, síťových úložišť, prostředí virtuálních počítačů.
- Rychlé třídění, identifikaci dat a získávat užitečné informace z pevného disku za max 90 minut nebo méně.
- Správně shromažďovat data z úložišť SharePointu.
- Identifikace a shromáždění velkého počtu uživatelských dat, kde se k nim přistupuje pomocí protokolu SMB.
- Správně shromažďovat e-maily ze serverů Exchange.
- Principy pokročilých kontejnerů úložiště, jako jsou RAID a JBOD.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky forenzní analýzy, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Forenzní analýza Windows**

Minimální náplň školení v teoretické i praktické výuce:

- Provádění hloubkové forenzní analýzy operačních systémů Windows a zneužití médií v produktech Windows XP, Windows 7, Windows 8/8.1, Windows 10, Windows 11 a Windows Server.
- Identifikování umístění artefaktů a důkazů pro zodpovězení základních otázek forenzní analýzy, včetně spouštění aplikací, přístupu k souborům, krádeže dat, využití externích zařízení, cloudových služeb, geografické polohy zařízení, přenosů souborů, antiforenzní analýzy a podrobné aktivity systému a uživatelů.
- Extrahování kritických zjištění a vytvoření si interní forenzní kapacity prostřednictvím různých bezplatných, opensourcových a komerčních nástrojů.
- Praktické cvičení v oblasti vytěžení databázi Windows Search, metadat souborů, obsahu souborů z místních disků, vyměnitelných médií a aplikací, jako je Microsoft Outlook, OneNote, SharePoint a OneDrive.
- Práce s databází Parse Electron Application umožňující zkoumání stovek aplikací třetích stran včetně většiny chatovacích klientů.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky TCP IP, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Pokročilá reakce na incidenty, vyhledávání hrozeb**

Minimální náplň školení v teoretické i praktické výuce:

- Podrobný rozbor postupu pro efektivní vyhledávání hrozeb a reakcí na incidenty.
- Postupy pro identifikaci napadených informačních systémů.

- Teoretická i praktická výuka metod a možností, jak správně sledovat protivníky a shromažďovat informace o hrozbách tak, aby se včas provedly kroky k zabezpečení IS.
- Vybudování pokročilých dovedností v oblasti forenzní analýzy pro boj s antiforenzními metodami.
- Ukázka a praktická výuka k používání nástrojů pro analýzu paměti, reakce na incidenty a proaktivní vyhledávání hrozeb v pracovní stanici SIFT čímž je možnost detekovat skryté procesy, malware, příkazové řádky útočníka, rootkity, síťová připojení a další.

Forma kurzu:
- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:
- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, vstupy do virtuálních laboratoří;
- osvědčení o absolvování kurzu.

**Ransomware pro odpovídače incidentů**

Minimální náplň školení v teoretické i praktické výuce:
- Teroretická a praktická výuka v oblasti správných postupů při specifik při útoku typu ransomware, od počáteční detekce až po reakci na incident a analýzu.
- Výuka metod, jak nejlépe připravit informační síť a uživatele na tuto hrozbu.
- Identifikace nástrojů, které útočníci používají k tomu, aby se během útoku ranwomware dostali do prostředí organizace.
- Teoretická i praktická výuka v oblasti správné reakce na prostředí, v němž reálně běží ramsomware.
- Praktické cvičení s daty z reálného světa, která vycvičí studenty, jak se připravit na ranwomware, odhalit jej, lovit, reagovat na něj a vypořádat se s ním.
- Jaké by měly být kroky po útoku ransomware.
- Rozbor forenzních artefaktů systému Windows důležitých pro reakci na ransomwarové incidenty (Shellbagy, Shimcache, atd.).
- Přijímání analyzovaných dat do systému SIEM a jejich následné zpracování.

