Możliwość dofinansowania

Inżynier bezpieczeństwa systemu MikroTik RouterOS (MTCSE) - szkolenie certyfikowane z egzaminem

Numer usługi 2026/02/12/202969/3330062

3 813,00 PLN brutto
3 100,00 PLN netto
238,31 PLN brutto/h
193,75 PLN netto/h
196,00 PLN cena rynkowa

MIKROTIK WARSAW TRAINING CENTER PIOTR WASYK, MICHAŁ FILIPEK SPÓŁKA CYWILNA

Brak ocen dla tego dostawcy

Warszawa / stacjonarna
Usługa szkoleniowa
16 h
09.04.2026 do 10.04.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do osób, które chcą wyspecjalizować się w obszarze cyberbezpieczeństwa sieci MikroTik. Administratorzy sieci, inżynierowie systemowi oraz specjaliści IT odpowiedzialni za bezpieczeństwo infrastruktury LAN/WAN.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	02-04-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Głównym celem szkolenia jest przygotowanie uczestnika do samodzielnego projektowania, wdrażania oraz zarządzania zaawansowanymi mechanizmami bezpieczeństwa w infrastrukturze sieciowej opartej na systemie MikroTik RouterOS.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje współczesne wektory ataków na usługi sieciowe oraz metody ich wykrywania	Wymienia najpopularniejsze typy ataków i opisuje mechanizmy działania skanowania portów oraz prób siłowych (brute-force)	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje zaawansowane reguły filtrowania w warstwie drugiej (L2) i trzeciej (L3) systemu RouterOS	Implementuje bezpieczne filtrowanie na mostach (Bridge) oraz buduje zaawansowane łańcuchy w IP Firewall	Obserwacja w warunkach symulowanych
Wdraża mechanizmy ochrony dostępu do infrastruktury sieciowej	Uruchamia funkcję Port Knocking oraz konfiguruje reguły mitygujące ataki typu brute-force	Test teoretyczny z wynikiem generowanym automatycznie
Zestawia bezpieczne i szyfrowane połączenia tunelowe VPN	Konfiguruje tunele zgodnie z najlepszymi praktykami bezpieczeństwa MikroTik	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	MikroTik
Nazwa Podmiotu certyfikującego	MikroTik

Program

Program obejmuje 16 godzin dydaktycznych realizowanych w ciągu 2 dni.

Informacje organizacyjne

• **Czas trwania:** 16 godzin dydaktycznych (2 dni po 8h).

• **Godzina rozpoczęcia:** 09:00.

• **Metodyka:** Szkolenie prowadzone metodami aktywizującymi (warsztaty praktyczne stanowią min. 60% czasu).

• **Stanowisko pracy:** Samodzielne stanowisko komputerowe z dostępem do dedykowanego routera MikroTik dla każdego uczestnika.

• **Materiały:** Uczestnicy otrzymują komplet materiałów dydaktycznych w formie cyfrowej.

• **Walidacja:** Integralna część usługi (egzamin certyfikujący), której czas jest wliczony w łączny wymiar godzin

Zakres tematyczny szkolenia

Dzień 1: Analiza zagrożeń i bezpieczeństwo warstwy 2 (8h dydaktycznych)

1. **Analiza bezpieczeństwa sieci:** Przegląd współczesnych wektorów ataków na wybrane usługi sieciowe oraz charakterystyka metodologii działań intruzów.

2. **Mechanizmy wykrywania ataków:** Konfiguracja systemów logowania zdarzeń i monitorowania ruchu w celu identyfikacji incydentów bezpieczeństwa.

3. **Bezpieczeństwo warstwy drugiej (L2):** Zabezpieczanie mostów (Bridge), filtrowanie ruchu na podstawie adresów MAC oraz ograniczanie nieautoryzowanego dostępu do infrastruktury lokalnej.

