Nabídka školení kyberbezpečnosti

Telco Pro Services, a. s.,

Masarykova univerzita

Žerotínovo nám. 617/9, 601 77 Brno, Česká republika
T: +420 549 49 1111, E: info@muni.cz, W: www.muni.cz

1. Obsah nabídky

Obsahem nabídky je zajištění praktického školení z oblasti kybernetické bezpečnosti v prostorách KYPO laboratoře Masarykovy univerzity v Brně v rozsahu pěti dnů. Nedílnou součástí služby je analýza vstupních znalostí a dovedností účastníků, vyhodnocení průběhu školení a zajištění občerstvení pro účastníky školení.

2. Profil účastníka a požadované znalosti

Navrhované školení je vhodné zejména pro členy bezpečnostního týmu SOC/CSIRT a je primárně zaměřeno na procvičení jejich schopností. S ohledem na technická specifika lze do školení zahrnout také administrátory Windows a Linux strojů. Po účastnících je požadována následující množina znalostí:

- Základní znalosti správy Windows, Linux a počítačových sítí.
- Základní znalosti řešení kyberbezpečnostních incidentů.

3. Osnova školení

Primárně je školení zaměřeno na procvičení spolupráce při řešení jednotlivých fází kyberbezpečnostního incidentu společně se školením potřebných technických, procesních a právních postupů nutných k úspěšnému vyřešení incidentu. Konkrétní obsah jednotlivých částí školení je dále přizpůsoben dle potřeb zákazníka v průběhu jejich přípravy.

3.1. Teoretická část

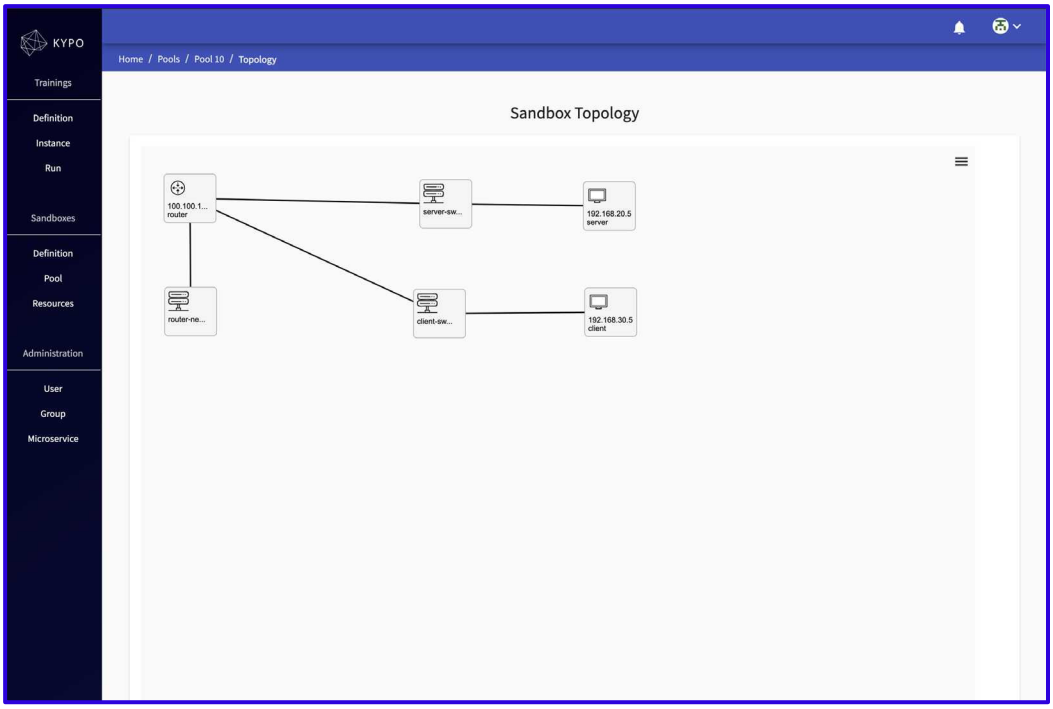
Během teoretické části projdou účastníci teoretickou přípravou zejména v oblasti řešení kyberbezpečnostních incidentů ale také penetračního testování, forenzní analýzy, analýzy provozu a práva. Tyto aktivity jsou doplněny o praktické úkoly, které pomáhají pochopení problematiky.

Teoretická část pomocí níže uvedených modulů rozdělených do tří přednáškových bloků pokrývá oblastí potřebné vědomosti pro řešení incidentů. Každý z modulů je doplněn praktickými ukázkami a úkoly.