Forma kurzu:
- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, vstupy
  do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Pokročilá síťová forenzní analýza – hledání hrozeb, analýza, reakce**

Minimální náplň školení v teoretické i praktické výuce:

- Teoretická i praktická výuka v oblasti správné reakce na incident při krádeži dat v organizaci.
- Praktické procvičení proaktivního odhalování protivníka při monitoringu sítě.
- Výuka pokročilých technik za využití různých nástrojů, technologií a procesů potřebných k integraci zdrojů a síťových důkazů pro vyšetřování.
- Rychlé zjištění důkazů a efektivní práci při analýze.
- Praktická výuka v oblasti použití různých technik k extrahování souborů ze zachycených síťových paketů a souborů proxy cache, což umožňuje následnou analýzu malwaru nebo definitivní určení ztráty dat.
- Výuka technik správného použití historických dat NetFlow k identifikaci relevantních síťových událostí v minulosti, což umožňuje přesné stanovení rozsahu incidentu.
- Zpětně analyzuje vlastní síťové protokoly a identifikuje schopnosti a akce útočníka v oblasti příkazů a řízení.
- Podrobný rozbor technik pro dešifrování zachyceného provozu SSL/TLS a identifikování akcí útočníků a dat, která od oběti získali.
- Využití dat z typických síťových protokolů ke zvýšení kvality výsledků vyšetřování.
- Identifikování možnosti shromažďování dalších důkazů na základě stávajících systémů a platforem v rámci síťové architektury.
- Praktické sledování provozu pomocí běžných síťových protokolů, k identifikaci vzorce činnosti, které vyžadují další vyšetřování.
- Praktická výuka způsobů, jak nejlépe odhalit útočníka, který použil nástroje typu meddler-in-the-middle k zachycení zdánlivě bezpečné komunikace.
- Analýza síťového protokolu (protokol HTTP (Hypertext Transfer Protocol), služba DNS (Domain Name Service), protokol FTP (File Transfer Protocol), protokol SMB (Server Message Block) a související protokoly společnosti Microsoft, protokol SMTP (Simple Mail Transfer Protocol).

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, vstupy do virtuálních laboratoří;
- osvědčení o absolvování kurzu.

**Kybernetické hrozby**

Minimální náplň školení v teoretické i praktické výuce:

- Teoretická i praktická výuka zaměřená na strukturovanou analýzu s cílem vytvoření pevného základu pro řešení sofistikovanější pokročilé hrozby.
- Rozvíjet analytické dovednosti za využití složitých praktických scénářů k řešení.
- Identifikovat a vytvářet požadavky na zpravodajské informace prostřednictvím postupů, jako je modelování hrozeb.
- Pochopit a rozvíjet dovednosti v oblasti sběru informací o hrozbách na taktické, operační a strategické úrovni.
- Naučit se různé zdroje pro shromažďování údajů o protivníkovi a způsoby, jak tyto údaje využívat proti samotnému útočníkovi.
- Praktická výuka vedoucí ke správnému získávání a ověřování informací z venčí a tím minimalizovat špatné zpravodajské informace.
- Praktická výuka vedoucí k vytváření indikátorů kompromitace (IOC) ve formátech jako jsou YARA a STIX/TAXII.
- Podrobně rozebírá různé taktiky, techniky a postupy protivníka za využití Kill Chain, Diamond Model a MITRE ATT&CK.

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, příručky TCP IP, vstupy do virtuálních laboratoří;
- osvědčení o absolvování kurzu.

**Hloubková forenzní analýza mobilního zařízení**

Minimální náplň školení v teoretické i praktické výuce:

- Teoretická i praktická výuka v oblasti přípravy specialistů na práci s nejúčinnějšími forenzními nástroji, technikami a postupy pro efektivní analýzu dat ze smartphonu.

