Obsah

[Technické požiadavky 1](#_Toc93999024)

[Flexibilita, škálovateľnosť a prispôsobiteľnosť 1](#_Toc93999025)

[Dostupné bezpečnostné nástroje 2](#_Toc93999031)

[Hodnotenie tréningov 2](#_Toc93999033)

[Nefunkčné požiadavky 2](#_Toc93999036)

[PodporaSupport 3](#_Toc93999045)

[Scenáre 4](#_Toc93999048)

[Tréning a školenie 5](#_Toc93999056)

[Virtuálna infraštruktúra ministerstva 5](#_Toc93999059)

[Priestory 6](#_Toc93999061)

[Softskills scenáre a platforma 6](#_Toc93999064)

[Projektový manažment 7](#_Toc93999068)

[Popis navrhovaného riešenia 8](#_Toc93999070)

[TECHNOLOGICKÁ VRSTVA 10](#_Toc93999071)

[Kritérium na vyhodnotenie ponúk 10](#_Toc93999072)

# Opisu predmetu zákazky „Vybudovanie Výcvikového a školiaceho strediska pre bezpečnosť prevádzky a správy IT pre sektor VS“

Výcvikové a Modul kybernetickej arény školiaceho a výcvikového stredisko by malo zabezpečiť prepojenie teoretických znalostí v oblasti bezpečnosti s praktickými skúsenosťami (reálne reakcie na incidenty). V tejto súvislosti je potrebné dodať riešenie, ktoré splní nižšie uvedené požiadavky.

# Technické požiadavky

## Flexibilita, škálovateľnosť a prispôsobiteľnosť

### RQ001

Za účelom kvalitného tréningu musí byť prostredie jednoducho „customizovateľné“, aby bolo možné nasimulovať rôzne druhy IKT infraštruktúry a architektúry, resp. rôzne typy IT prostredí druhy organizácií VS.

Spôsob hodnotenia (ak verejný obstarávateľ uplatní okrem ceny kritérium kvality dodania predmetu zákazky): Vyšší počet bodov bude pridelený riešeniu, ktoré bude:

* mať customizovateľných viac parametrov,
* nastavenie konfigurácie bude možné cez grafické rozhranie.

### RQ002

Riešenie musí poskytovať rôzne druhy šablón IT architektúry, vrátane sieťovej architektúry. Tieto šablóny musia byť jednoducho modifikovateľné a „nasaditeľné“ – napr. prostredníctvom virtualizácie a programovania infraštruktúry. Šablóny budú obsahovať minimálne: domain controller servery, aplikačné servery, databázové servery, routre, load balancery, DMZ, IPS, ako aj simulovaný internetový segment.

Spôsob hodnotenia (ak verejný obstarávateľ uplatní okrem ceny kritérium kvality dodania predmetu zákazky): Vyšší počet bodov bude pridelený riešeniu, ktoré bude:

* mať viac šablón,
* mať vyriešené jednoduché nasadzovanie týchto šablón,
* ktorého šablóny budú obsahovať väčšie množstvo rôznych prvkov.

### RQ003

Infraštruktúra musí byť exportovateľná a následne importovateľná medzi rôznymi prostrediami a za účelom zálohy a jej obnovy.

Spôsob hodnotenia (ak verejný obstarávateľ uplatní okrem ceny kritérium kvality dodania predmetu zákazky): ak bude požiadavka splnená, bude pridelený jeden bod.

### RQ004

Riešenie bude schopné simulovať sieťovú prevádzku medzi všetkými prvkami z RQ002. Simulácia zahŕňa bežnú prevádzku ako aj škodlivú prevádzku založenú na aktuálnych hrozbách (aktualizovanú z open source zdrojov).

Výsledkom bude simulácia aktéra s komplexnou sieťovou infraštruktúrou a 3 agendovými systémami, registratúrou, a ďalšou bežnou SW výbavou (predovšetkým na báze Microsoft, t.j. AD, Exchange, atď.), pričom jeden z agendových systémov bude mať integráciu na testovacie prostredie UPVS a jedného iného ISVS (napr. verejne dostupné služby niektorého z registrov).

