Możliwość dofinansowania

Cyberbezpieczeństwo: Bezpieczeństwo Systemu Windows (praktyczne warsztaty z ochrony systemu)

Numer usługi 2025/07/10/148153/2871303

7 488,24 PLN brutto
6 088,00 PLN netto
534,87 PLN brutto/h
434,86 PLN netto/h

Niebezpiecznik.pl
Piotr Konieczny

4,7 / 5
30 ocen

Kraków / stacjonarna
Usługa szkoleniowa
14 h
20.11.2025 do 21.11.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie kierujemy przede wszystkim do osób, które zarządzają firmowymi sieciami opartymi systemy Windows lub muszą analizować ich bezpieczeństwo: • administratorów oraz architektów i projektantów systemów komputerowych • audytorów i pentesterów, ...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie bezpieczeństwa systemu Windows — dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-) Uczestnik powinien sprawnie poruszać się w Active Directory (przynajmniej w podstawowym zakresie) oraz posiadać umiejętność korzystania z narzędzi zdalnej administracji (RSAT). Istotne jest również, by orientował się w systemach operacyjnych Microsoft i ich elementach.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	12-11-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	14
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Bezpieczeństwa Systemu Windows. Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.	**Laboratoria przygotowane na symulowanym środowisku kształcenia.**	**Obserwacja w warunkach symulowanych**

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-windows-warsztaty/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Analiza wykorzystywanych narzędzi:

- Active Directory Domain Services
- Group Policy Object
- Microsoft Security Compliance Toolkit
- Local Admin Password Solution
- Sysinternals Sute

Omówienie rekomendacji:

- NIST – National Institute of Standards and Technology
- STIG – Security Technical Implementation Guides
- CIS Security Benchmark

Pozyskiwanie wiedzy na temat bezpiecznego środowiska pracy & centralnego zarządzania konfiguracją wykorzystując narzędzia:

- Access Control List – ograniczenie dla zwykłego użytkownika do tworzenia plików tylko w profilu
- Advanced Auditing – ustawienia audytu zdarzeń w systemie
- Event Viewer – ustawienia, archiwizacja logów
- Event Forwarding – centralna archiwizacja logów,
- User Rights – uprawnienia użytkownika w systemie
- Restricted Groups – zarządzanie przynależnością do grup lokalnych
- Security Options – opcje bezpieczeństwa systemu
- Local Admin Password Solution – zarządzanie wbudowanymi kontami administracyjnymi
- Services – usługi systemowe
- AppLocker/SRP – ograniczenie uruchamianych aplikacji tylko do autoryzowanych
- Integrity Levels – zarządzanie uprawnieniami na obiektach systemowych
- Firewall & IPSec – systemowa zapora sieciowa
- Preferences – specyficzne zmiany w rejestrach, np. konfiguracja Adobe Reader, Java
- Folder Redirection –
- Internet Explorer 11/Edge
- Office 2013/2016/2019/2021
- Enhanced Mitigation Experience Toolkit 5.52/ Windows Defender Exploit Guard
- Windows Defender Security Center
- BitLocker – szyfrowanie dysków
- Microsoft Security Compliance Toolkit – zbiór rekomendowanych ustawień dla produktów Microsoft
- Sysinternal Suite – pakiet przydatnych narzędzi np. AccessChk, Procmon
- System Microsoft Windows – konfiguracja środowiska,
- Sysmon
- File Screening – zarzadzanie zawartością na serwerze plików
- Dynamic Access Control – nowe podejście do nadawania uprawnień

Laboratoriom poświecono najwięcej czasu, ponieważ dzięki temu każdy uczestnik szkolenia może własnoręcznie skonfigurować, a przez to lepiej zrozumieć omawiany problem i skuteczne metody ochrony. Podczas szkolenia pracujemy na specjalnym środowisku, zawierającym aktualne oprogramowanie Microsoft, które zostało skonfigurowane tak, aby najwierniej oddać sytuacje panujące w większości firm (kontoler domeny i stacje klienckie). Na szkoleniu wspólnie budujemy bezpieczną konfigurację stacji roboczej z omówieniem na przykładach poszczególnych jej elementów oraz demonstracją możliwych nadużyć.

Harmonogram

Liczba przedmiotów/zajęć: 3

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 3 Analiza wykorzystywanych narzędzi	Paweł Tworek	20-11-2025	10:00	14:00	04:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 3 Omówienie rekomendacji	Paweł Tworek	20-11-2025	14:00	17:00	03:00
3 z 3 Pozyskiwanie wiedzy na temat bezpiecznego środowiska pracy & centralnego zarządzania konfiguracją wykorzystując narzędzia	Paweł Tworek	21-11-2025	10:00	17:00	07:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 488,24 PLN
Koszt przypadający na 1 uczestnika netto	6 088,00 PLN
Koszt osobogodziny brutto	534,87 PLN
Koszt osobogodziny netto	434,86 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Tworek

Tak.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (zapis prezentacji).

Warunki uczestnictwa

Każdy uczestnik **musi** podpisać deklarację, że poznane techniki ataków i narzędzia będzie wykorzystywał dla swojej infrastruktury.

Informacje dodatkowe

Z dokładnymi terminami tego szkolenia zapoznać się można pod poniższym linkiem:

https://niebezpiecznik.pl/szkolenia/bezpieczenstwo-windows-warsztaty/?zai

Po wybraniu terminu prosimy o kontakt mailowy: szkolenia@niebezpiecznik.pl

Adres

ul. Armii Krajowej 11
30-150 Kraków
woj. małopolskie

Szczegóły miejsca realizacji usługi wysyłane są do Uczestników szkolenia na tydzień przed danym terminem.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Magda Kowalska

E-mail szkolenia@niebezpiecznik.pl
Telefon (+48) 124 420 244