Możliwość dofinansowania

Bezpieczeństwo Windows – ataki i ochrona środowiska Microsoft Windows w firmie - szkolenie

Numer usługi 2026/07/09/172284/3679782

3 000,00 PLN brutto
3 000,00 PLN netto
93,75 PLN brutto/h
93,75 PLN netto/h
261,33 PLN cena rynkowa

UKNOW EDU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

2 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
32:00 h
09.11.2026 do 13.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób odpowiedzialnych za administrację, utrzymanie i bezpieczeństwo środowisk Microsoft Windows w organizacji. Adresatami szkolenia są w szczególności administratorzy systemów Windows, administratorzy Active Directory, specjaliści IT, pracownicy działów bezpieczeństwa informacji, osoby odpowiedzialne za infrastrukturę IT, helpdesk/second line support oraz osoby zajmujące się ochroną stacji roboczych, serwerów i środowisk domenowych. Szkolenie jest przeznaczone dla osób, które chcą rozwinąć praktyczne umiejętności w zakresie rozpoznawania wektorów ataków na środowisko Windows, analizy podatności, podstaw testów penetracyjnych, zabezpieczania systemów, hardeningu, ochrony Active Directory oraz reagowania na zagrożenia w infrastrukturze firmowej.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	6
Data zakończenia rekrutacji	30-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem edukacyjnym szkolenia jest przygotowanie uczestników do identyfikowania zagrożeń i podatności w środowisku Microsoft Windows oraz stosowania podstawowych i zaawansowanych mechanizmów ochrony stacji roboczych, serwerów i środowiska domenowego.

Po zakończeniu szkolenia uczestnik będzie potrafił rozpoznawać typowe wektory ataków na systemy Windows, interpretować etapy ataku zgodnie z modelem Cyber Kill Chain, analizować wybrane techniki ofensywne, wskazywać podatności związane z poświadczeni

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozpoznaje podstawowe zagrożenia i wektory ataków na środowisko Microsoft Windows.	Poprawnie wskazuje przykładowe wektory ataków oraz etapy ataku zgodnie z modelem Cyber Kill Chain.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje podatności związane z konfiguracją systemów Windows, usługami systemowymi i poświadczeniami.	Poprawnie rozpoznaje przykładowe podatności dotyczące kont użytkowników, haseł, usług systemowych, LSASS, SAM, NTLM/LM oraz konfiguracji lokalnej.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje działania zabezpieczające stacje robocze, serwery i środowisko domenowe Windows.	Poprawnie dobiera przykładowe mechanizmy ochrony, w tym BitLocker, Windows Firewall, aktualizacje, LAPS, JEA/JIT oraz zabezpieczenia Active Directory.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik dobiera podstawowe rekomendacje naprawcze po analizie zagrożeń w środowisku Windows.	Poprawnie wskazuje działania ograniczające ryzyko oraz przykładowe zalecenia naprawcze dla administratorów systemów Windows.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Podstawy cyberbezpieczeństwa Windows i modelowanie zagrożeń

- bezpieczeństwo systemów Microsoft Windows,
- model Cyber Kill Chain,
- lokalne, zdalne i socjotechniczne wektory ataków.

1. Metodologia testów penetracyjnych i ramy prawne

- podstawowe pojęcia i standardy testów penetracyjnych,
- aspekty prawne prowadzenia testów,
- fazy testu penetracyjnego.

1. Rekonesans i zbieranie informacji

- pasywne i aktywne techniki zbierania informacji,
- wykorzystanie narzędzi do skanowania i identyfikacji podatności,
- analiza środowiska Windows pod kątem możliwych wektorów ataku.

1. Analiza ruchu sieciowego

- przechwytywanie pakietów w środowisku Windows,
- analiza komunikacji sieciowej,
- identyfikacja anomalii i analiza protokołów systemowych.

1. Ataki lokalne i przejmowanie kontroli

- przejmowanie kont użytkowników,
- eskalacja uprawnień,
- nadużycia w konfiguracji usług systemowych.

1. Poświadczenia Windows i techniki łamania haseł

- mechanizmy przechowywania i ochrony poświadczeń,
- SAM, LSASS, sekrety LSA,
- protokoły NTLM/LM,
- analiza podatności baz poświadczeń.

1. Hardening stacji roboczych i serwerów

- szyfrowanie dysków BitLocker,
- konfiguracja Windows Firewall,
- zarządzanie aktualizacjami i patch management,
- zabezpieczenia lokalne systemów Windows.

1. Utrzymanie dostępu i złośliwe oprogramowanie

- techniki persystencji,
- backdoor i rootkit w architekturze Windows,
- podstawowe metody wykrywania i ograniczania zagrożeń.

1. Eksploitacja podatności i kompromitacja Active Directory

- analiza znanych podatności systemowych,
- ruch boczny w sieci,
- ataki typu Pass-the-Hash,
- wektory ataków na Active Directory i strukturę domenową.

1. Zaawansowane zabezpieczenia środowiska Windows

- Managed Service Accounts i Group Managed Service Accounts,
- wdrażanie LAPS,
- architektura uprawnień Microsoft,
- JEA i JIT,
- koncepcja Bastion Forest / Red Forest.

1. Socjotechnika, evasion i ukrywanie działań

- phishing w środowisku korporacyjnym,
- wprowadzenie do fuzzingu,
- omijanie systemów bezpieczeństwa,
- modyfikacja i czyszczenie dzienników zdarzeń.