Prostredie na simuláciu organizácie VS – ministerstva bude obsahovať:

* Sieťová tréningová platforma (Routers, LAN switches , atď.etc).
* Wifi technológie (rôzne zariadenia – napr. Cisco, Ubiquiti, Mikrotik, Turris a pod.... ), časť simulovanej prevádzky pôjde aj cez wifi.,
* Bezpečnostné produkty typu FW, IDS/IPS senzory, WAF a pod. -napr. Checkpoint, Palo Alto, Fortinet, F5, Snort/Suricata.,
* Servery a virtualizácie – aspoň dve z technológií VMware, XEN, KVM, MS HyperV.
* Kontajnerové technológie, napr. Kubernetes.
* Server OS - Windows Server (rôzne verzie), OS Linux (rôzne verzie, rôzne server distribúcie).
* Mail (rôzne aj aplikácie, Windows, Mac aj Linux SW, povinne vrátane MS Exchange).
* DB (rôzne free databázy - SQL, NoSQL ESK, Hadoop).
* Rôzny software (DNS/DNSSEC servery, AV - ESET, Trend Micro a pod..,
* Desktopy/NB (Windows rôzne verzie, Linux – rôzne distribúcie a Apple Mac OS X).
* Mobilné platformy (rôzne Android a iIOS zariadenia).
* IOT zariadenia – najmä kamery, led žiarovky, senzory.,
* HSM zariadenia, dvojfaktorová autentifikácia.,

Spôsob hodnotenia (ak verejný obstarávateľ uplatní okrem ceny kritérium kvality dodania predmetu zákazky): Vyšší počet bodov bude pridelený riešeniu, ktoré bude:

* mať vyšší počet a rôznorodosť simulovaných prvkov,
* bude mať simulovaný agendový systém,
* bude mať integráciu na testovacieho/vývojového prostredie reálneho ISVS,
* ktoré bude vernejšie simulovať reálnu organizáciu.

### RQ005

Riešenie musí byť škálovateľné a postavené na ne-proprietárnej architektúre, čo umožní integráciu rôznych COTS riešení/softvérov (vrátane riešenia na „customizáciu“ scenárov).

## Dostupné bezpečnostné nástroje

### RQ006

Riešenie umožní použitie rôznych bezpečnostných COTS produktov, vrátane vedúcich SIEM riešení, sandboxových technológií, analyzačných nástrojov atď.. Príkladom sú Qradar, Arcight, Splunk, Logstash, Logmanager, atď..

## Hodnotenie tréningov

### RQ007

Riešenie umožní účastníkom školenia zobraziť priebežné automatické hodnotenie na základe plnenia určených cieľov. Riešenie musí na konci cvičenia poskytnúť hodnotiacu správu, a to pre účastníkov aj pre dohľad.

### RQ008

Riešenie musí pracovníkovi dohľadu umožniť dohľad nad každou individuálnou session účastníka školenia, vrátane kontroly a usmernenia. Riešenie umožní aj spracovanie a zobrazeniepríjem priebežného hodnotenia.

Platforma musí podporovať viacero typov monitoringu, najmä:

* monitoring priebehu cvičenia a dosahovaných cieľov, ako ich definuje scenár a jeho komponenty,
* detailný monitoring naprieč všetkými cvičeniami,
* technický monitoring priebehu cvičenia a aktivity hráčov formami,
* session recorder, ktorý umožní spätne prehrávať a analyzovať akcie hráčov a ich reakcie na scenár za účelom vzdelávania počas záverečnej fázy cvičenia alebo ako ukážkový materiál pri ďalších cvičeniach.

## Nefunkčné požiadavky

### RQ009

Riešenie umožní pripojenie sa do tréningu aj vzdialeným používateľom (jednotlivcom alebo celému tímu).