- Výuka metod k provedení rekonstrukce události pomocí informací z chytrých telefonů, včetně vypracování časové osy a analýzy souvislostí (např. kdo, kde a kdy s kým komunikoval).
- Podrobně rozebírá způsoby uložení dat souborových systémů chytrých telefonů, jak se liší a jak budou důkazy uloženy v jednotlivých zařízeních.
- Interpretovat souborové systémy v chytrých telefonech a vyhledávat informace, které nejsou uživatelům běžně přístupné
- Určit, jak se důkazy dostaly do mobilního zařízení. Odhalit, zda data vytvořil uživatel, nebo tam byly vloženy jinak.
- Začlenění technik ručního dekódování pro obnovu nerozluštěných dat uložených v chytrých telefonech.
- Odhalit konkrétního uživatele s chytrým telefonem v určitý den/čas a na různých místech.
- Obnovit skrytou nebo zastřenou komunikaci z aplikací v chytrých telefonech.
- Dešifrovat nebo dekódovat data aplikací, která nejsou analyzovatelná běžnými forenzními nástroji.
- Odhalit smartphony napadené malwarem a spywarem pomocí forenzních metod.
- Dekompilovat a analyzovat mobilní malware pomocí nástrojů s otevřeným zdrojovým kódem.
- Zvládnout šifrování v chytrých telefonech a prolomit záložní soubory iOS, které byly zašifrovány pomocí iTunes.
- Extrahovat a používat informace ze smartphonů a jejich součástí ze systémů Android, iOS a karet SD.

Forma kurzu:
- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:
- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Malware reverzní inženýrství – pokročilá analýza kódu**

Minimální náplň školení v teoretické i praktické výuce:
- Šifrování souborů a ochrana klíčů. Připravuje specialisty na analýzu malware a podrobný rozbor kódu sofistikovaných spustitelných souborů Windows.
- Teoretická i praktická výuka v oblasti použití
- nejlepší techniky jak se vypořádat se scénáři reverzního inženýrství v reálném světě.
- Řešení techniky obfuskace kódu, které brání statické analýze kódu, včetně použití steganografie.
- Praktická výuka v oblasti identifikace klíčové součásti provádění programu pro analýzu vícestupňového malwaru v paměti.

- Rozebírá možnosti efektivního vyhledávání a extrahování deobfuskovaného shellcode.
- Praktická výuka v oblasti prozkoumání struktury a pole související s hlavičkou PE.
- Řeší techniku použití WinDBG Preview pro ladění a posuzování klíčových datových struktur procesu v paměti.
- Identifikuje šifrovací algoritmy v ransomwaru používané.
- Rozpoznává rozhraní API systému Windows, která usnadňují šifrování, a vyjádření jejich účelu.
- Rozebírá možnosti obfuskace dat v malwaru, následnou implementaci algoritmů a dekódování obsahu.
- Vytváření skriptů v jazyce Python pro automatizaci extrakce a dešifrování dat.
- Vytváření pravidla pro identifikaci funkcí v malwaru.
- Používat frameworky DBI (Dynamic Binary Instrumentation) k automatizaci běžných pracovních postupů reverzního inženýrství.
- Psát skripty v jazyce Python v rámci aplikace Ghidra pro urychlení analýzy kódu.
- Používat rámce pro binární emulaci k simulaci provádění kódu.

Forma kurzu:
- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:
- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Základy vedení bezpečnosti pro manažery**

Minimální náplň školení v teoretické i praktické výuce:
- Výuka zaměřená na lídry v oblasti bezpečnosti. Cílem je aby lídr pochopil, co techničtí pracovníci skutečně dělají tak, aby mohli efektivně plánovat a řídili bezpečnostní projekty.
- Rychlé pochopení kritických problémů a terminologie v kybernetické bezpečnosti se zaměřením na bezpečnostní rámce, architekturu zabezpečení, bezpečnostní inženýrství, zabezpečení počítačů/sítí, správu zranitelností, kryptografii, ochranu dat, povědomí o bezpečnosti, zabezpečení aplikací, DevSecOps, cloudové zabezpečení a bezpečnostní operace.
- Řídit a vést technické týmy a projekty.
- Vytvořit program správy zranitelností
- Vložení zabezpečení do moderních pracovních postupů DevOps
- Strategicky využívat systém SIEM

- Vést bezpečnostní operační centrum (SOC)
- Vybudovat schopnosti bezpečnostního inženýrství s využitím automatizace a infrastruktury jako kódu (IaC).