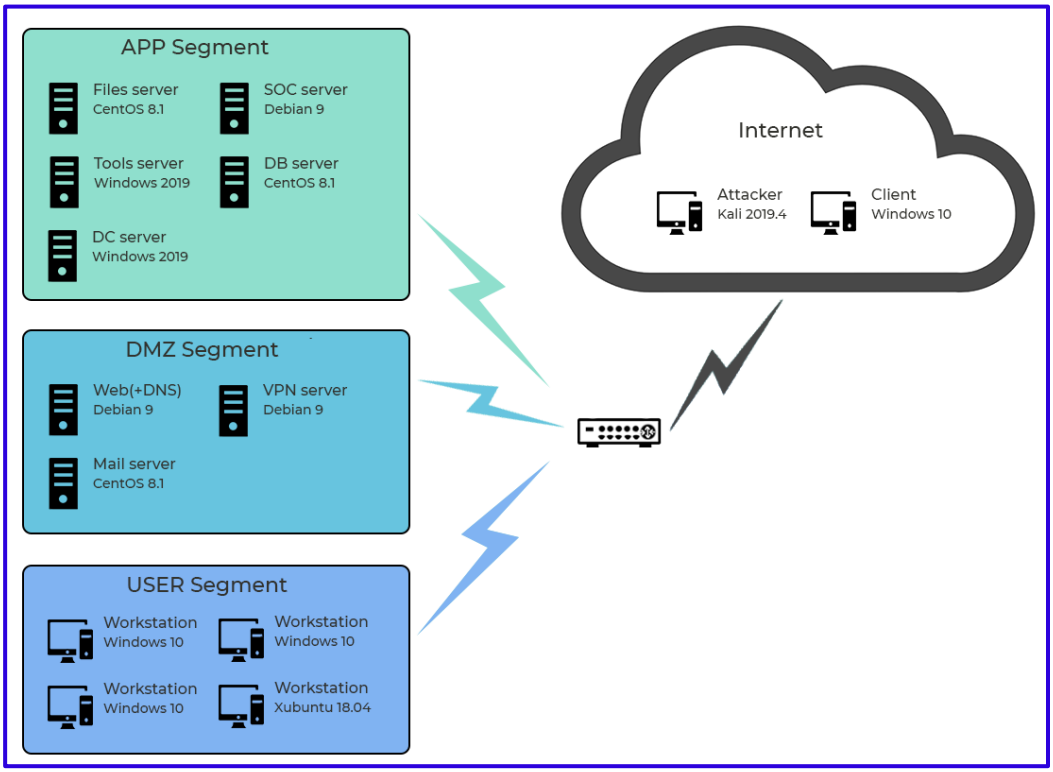
- **Odezva na počítačový bezpečnostní incident:** Modul představuje typický životní cyklus bezpečnostního incidentu, jehož kroky jsou vysvětleny na skutečných příkladech incidentů. Zároveň představuje CERT / CSIRT v organizaci a popisuje její služby.
- **Legislativa a reporting:** Je poskytnut základní přehled české legislativy týkající se kybernetické bezpečnosti a jejích důsledků pro týmy CSIRT. Představeny jsou zásady organizace a komunikaci s vrcholovým managementem včetně posouzení škod pro rozhodování na nejvyšší úrovni
- **Obrana při bezpečnostním incidentu:** Jsou představeny základní koncepty ochrany infrastruktury na úrovni sítě a její topologii, brány firewall a na úrovni systému na koncových hostitelích s ohledem na základní teoretické koncepty.
- **Penetrační testování:** Seznamuje s fázemi procesu penetračního testování, od interakcí s klientem, přes skutečné testování až po reporting. Zohledněny jsou také standardy pro oblast penetračního testování a řada volně dostupných nástrojů i s praktickou ukázkou.
- **Analýza strojů:** Představuje základní informace o roli forenzní techniky, pojmu digitální evidence, zásady pro zabezpečení digitálních důkazů a demonstruje základní techniky pro analýzu perzistentního úložiště (disků) a paměti.
- **Analýza sítí:** Představuje monitorování sítě pomocí snímání nezpracovaných paketů a síťových toků. Dále analýzu sítě a jejích služby k detekci škodlivého chování a síťových útoků.

3.2. Praktická část

Praktická část školení je zaměřena na praktické řešení proběhlých, či aktivních kyberbezpečnostních událostí a incidentů. Účastníci budou rozděleni do týmů o 3-4 osobách a zhostí se role kyberbezpečnostního týmu. Využijí znalosti získané v teoretickém bloku pro řešení incidentů.