### RQ010

Riešenie bude jednoducho použiteľné (user friendly) pre používateľov aj dohľad a zároveň jednoducho spravovateľné administrátorom.

### RQ011

Produkt bude podporovať cvičenie pre 50 konkurentných používateľov a dokáže nasimulovať prostredie s cca 300 používateľmi (pozri aj RQ004).

### RQ012

Riešenie umožní čo najväčšiu automatizáciu administrátorských a dohľadových rolí s cieľom maximalizovať produktivitu a minimalizovať ľudské chyby.

### RQ013

Celé prostredie bude v ľubovoľnom čase podporovať uloženie a spätnú obnovu tréningu. Taktiež umožní resetnúť prostredie do počiatočného východzieho nastavenia (pripravené na nové cvičenie).

Riešenie umožní nastaviť a spustiť cvičenie založené na existujúcom scenári v krátkom čase (maximálne 60 minút).

### RQ014

Riešenie bude založené primárne na open source licenciách. Prípadné komerčné licencie budú zvolené tak, aby minimalizovali každoročné prevádzkové náklady.

V popise tejto požiadavky je potrebné vypísať zoznam softvéru, na ktorom je platforma založená, pričom pri každom bude uvedený aj ročný náklad na prípadné licencie.

Nižšia prevádzkové náklady na licencie budú znamenať vyššie hodnotenie.

### RQ015

Bude možné spustiť 3 paralelné tréningy, každé s vlastným prostredím, kde budú trénovať nezávislí používatelia.

### RQ016

Riešenie je obstarávané ako kompletné krabicové riešenie a by malo byť z fyzického pohľadu by malo byť čo najmenšie. Výhodou bude jednoduchý transport serverovej infraštruktúry na iné miesto.

Riešenie môže obsahovať napríklad prenosný rack polovičnej veľkosti (12u), alebo aj zariadenie na transport do 15 notebookov s príslušenstvom.

Môžu byť ponúknuté aj iné riešenia, pričom menší fyzický rozsah dodávaného riešenia bude ohodnotený vyšším počtom bodov.

## Podpora a support

### RQ017

Ponuka na riešenie bude zahŕňať:

podporu riešenia na 2 roky, pričom podpora zahŕňa minimálne:

* vzdialenú podporu počas pracovných dní (od 9:00 do 17:00), pričom bude dostupná buď telefonická podpora, alebo ticketovací nástroj s ľudskou odpoveďou do 2 hodín,
* podpora onsite do 2 pracovných dní,
* pravidelná profilaktika raz s výstupnou správou min. raz 2x ročne,
* manažment licencií, t.j. sledovanie exspirácie licencií a maintenance a v spolupráci s verejným obstarávateľom aj upgrade,
* reinštaláciu systému v prípade potreby,
* upgrade na nové verzie softvéru raz ročne,
* záručnú opravu/výmenu hardvéru.

### RQ018

Riešenie by malo byť prevádzkovateľné internými zamestnancami obstarávateľa bez závislosti na externom dodávateľovi. Všetok softvér a hardvér musí byť všeobecne dostupný na trhu, aby si ho mohol obstarávateľ aj nezávisle zakúpiť (napríklad nie iba výhradné licencie iba cez dodávateľa atď.).

## Scenáre

### RQ020

Riešenie bude obsahovať katalóg predpripravených tréningových scenárov s rôznymi úrovňami zložitosti (aspoň základná, stredná a zložitá), pričom scenáre budú obsahovať viac- stupňové útoky.

Každý scenár bude obsahovať:

pPopis úlohy (pre každú úroveň zložitosti), predpokladanú, resp. potrebnú aktivitu zo strany účastníka, odhad trvania, ciele, popis vetiev/alternatív scenára podľa akcií účastníka cvičenia,

* hodnotiace kritéria,
* teoretická časť pre účastníka (schémy, diagramy, prezentácia, alebo text),
* konfiguračné súbory, pomocné súbory potrebné pre spustenie cvičenia na riešení.