1. Warsztaty przekrojowe i rekomendacje końcowe

- symulacja pełnego ataku i obrony,
- scenariusz Red vs Blue,
- raportowanie wyników testów,
- opracowanie zaleceń naprawczych,
- podsumowanie szkolenia i sesja Q&A.

1. Walidacja efektów uczenia się

- test teoretyczny z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 29

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Podstawy cyberbezpieczeństwa Windows i modelowanie zagrożeń	Zajęcia	Monika Bienies	09-11-2026	08:00	10:00	02:00
2 z 29 -	Przerwa	-	09-11-2026	10:00	10:15	00:15
3 z 29 Metodologia testów penetracyjnych i ramy prawne	Zajęcia	Monika Bienies	09-11-2026	10:15	12:00	01:45
4 z 29 -	Przerwa	-	09-11-2026	12:00	12:30	00:30
5 z 29 Pasywne i aktywne zbieranie informacji	Zajęcia	Monika Bienies	09-11-2026	12:30	14:15	01:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 29 -	Przerwa	-	09-11-2026	14:15	14:30	00:15
7 z 29 Analiza ruchu sieciowego na poziomie hosta i sieci	Zajęcia	Monika Bienies	09-11-2026	14:30	16:00	01:30
8 z 29 Anatomia ataku lokalnego i przejmowanie kontroli	Zajęcia	Monika Bienies	10-11-2026	08:00	10:00	02:00
9 z 29 -	Przerwa	-	10-11-2026	10:00	10:15	00:15
10 z 29 Poświadczenia Windows — architektura i techniki łamania	Zajęcia	Monika Bienies	10-11-2026	10:15	12:00	01:45
11 z 29 -	Przerwa	-	10-11-2026	12:00	12:30	00:30
12 z 29 Hardening stacji roboczych i serwerów	Zajęcia	Monika Bienies	10-11-2026	12:30	14:15	01:45
13 z 29 -	Przerwa	-	10-11-2026	14:15	14:30	00:15
14 z 29 Utrzymanie dostępu i złośliwe oprogramowanie	Zajęcia	Monika Bienies	10-11-2026	14:30	16:00	01:30
15 z 29 Eksploitacja znanych podatności systemowych	Zajęcia	Monika Bienies	12-11-2026	08:00	10:00	02:00
16 z 29 -	Przerwa	-	12-11-2026	10:00	10:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 29 Ruch boczny i kompromitacja Active Directory	Zajęcia	Monika Bienies	12-11-2026	10:15	12:00	01:45
18 z 29 -	Przerwa	-	12-11-2026	12:00	12:30	00:30
19 z 29 Zaawansowane zabezpieczenia sieciowe w domenie Windows	Zajęcia	Monika Bienies	12-11-2026	12:30	14:15	01:45
20 z 29 -	Przerwa	-	12-11-2026	14:15	14:30	00:15
21 z 29 Izolacja i nowoczesna architektura uprawnień Microsoft	Zajęcia	Monika Bienies	12-11-2026	14:30	16:00	01:30
22 z 29 Socjotechnika i testowanie aplikacji/usług Windows	Zajęcia	Monika Bienies	13-11-2026	08:00	10:00	02:00
23 z 29 -	Przerwa	-	13-11-2026	10:00	10:15	00:15
24 z 29 Evasion — omijanie systemów bezpieczeństwa i ukrywanie działań	Zajęcia	Monika Bienies	13-11-2026	10:15	12:00	01:45
25 z 29 -	Przerwa	-	13-11-2026	12:00	12:30	00:30
26 z 29 Warsztaty przekrojowe: symulacja pełnego ataku i obrony	Zajęcia	Monika Bienies	13-11-2026	12:30	14:15	01:45
27 z 29 -	Przerwa	-	13-11-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 29 Raportowanie, rekomendacje i zamknięcie szkolenia	Zajęcia	Monika Bienies	13-11-2026	14:30	15:45	01:15
29 z 29 -	Walidacja	Monika Bienies	13-11-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	27:45
w tym suma godzin walidacji	00:15
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	37:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 000,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	3 000,00 PLN
Koszt osobogodziny brutto	93,75 PLN
Koszt osobogodziny netto	93,75 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin

Liczba godzin zegarowych usługi	32:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Monika Bienies

Osoba wskazana w karcie pełni funkcję koordynatora organizacyjnego usługi. Prowadzący merytoryczny zostanie przypisany do usługi przed rozpoczęciem szkolenia, zgodnie z zakresem tematycznym usługi oraz wymaganiami dotyczącymi doświadczenia w obszarze bezpieczeństwa środowisk Microsoft Windows, Active Directory i infrastruktury IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały szkoleniowe wyłącznie w formie elektronicznej, najpóźniej w pierwszym dniu szkolenia. Materiały zostaną udostępnione w języku polskim.

Warunki techniczne

Szkolenie będzie realizowane w formie zdalnej, za pośrednictwem platformy szkoleniowej / komunikatora internetowego udostępnionego przez Wykonawcę.

Uczestnik powinien posiadać komputer lub laptop z dostępem do Internetu, aktualną przeglądarką internetową, głośnikami lub słuchawkami oraz mikrofonem. Zalecane jest stabilne łącze internetowe umożliwiające udział w wideokonferencji oraz odbiór obrazu i dźwięku w czasie rzeczywistym.

Kontakt

Monika Bienies

E-mail szkolenia@uknowedu.pl

Telefon (+48) 693 708 705