Forma kurzu:

- prezenční/on-line, pořádaná na území států NATO nebo EU.

Další požadavky na poskytovatele:

- Poskytnutí výukových a studijních materiálů v elektronické podobě z důvodu kontroly ze strany zadavatele (zvukové soubory MP3, vstupy do virtuálních laboratoří);
- osvědčení o absolvování kurzu.

**Agentura komunikačních a informačních systémů**
**Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk**

Příloha č. 2 k čj. MO 264723/2025-3255
Počet stran: 3

# Realizační smlouva
# č. (BUDE DOPLNĚNO)

dle Rámcové dohody č. **25106000291** pro **„Kurzy SANS“** uzavřené v elektronickém nástroji NEN pod systémovým číslem N006/24/V00029855.

## I. Smluvní strany

**Česká republika – Ministerstvo obrany**
Se sídlem: Tychonova 221/1, 160 00 Praha 6 - Hradčany
IČ: 6016269
DIČ: CZ60162694
[redacted]
(dále jen „**objednatel**“)

a

The Escal Institute of Advanced Technologies, Inc.
Sídlo: 11200 Rockville Pike, Suite 200, 20852, Maryland, Spojené státy americké
IČ: 252 67 77
DIČ: CZ681636906
[redacted]

[redacted]

(dále jen „**poskytovatel**“)
(objednatel a poskytovatel dále společně také „**smluvní strany**“ jednotlivě „**smluvní strana**“)

Smluvní strany uzavírají na základě Rámcové dohody č. **25106000291** (dále jen „**Rámcová dohoda**“) tuto Realizační smlouvu (dále také jen „**smlouva**“).

## II. Předmět smlouvy

2.1. Předmětem smlouvy je poskytnutí služby, a to **školení XXXX (bude doplněn název školení) (dále jen „školení“) dle přílohy č. 1 Rámcové dohody.**

## III. Doba a místo plnění

3.1. Poskytovatel se zavazuje službu poskytnout v termínu **XXXX (bude doplněno objednatelem)** pro **XXXX (bude doplněno objednatelem)** účastníků.

3.2. Místo plnění služby: **XXXX (BUDE DOPLNĚNO: prostory/zařízení/školící centrum + celá adresa)** / on-line výuka na adrese poskytovatele **XXXX (BUDE DOPLNĚN** internetový odkaz před uzavřením Realizační smlouvy**)**.

## IV. Cena

4.1. Celková cena za službu je **XXXX Kč bez DPH a ve výši XXXX Kč s DPH (slovy XXXX korun českých)** (dále také „**cena**“). Cena představuje maximální cenu za službu. Smluvní strany nejsou zavázány k vyčerpání maximální ceny za službu v případě sníženého počtu účastníků školení.

4.2. V ceně jsou zahrnuty veškeré náklady poskytovatele související s plněním této smlouvy (např. DPH, zajištění prostor pro školení, materiály, clo apod.).

4.3. Detailní kalkulace ceny je stanovena v příloze č. 1 Rámcové dohody.

4.4. Cenu je možné zvýšit pouze z důvodů zvýšení DPH, a to na základě písemného dodatku ve smyslu čl. XII. odst. 12.8. Rámcové dohody.

## V. Závěrečná ustanovení

5.1. Podmínky plnění, platební a fakturační podmínky, odpovědnost za škodu, smluvní pokuty a další podmínky smluvního vztahu se řídí příslušnými ustanoveními Rámcové dohody, pokud není v této smlouvě uvedeno jinak.