Vyšší počet bodov bude udelený návrhu, ktorý bude obsahovať viac scenárov, resp inovatívne/rozšírené možnosti, ako napríklad: scenár s možnosťami, resp. rôznymi alternatívami podľa reakcií účastníka, možnosti pre dohľad ako účastníkovi pomôcť, tipy pre účastníkov (zobrazené napr. po uplynutí určitého času pri riešení úlohy daného scenára).

### RQ021

Riešenie bude obsahovať komplexnú sadu útočných scenárov, napríklad:

* malware (ransomware, vírusy, ...)
* botnet / C&C schémy,
* rôzne zraniteľnosti, exploity a APT (advanced persistent threats),
* únik dát,
* a iné.

### RQ022

Scenáre budú zahŕňať cvičenia pre rôzne roly:

* L1 až L3 bezpečnostný dohľad,
* bezpečnostný analytik/analytik malwéru,
* red/blue tím,
* penetračný testeri,
* manažér kybernetickej bezpečnosti,
* data privacy officer,
* administrátor,
* audítor,
* predseda bezpečnostného výboru,
* prípadne iní.

### RQ023

Tréningové scenáre budú zahŕňať celý životný cyklus bezpečnostného incidentu.

### RQ024

Riešenie umožní vytvoriť nové a meniť existujúce scenáre využitím jednoduchého a flexibilného nástroja na tvorbu a aplikáciu scenárov (scenario builder/manager).

### RQ025

Riešenie umožní (bude v scenároch rátať) s účasťou (reálnou alebo simulovanou) green tímu (obrancovia), red tímu (útočníci) a yellow tímu (nevedomo škodliví aktéri).

### RQ026

Scenár musí byť exportovateľný a následne importovateľný medzi rôznymi prostrediami a za účelom zálohy a jeho obnovy.

## Tréning a školenie

### RQ027

Súčasťou dodávky je aj školenie pre administrátorov a dohľad (white tím).

Cieľom školenia je, aby si verejný obstarávateľ pomocou vlastných IT zamestnancov vedel realizovať prevádzku celého systému a základnú úroveň údržby a riešenia prípadných problémov.

Cieľom školenia dohľadu je, aby členovia tímu vedeli realizovať nasledovné činnosti:

* spustiť, reštartovať a resetovať scenáre,
* vytvoriť nové cvičenie na základe šablóny a existujúceho scenára/scenárov, prípade scenár modifikovať,
* spustiť simulovanú architektúru na základe šablóny, alebo vytvoriť úplne novú,
* dohľadovať priebeh cvičenia,
* poskytovať rady účastníkom cvičenia,
* rozumieť logom z cvičenia a hodnotiacim správam,
* pracovať ako green alebo yellow tím počas cvičenia.

Dĺžka školenia: 3 plné pracovné dni rozložené tak, aby bol medzi nimi jeden voľný deň. Školenie bude realizované prezenčnou formou.

### RQ028

Školenie uvedené v RQ027 bude poskytnuté 4 krát počas podpory projektu (2 roky).

## Virtuálna infraštruktúra ministerstva

### RQ029

Dodávateľ riešenia pripraví a bude dohľadovať 6 samostatných cvičení veľkého rozsahu, ktorých cieľom bude okrem iného ukázať interným zamestnancom spôsob práce s dodávaným riešením.

## Priestory

### RQ030

Riešenie poskytne hardvérové vybavenie (t.j. počítače, monitory, notebooky, projektory, tlačiarne atď.) pre nasledovné priestory:

* Školiaca (zasadacia) miestnosť pre White team – základné IT vybavenie (PC, NB, tlačiareň, projektor alebo veľký monitor, flip chart, ...) – kapacita cca 15 osôb.
* Priestor pre Red (útočníci) a Green team – základné IT vybavenie (PC, NB, cca 2-4 veľké monitory, ...) – kapacita cca 15 osôb.
* Priestor pre White team (dohľad nad celou akciou) – základné IT vybavenie (PC, NB, tlačiareň, cca 4 veľké monitory, flip chart, ...) – kapacita cca 4 osoby.
* sieťové prvky – prepojenie miestností (tímov) a core IKT prostredia,
* 2 veľké televízory pre priebežné zobrazovanie výsledkov cvičenia,
* mobilné vybavenie pre jeden tím, aby bolo možné cvičenie realizovať aj v iných priestoroch.

