



Compendium -
Centrum Edukacyjne
Spółka z o.o.



Zarządzanie bezpieczeństwem w środowisku MS Windows Server i Windows 10/11

Numer usługi 2024/10/22/10100/2374540

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 40 h

📅 16.12.2024 do 20.12.2024

3 400,00 PLN brutto

3 400,00 PLN netto

85,00 PLN brutto/h

85,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Zainteresowani szkoleniem Microsoft.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	15-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Celem szkolenia popartego licznymi przykładami jest zwiększenie świadomości w zakresie zagrożeń i zarządzania bezpieczeństwem środowisk opartych o produkty serwerowe i klienckie systemy operacyjne firmy Microsoft.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>Po ukończeniu kursu:</p> <p>Uczestnik Identyfikacje zagrożeń występujące w środowisku Windows wg norm ISO/IEC</p> <p>Bezpiecznie uwierzytelnia i ochrania za pomocą poświadczeń w systemie Windows (z wykorzystaniem narzędzia MimiKatz)</p> <p>Autoryzacje dostępu do zasobów</p> <p>Szyfruje dane w oparciu o dobre praktyki</p> <p>Kontroluje prawa i uprawnienia użytkowników</p> <p>Uwierzytelniania dwuskładnikowe w oparciu o karty inteligentne</p> <p>Zna i rozumie Network Policy Server</p> <p>Analizuje ruchu sieciowy i hardening systemów</p>	<p>Klasyfikuje współczesne zagrożenia, określa zakres systemu zarządzania bezpieczeństwem</p> <p>Szacuje koszty, i szansę osiągnięcia założonego poziomu zabezpieczeń,</p> <p>Przegląda metody uwierzytelniania</p> <p>Analizuje płynnie ryzyka procesu uwierzytelniania, oraz Ataków typu Offline - eskalacja uprawnień</p> <p>Ataków Pass-the-hash i Pass-the-Ticket, jak i Legacy LAPS i Windows LAPS</p> <p>Zna polityki hasła domenowych z uwzględnieniem PSO oraz zarządzalne konta serwisowe (gMSA)</p> <p>Kontroluje i dokonuje inspekcji dostępu na podstawie ACL</p> <p>Projektuje zaawansowane zasady inspekcji</p> <p>Wdraża autoryzacje opartą na oświadczeniach</p> <p>Zna i potrafi planować, wdrożenie i utrzymanie roli AD CS, metody dystrybucji i zarządzanie certyfikatami</p> <p>Zabezpieczanie komunikacji – protokoły TLS i IPsec oraz rola Windows Defender Firewall with Advanced Security</p> <p>Podpisuje cyfrowe dokumentów MS Office i plików PDF</p> <p>Podpisuje skryptów PowerShell</p>	<p>Wywiad swobodny</p>

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

- Identyfikacja zagrożeń występujących w środowisku Windows wg norm ISO/IEC
- Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows (z wykorzystaniem narzędzia MimiKatz)
- Autoryzacja dostępu do zasobów
- Szyfrowanie danych w oparciu o dobre praktyki
- Kontrola praw i uprawnień użytkowników
- Infrastruktura Klucza Publicznego
- Uwierzytelnianie dwuskładnikowe w oparciu o karty inteligentne
- Network Policy Server
- Analiza ruchu sieciowego
- Analiza bezpieczeństwa i hardening systemów

Harmonogram

Liczba przedmiotów/zajęć: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Identyfikacja zagrożeń występujących w środowisku Windows wg norm ISO/IEC Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows (z wykorzystaniem narzędzia MimiKatz)	Bogdan Gacek	16-12-2024	09:00	12:00	03:00
2 z 16 Identyfikacja zagrożeń występujących w środowisku Windows wg norm ISO/IEC Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows (z wykorzystaniem narzędzia MimiKatz)	Bogdan Gacek	16-12-2024	12:00	14:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>3 z 16</p> <p>Identyfikacja zagrożeń występujących w środowisku Windows wg norm ISO/IEC Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows (z wykorzystaniem narzędzia MimiKatz)</p>	Bogdan Gacek	16-12-2024	14:00	17:00	03:00
<p>4 z 16</p> <p>Szyfrowanie danych w oparciu o dobre praktyki Kontrola praw i uprawnień użytkowników</p>	Bogdan Gacek	17-12-2024	09:00	12:00	03:00
<p>5 z 16</p> <p>Szyfrowanie danych w oparciu o dobre praktyki Kontrola praw i uprawnień użytkowników</p>	Bogdan Gacek	17-12-2024	12:00	14:00	02:00
<p>6 z 16</p> <p>Szyfrowanie danych w oparciu o dobre praktyki Kontrola praw i uprawnień użytkowników</p>	Bogdan Gacek	17-12-2024	14:00	17:00	03:00
<p>7 z 16</p> <p>Infrastruktura Klucza Publicznego Uwierzytelnianie dwuskładnikowe w oparciu o karty inteligentne</p>	Bogdan Gacek	18-12-2024	09:00	12:00	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 16 Infrastruktura Klucza Publicznego Uwierzytelnianie dwuskładnikowe w oparciu o karty inteligentne	Bogdan Gacek	18-12-2024	12:00	14:00	02:00
9 z 16 Infrastruktura Klucza Publicznego Uwierzytelnianie dwuskładnikowe w oparciu o karty inteligentne	Bogdan Gacek	18-12-2024	14:00	17:00	03:00
10 z 16 Network Policy Server	Bogdan Gacek	19-12-2024	09:00	12:00	03:00
11 z 16 Network Policy Server	Bogdan Gacek	19-12-2024	12:00	14:00	02:00
12 z 16 Network Policy Server	Bogdan Gacek	19-12-2024	14:00	17:00	03:00
13 z 16 Analiza ruchu sieciowego Analiza bezpieczeństwa i hardening systemów	Bogdan Gacek	20-12-2024	09:00	12:00	03:00
14 z 16 Analiza ruchu sieciowego Analiza bezpieczeństwa i hardening systemów	Bogdan Gacek	20-12-2024	12:00	14:00	02:00
15 z 16 Analiza ruchu sieciowego Analiza bezpieczeństwa i hardening systemów	Bogdan Gacek	20-12-2024	14:00	17:00	03:00
16 z 16 Walidacja	-	20-12-2024	17:00	17:15	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 400,00 PLN
Koszt przypadający na 1 uczestnika netto	3 400,00 PLN
Koszt osobogodziny brutto	85,00 PLN
Koszt osobogodziny netto	85,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Bogdan Gacek

Autoryzowany Trener, posiadający wieloletnie doświadczenie / ponad 5 lat/ oraz wymaganą certyfikację popartą ukończonymi szkoleniami oraz zdanymi egzaminami.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autoryzowane materiały.

Warunki techniczne

Szkolenie odbywa się za pośrednictwem platformy **Microsoft Teams**.

Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 10Mb/s.
- urządzenie do obsługi audio - słuchawki/głośniki oraz mikrofon.
- zainstalowana dowolna przeglądarka internetowa - np. **Google Chrome**

Kontakt



Michał Dobrzański

E-mail michal.dobrzanski@compendium.pl

Telefon (+48) 122 984 777