Dzień 2: Zaawansowany Firewall, ochrona dostępu i walidacja (8h dydaktycznych)

1. **Zaawansowany IP Firewall:** Konfiguracja łańcuchów filtrów, zarządzanie stanami połączeń (Connection Tracking) oraz optymalizacja reguł zapory sieciowej.

2. **Ochrona dostępu do routera:** Implementacja mechanizmu Port Knocking oraz tworzenie reguł mitygujących ataki typu brute-force (próby siłowe).

3. **Bezpieczeństwo komunikacji zdalnej:** Zestawianie i zabezpieczanie tuneli VPN z wykorzystaniem zaawansowanych algorytmów szyfrowania.

4. **Diagnostyka i walidacja:** Warsztaty rozwiązywania problemów (troubleshooting) w konfiguracjach bezpieczeństwa oraz przeprowadzenie oficjalnego procesu walidacji

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 - Przegląd zagrożeń i ataków na wybrane usługi - Omówienie najpopularniejszych ataków - Wykrywanie ataków - Filtrowanie L2	Michał Filipek	09-04-2026	09:00	17:00	08:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 2 - Zaawansowana konfiguracja IP->Firewall - Port knocking - Ataki typu brute-force - Wykrywanie skanowania portów - Kryptografia	Michał Filipek	10-04-2026	09:00	17:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 813,00 PLN
Koszt przypadający na 1 uczestnika netto	3 100,00 PLN
Koszt osobogodziny brutto	238,31 PLN
Koszt osobogodziny netto	193,75 PLN
W tym koszt walidacji brutto	615,00 PLN
W tym koszt walidacji netto	500,00 PLN
W tym koszt certyfikowania brutto	615,00 PLN
W tym koszt certyfikowania netto	500,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Michał Filipek

Michał Filipek posiada ponad 12-letnie doświadczenie w branży IT i telekomunikacyjnej, przy czym w ciągu ostatnich 5 lat stale realizuje zaawansowane projekty dla operatorów telekomunikacyjnych w zakresie projektowania, wdrażania i utrzymania infrastruktury sieciowej IP oraz systemów wysokiej

dostępności (HA). Jego wykształcenie techniczne (Informatyka na Politechnice Warszawskiej) jest na bieżąco uzupełniane o praktykę w najnowszych technologiach sieciowych.
Wszystkie kluczowe uprawnienia trenerskie i techniczne Michała są aktualne i zostały zdobyte lub odnowione nie wcześniej niż 3 lata temu.
• MikroTik Trainer oraz pełny komplet certyfikatów inżynierskich (w tym MTCNA, MTCRE, MTCINE, MTCSE) – wszystkie odnowione w ciągu ostatnich 3 lat.
• Zabbix Trainer oraz najwyższe poziomy certyfikacji (Certified Expert, Professional).
• Ubiquiti Trainer i certyfikacje z zakresu rozwiązań bezprzewodowych (UWA, UBWA, URSCA).
• Red Hat Certified Engineer (RHCE) oraz RHCSA – potwierdzające biegłość w administracji systemami Linux

Michał regularnie występuje jako prelegent na konferencjach branżowych, dzieląc się wiedzą z zakresu budowy bezpiecznych i monitorowanych systemów sieciowych.
Zgodnie ze standardami jakościowymi, Michał Filipek dba o aktualność swoich kompetencji: jego certyfikaty MikroTik są odnawiane co 3 lata. Dodatkowo posiada udokumentowane doświadczenie dydaktyczne, przeprowadzając w ostatnich latach ponad 120 godzin szkoleń dla osób dorosłych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują komplet materiałów dydaktycznych w formie cyfrowej.

Warunki uczestnictwa

Posiadanie certyfikatu Mikrotik MTCNA

Adres

ul. Ogrodowa 58
00-876 Warszawa
woj. mazowieckie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

IWONA WASYK

E-mail iwona@mwtc.pl
Telefon (+48) 503 446 641