### RQ031

Riešenie bude možné pripojiť aj reálne systémy/zjednodušené verzie, napr. jednoduché aktuátory cez arduino atď.

## Softskills scenáre a platforma

### RQ032

Riešenie bude podporovať aj soft-skills / tabletop scenáre a ich integráciu s technickými scenármi, aby do cvičenia mohli byť zapojené aj netechnické roly. Softskill a tabletop cvičenia a simulácie môžu byť realizované papierovo, alebo elektronicky nad špecifickým tabletop enginom. Tento engine bude môcť byť riadený komplexnými scenármi.

Softskills platforma umožní realizovať a vyhodnotiť softskill scenáre, pričom relevantné požiadavky sú analogické k technickej platforme (najmä hodnotenie a monitoring v prípade online scenárov).

Riešenie zároveň bude obsahovať minimálne nasledovný pomocný softvér:

* helpdesk a ticketovacie riešenie,
* komunikačný nástroj pre jednotlivé roly.

### RQ033

V rámci riešenia budú školené aj manažérske a netechnické roly. Pre tieto roly bude vytvorené podporné prostredie, ktoré bude pozostávať zo systému dokumentov, ktorý by mal simulovať príslušnú organizáciu. Minimálne však:

* bezpečnostné smernice, klasifikácia aktív, analýzu rizík,
* výsledky auditu kybernetickej bezpečnosti,
* BCP a DRP plány,
* vytvorené bezpečnostné roly s popisom práce, napr. manažér kybernetickej bezpečnosti, data privacy officer, hovorca, administrátor, audítor, predseda bezpečnostného výboru atď.,
* zoznam zamestnancov,
* dokumentácia k change requestom.

Tieto dokumenty budú prepojené na minimálne jedno technické prostredie. V prípade viacerých prostredí bude viacero sád dokumentov.

### RQ034

V rámci soft skill platformy budú dodané scenáre, ktoré budú spustiteľné samostatne, t.j. iba ako softskill tréning a scenáre, ktoré budú prepojené aj na prebiehajúce technické tréningy a bude medzi nimi (technický a softskill tréning) interakcia.

Scenáre môžu byť rôznych tipov:

role play,

distruptor scenáre,

a pod..….

## Projektový manažment

### RQ0035

V rámci projektu je potrebné dodať manažérske výstupy v zmysle vyhlášky 85/2020 Z.z. Je k dispozícii aj [checklist](https://www.slov-lex.sk/pravne-predpisy/prilohy/SK/ZZ/2020/85/20200501_5234396-2.pdf) povinností z tejto vyhlášky. V projekte sú predpokladané nasledovné výstupy:

• PID

• Model požiadaviek a prípadov použitia

• Návrh kontraktov SLA

• Detailná funkčná špecifikácia

• Dodávka licencií (ak relevantné)

• Zoznam konfiguračných položiek a ich profilov v štruktúrovanej podobe

• Nástroj dodávaný agilným spôsobom

• Testovacie scenáre - akceptačné, bezpečnostné, záťažové a UX

• Výsledky testov

• Používateľská dokumentácia

• Administračná dokumentácia

• Inštalačná dokumentácia

• Školiace materiály pre jednotlivé roly

• Školenia

• Odborná technická podpora formou konzultačných hodín počas záručnej doby.

# Popis navrhovaného riešenia

Pre predstavu uchádzačov uvádzame aj našu predstavu navrhovaného riešenia, ktorá vyplýva z povinne realizovaných dokumentov [projektový zámer a projektový prístup](https://metais.vicepremier.gov.sk/detail/Projekt/b71faaa8-f0cf-40ee-8544-f36b45719464/cimaster?tab=documentsForm) v zmysle vyhlášky o riadení projektov 85/2020 Z.z.