Školení je realizováno na platformě KYPO CRP s využitím aktuálních zranitelností a postupů nad virtualizovaným prostředím kopírujícím typické rozložení podnikové sítě. Podniková síť se skládá z aplikačního segmentu sdružujícího servery, uživatelského segmentu, jehož součástí jsou i cvičící a v neposlední řadě demilitarizované zóny, která také obsahuje VPN server pro připojení z internetu a vzdálenou práci. V rámci školení jsou využity operační systémy Windows a Linux na serverech i pracovnách stanicích. Využívané služby v infrastruktuře jsou vždy založeny na open-source software.



Cílem praktické části je komplexně procvičit technické znalosti potřebné k řešení kyberbezpečnostních incidentů společně s procesní stránkou a komunikací uvnitř i vně týmu. Důraz tedy bude kladen nejen na schopnost odhalení, klasifikace a řešení kyberbezpečnostního incidentu ale také na sdílení relevantních informací s možností sběru důkazního materiálu a jeho sdílení v rámci týmu organizace ale také s týmy v dalších organizacích, případně s hlavním koordinátorem kyberbezpečnosti.

Scénář praktické části je založen na útoku typu „Advanced persistent threat“ na organizaci, jehož cílem je exfiltrace duševního vlastnictví. V okamžiku startu školení již útok probíhá a některé stroje a účty jsou tedy již kompromitovány. Útok pak pokračuje s různou intenzitou po celou dobu praktické části. Paralelně s tímto útokem dochází k nesouvisejícím, útokům typu phishing, odepření dostupnosti, ransomware a dalším událostem. Některé z nich může zachytit tým samotný a jiné jsou hlášeny uživateli podnikové sítě.

Absolvováním závěrečné části kurzu získají účastníci praktickou zkušenost s detekcí, identifikací a řešením široké řady bezpečnostních incidentů tematicky připravených na míru prostředí zadavatele. Zároveň účastníci zrychlí reakční dobu na incident a zkrátí čas vedoucí k obnově podnikového prostředí.

3.3. Vyhodnocení školení

Po ukončení školení účastníci obdrží certifikát s možností jeho uznání v rámci celoživotního vzdělávání Masarykovy univerzity. V rámci teoretických bloků jsou jednotliví účastníci hodnoceni pomocí krátkého testu znalostí. V rámci praktické části je realizováno kvantitativní a kvalitativní hodnocení týmu ze získaných dat a informací poskytnutých lektory.

4. Harmonogram školení

První den školení	
10:00 – 10:30	Příjezd a registrace
10:30 – 10:40	Seznámení s obsahem a cíli školení
10:40 – 12:00	Přednáškový blok I (80 minut)
12:00 – 13:00	Oběd
13:00 – 14:20	Přednáškový blok I (80 minut)
14:20 – 14:40	Přestávka
14:40 – 16:00	Přednáškový blok I (80 minut)
Druhý den školení	
09:00 – 10:20	Přednáškový blok II (80 minut)
10:20 – 10:40	Přestávka
10:40 – 12:00	Přednáškový blok II (80 minut)
12:00 – 13:00	Oběd
13:00 – 14:20	Přednáškový blok II (80 minut)
14:20 – 14:40	Přestávka
14:40 – 16:00	Přednáškový blok II (80 minut)

Třetí den školení	
09:00 – 10:20	Přednáškový blok III (80 minut)
10:20 – 10:40	Přestávka
10:40 – 12:00	Přednáškový blok III (80 minut)
12:00 – 13:00	Oběd
13:00 – 13:30	Představení virtuální organizace a platformy KYPO CRP
13:30 – 16:00	Praktická část školení (150 minut)
Čtvrtý den školení	
09:00 – 12:00	Praktická část školení (180 minut)
12:00 – 13:00	Oběd
13:00 – 16:00	Praktická část školení (180 minut)
Pátý den školení	
09:00 – 12:00	Praktická část školení (180 minut)
12:00 – 13:00	Oběd
13:00 – 14:30	Praktická část školení (90 minut)
14:30 – 15:00	Přestávka
15:00 – 15:30	Ukončení školení a závěrečné shrnutí

5. Termín a místo realizace

Realizace je stanovena na 22.–26. 11. 2021 v KYPO laboratoři Masarykovy univerzity.

6. Počet účastníků

— Počet účastníků skupiny ČEZ je předběžně stanoven na 24 osob, z toho 4 osoby za společnost Telco Pro Services, a. s.,

7. Cena realizace

Příprava, provedení a vyhodnocení školení pro celkem 24 osob	**1 320 000,-**
Přepočet na 4 osoby	220 000,-

Ceny jsou uvedeny v českých korunách bez DPH.

8. Kontaktní osoba

- 
-
-

9. Příloha – životopisy lektorů

-  cv.pdf
- _cv.pdf
- v.pdf
- l_cv.pdf
- pdf