5.2. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami V případě splnění podmínek stanovených zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, v platném znění, nabývá tato smlouva účinnosti uveřejněním v registru smluv.

5.3. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla sepsána podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, že nebyla uzavřena za nápadně nevýhodných podmínek ani v tísni, na důkaz čehož připojují níže své podpisy.

V_____dne_____ V_____dne_____

**Objednatel:**
pl[redacted]

**Poskytovatel:**
M[redacted]

…….
ředitel
podepsáno elektronicky

……
**General Counsel**
podepsáno elektronicky

**Agentura komunikačních a informačních systémů**
**Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk**

Příloha č. 3 k čj. MO 264723/2025-3255
Počet stran: 1

# PROTOKOL O PROVEDENÉM ŠKOLENÍ
## na základě Realizační smlouvy č. XXXXXXX
dle Rámcové dohody č. 25106000291 pro **„Kurzy SANS“**

Na základě Realizační smlouvy č. **XXXXXX** na provedení školení provedla společnost [redacted], školení na téma

……..
*(přesný název školení)*

Školení bylo provedeno na základě požadavku smlouvy dle odsouhlaseného harmonogramu v termínu **od** ***dd.mm.rrrr*** **do** ***dd.mm.rrrr*** v délce ***XX*** pracovních dnů pro *VÚ XXXX* pro ***XX*** účastníků.

Prezenční listina s uvedením jmenného seznamu a podpisy účastníků školení je uvedena na samostatném listě a je součástí tohoto zápisu.

Školení proběhlo v souladu s ustanovením Realizační smlouvy č. **XXXXX,** bylo provedené řádně a v dohodnutém termínu.

V *místě plnění* dne *dd.mm.rrrr*

| Pověřený zástupce objednatele | Pověřený zástupce poskytovatele |
|---|---|
| jméno | jméno |
| podpis | podpis |

Rozdělovník:
Výtisk č. 1 – objednatel
Výtisk č. 2 – poskytovatel

**Agentura komunikačních a informačních systémů**
**Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk**

Příloha č. 4 k čj. MO 264723/2025-3255
Počet stran: 1

# PREZENČNÍ LISTINA
## „Školení v působnosti komunikačních a informačních systémů“
## kurzy SANS na rok 2025

konané dne: ddmmrrrr 2025

| P. č. | Hodnost, jméno příjmení | Útvar (složka) | Telefon | Podpis |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |

**Agentura komunikačních a informačních systémů**
Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

Příloha č. 5 k čj. MO 264723/2025-3255
Počet stran: 1

# OBJEDNÁVKA K PLNĚNÍ č. XX
## na školení podle čl. VII. Rámcové dohody č. 25106000291

| | | | |
|---|---|---|---|
| **1. Specifikace dílčího plnění:** | **Kurzy SANS**<br>**Bude doplněn název školení** | | |
| 2. Jmenný seznam účastníků školení: | *Poř. číslo*<br>1<br>2<br>3<br>4<br>5<br>6<br>7<br>8<br>9<br>10<br>11<br>12<br>13<br>14<br>15<br>16<br>17<br>18<br>19<br>20 | *Hodnost, titul, jméno, příjmení* | *Kontaktní údaje* |
| 3. Požadavek na certifikáty o absolvování školení pro účastníky školení: | *Dále poskytovatel zabezpečí vystavení certifikátu o absolvování školení pro účastníky, kteří absolvovali minimálně 80% školení. Tento certifikát předá účastníkům v poslední den školení.* | | |
| 4. Místo plnění: | | | |
| 5. Termín zahájení dílčího plnění: | *čas / den / měsíc / rok* | | |
| | | | |
| 6. Termín ukončení dílčího plnění: | *čas / den / měsíc / rok* | | |
| | | | |
| 7. Za objednatele: | *hodnost, jméno, příjmení*<br>*datum a podpis* | *telefonické a faxové spojení* | |
| Zástupce objednatele | | | |



Elektronicky podepsal [redacted]