#### Infraštruktúra a repozitár

Výcvikové a školiace a výcvikové stredisko IB a KyB je tréningový systém založený na izolovanom a kontrolovanom virtuálnom prostredí, ktoré simuluje celú infraštruktúru organizácie VS. Na tomto prostredí sa spúšťajú tréningové scenáre pod dohľadom operátorov. Vo výcvikovom a školiacom a výcvikovom stredisku je možné simulovať rôzne prostredia, ktoré sa vyskladajú z HW a SW repozitára. Tieto repozitáre a virtualizačná platforma tvoria infraštruktúru školiaceho a výcvikového strediska.

#### Technické tréningy

Technické tréningy sa skladajú z:

* + - * scenárov, ktoré predstavujú obsah cvičenia, definíciu zraniteľností a hodnotenie, scenáre je možné dopĺňať a modifikovať,
* simulácie infraštruktúry - na základe konkrétneho scenára, ktorý sa spustí, tento komponent pripraví infraštruktúru, kde bude cvičenie prebiehať,
* scoring a reporting - výsledný report pre každého člena tímu a tím ako celok (pre red aj blue tím, resp. podľa scenára),
* integrácia so softskill/tabletop cvičeniami - komponent zabezpečuje realizáciu komplexných scenárov, ktoré si vyžadujú okrem red/blue tímu aj zapojenie softskill rolí ako projektový manažér, PR manažér, incident handler, atď.

#### Softskill a tabletop

#### Riadiaci a simulačný SW

* Vytváranie tréningovej infraštruktúry podľa potrieb tréningových skupín (od jednoduchej po náročnú infraštruktúru pozostávajúcu z rôznych HW a SW komponentov prepojených do sietí s rôznou architektúrou).
* Simulátor internetu pre potreby cvičení.,
* Využitie rôznych typov a platforiem pre aplikačné prostredie, malo by umožňovať ad-hoc inštaláciu SW nástrojov pre potreby tréningových skupín (špecifických tréningov) a pod..
* Vytváranie nových / užívateľských tréningových scenárov.
* Vytváranie (definovanie) tréningových úloh (typy a prevedenie útočných resp. obranných aktivít, ich monitorovacie a hodnotiace body a pod.).
* Automatizované a poloautomatizované vykonávanie tréningových scenárov.
* Vykonávať administratívu tréningov, evidenciu študentov a pod..
* Priebežný dohľad nad prebiehajúcim tréningom, priebežný scoring (platforma trénera).

Cvičenia sú vykonávané online na prostriedkoch tréningovej platformy. Každá aktivita sa zaznamenáva a vyhodnocuje. Na jednom tréningovom pracovisku je možné vykonávať súbežne viacero na sebe nezávislých cvičení.

Popis blue vs red team cvičení je napríklad [tu](https://ccdcoe.org/exercises/locked-shields/).



# TECHNOLOGICKÁ VRSTVA



## V prípade kritéria na vyhodnotenie ponúk „Najnižšia cena“ verejný obstarávateľ uvažuje nad nasledujúcou štruktúrou ceny

|  |  |  |
| --- | --- | --- |
| ID |  | Spolu v EUR s DPH |
| 1 | Infraštruktúra |  |
| 2 | Technické tréningy |  |
| 3 | Softskill tréningy |  |
| 4 | Scenáre |  |
| 5 | Support riešenia na 2 roky |  |
| 6 | Podpora v rozsahu 200 MDs |  |
| 7 | Spolu |  |

Ak verejný obstarávateľ uplatní okrem ceny kritérium kvality dodania predmetu zákazky), predmetom hodnotenia môže byť:

* celkový architektonický návrh, ktorého max. rozsah je 4 normostrany aj s obrázkami,
* návrh na plnenie požiadaviek, pričom spôsob plnenia každej požiadavky je max 1 normostrana,

# Lehota dodania predmetu zákazky

10 mesiacov od podpisu zmluvy