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

Příloha 1 Smlouvy - Specifikace předmětu smlouvy

Počet listů: 1

Specifikace předmětu smlouvy

Realizace kybernetického cvičení

1. Všeobecné požadavky na poskytovatele

Poskytovatel zajistí kompletní realizaci kybernetického cvičení, které zahrnuje:
- poskytnutí a provoz prostředí Cyber Range pro cvičení kybernetické cvičení konané v roce 2026;
- poskytnutí fyzického zázemí (kanceláří) během přípravného a realizačního týdne cvičení;
- technickou a organizační přípravu cvičení;
- podporu během průběhu cvičení (přípravný i realizační týden);
- zajištění Red Team a Green Team kapacit,
- vyhodnocení výsledků cvičení a prezentaci závěrů.

Minimální požadavky na službu:

2. Předmět plnění

2.1 Příprava scénáře a technického zázemí:

Tvorba injectů a scénáře: od 1. 10. 2025 do 31. 12. 2025
Poskytovatel musí:
- po uvedenou dobu spolupracovat se zadavatelem na tvorbě scénáře a injectů včetně vypořádání průběžných připomínek zadavatele,
- dodat časovou osu scénáře s injecty na základě požadavků zadavatele,
- dodat seznam již připravených injectů ze strany poskytovatele, ze kterého se bude vycházet,
- zajistit 2týdenní bloky (13. – 17. 10. 2025, 3. – 7. 11. 2025) vzájemné každodenní osobní spolupráce se zadavatelem (minimálně v rozsahu 40 hodin týdně) na scénáři a injectech, a to tak, aby finální provedení tohoto dílčího plnění bylo provedeno nejpozději do konce roku 2025,
- vytvořit předem image systému s malwarem pro cvičný forenzní export a analýzu,
- dodat:
• gamebook pro účastníky cvičení,
• dokumentaci cvičné sítě včetně topologie,
- zajistit fyzický přístup do prostorů provedení cvičení počínaje prvním dnem přípravného týdne a konče posledním dnem cvičení (23. 2. – 6. 3. 2026),
- v lednu 2026 provést dry run cvičení (zkušební průběh za účelem ověření připravenosti prostředí, infrastruktury a postupů) ve zrychleném režimu (2 dny, 1 Blue Team, Red Team) dle připraveného scénáře a injectů.

2.2 Kybernetické cvičení – přípravný týden:

Přípravný týden cvičení: 23. 2. 2026 – 27. 2. 2026.
Poskytovatel zajistí:
- úvodní seznámení účastníků s prostředím Cyber Range,
- umožnění aktivního testování a konfigurace prostředí Blue Teamy (s resetem před ostrým cvičením),
- odborné přednášky pro účastníky s odpovídající časovou dotací (minimálně 20 minut odborného výkladu na každou jednotlivou přednášku) zaměřené na následující problematiku:
o ELK stack
o OPNsense
o Ticketovací systém Freescout
- Green Team (min. 1 technik fyzicky na místě)
o k dispozici záložní technický tým (on-site),
- Red Team (3 osoby po celou dobu přípravného i realizačního týdne)
o ve spolupráci s interním Red Teamem zadavatele (3–4 osoby).

2.3 Kybernetické cvičení – realizační týden:

Realizační týden: 2. 3. 2026 – 6. 3. 2026
Poskytovatel dodá:
- plně připravené a funkční prostředí Cyber Range dle níže uvedených parametrů,
- technickou podporu během cvičení (Green Team on-site),
- přístupové údaje a monitoring aktivity Blue Teamů,
- koordinaci Red Teamu a jeho zapojení dle scénáře,
- podklady pro vyhodnocení a závěrečnou zprávu.

2.4 Parametry prostředí Cyber Range:

Přípravný týden cvičení: 23. 2. 2026 – 27. 2. 2026
Realizační týden: 2. 3. 2026 – 6. 3. 2026
Poskytovatel musí dodat prostředí splňující tyto technické požadavky:
- síťová infrastruktura
- 5 identických instancí virtuálních sítí pro 5 Blue Teamů,
- vycházející z poskytovatelem ověřených scénářů vhodných pro tento typ cvičení, přizpůsobené a schválené zadavatelem,
- dokumentace topologie sítě a jednotlivých prvků,
- generátory provozu na síti pro lepší realističnost.

2.5 Služby a nástroje:

- ELK stack v každé instanci s centrální agregací na L3/IHO/CTI úrovni,
- MISP instance v každé síti + centrální agregovaný MISP,
- ticketovací systém,
- VPN přístupy do každé sítě (zvlášť pro Blue Teamy a Red Team),
- možnost vytvoření obrazů disků (stanic/serverů) pro forenzní analýzu,
- 2 servery pro nasazení kontejnerizovaných aplikací (pro InfoOps/WebOps)
- poskytovatel zajistí testování funkčnosti nasazení a přístupu,
- přístup ke stanicím/serverům přes SSH a/nebo RDP.

2.6 Fyzické prostory a zázemí: