Szkolenie: Microsoft

SC-500T00: Implement end-to-end security controls for cloud and AI workloads

Microsoft Partner

DOSTĘPNE TERMINY

2026-12-14 | 4 dni | Wirtualna sala

Cel szkolenia:

Dowiedz się, jak zabezpieczyć dostęp do zasobów platformy Azure przy użyciu usługi Microsoft Entra, wdrożyć zabezpieczenia typu defense-in-depth dla usługi Microsoft Key Vault i zapewnić zgodność z przepisami. Zagłęb się w najlepsze praktyki dotyczące zabezpieczeń w przypadku usługi Azure Storage, baz danych Azure SQL i środowisk sieciowych. Dowiedz się, jak zabezpieczać aplikacje sztucznej inteligencji przy użyciu usługi Microsoft Entra i Microsoft Defender for Cloud, zarządzać stanem zabezpieczeń oraz wdrażać rozwiązanie Microsoft Security Copilot. Chroń serwery, maszyny wirtualne i platformy aplikacji. Gromadź działania i zdarzenia w usłudze Microsoft Sentinel, aby utrzymać solidne operacje związane z bezpieczeństwem.

Profil odbiorców:
Jako kandydat do tego kursu jesteś inżynierem ds. bezpieczeństwa, który chroni systemy organizacyjne i dane w środowiskach chmurowych i hybrydowych poprzez wdrażanie kompleksowych kontroli bezpieczeństwa, które zapobiegają nieautoryzowanemu dostępowi i proaktywnie ograniczają ryzyko. Ta rola obejmuje wiele domen bezpieczeństwa, w tym tożsamość, sieć, aplikacje, dane i zasoby obliczeniowe. Ta rola zapewnia również, że platformy, dane, tożsamości i infrastruktura używane przez obciążenia sztucznej inteligencji są bezpiecznie wdrażane i monitorowane. Ściśle współpracujesz z architektami, administratorami, inżynierami, analitykami i programistami odpowiedzialnymi za platformę Azure, platformę Microsoft 365, tożsamość i dostęp, ochronę informacji, operacje związane z bezpieczeństwem, metodykę DevOps, tworzenie aplikacji, platformy baz danych i sieci.

Plan szkolenia:

- Zabezpieczanie dostępu do zasobów przy użyciu usługi Microsoft Entra
  - Moduł 1: Zarządzanie i wdrażanie metod uwierzytelniania w usłudze Microsoft Entra ID
  - Moduł 2: Wdrażanie i konfigurowanie usługi Privileged Identity Management (PIM)
  - Moduł 3: Zabezpieczanie agentów deklaratywnych i aplikacji AI za pomocą usługi Microsoft Entra
- Zabezpieczanie usługi Azure Key Vault za pomocą defense in depth dla chmury i obciążeń AI

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Moduł 1: Konfigurowanie i zabezpieczanie usługi Azure Key Vault
- Moduł 2: Zarządzanie kluczami i wpisami tajnymi w usłudze Azure Key Vault
- Moduł 3: Zarządzanie certyfikatami i monitorowanie usługi Azure Key Vault
- Moduł 4: Wykrywanie zagrożeń dla usługi Azure Key Vault przy użyciu Microsoft Defender for Cloud

- Wymuszanie ładu w zakresie bezpieczeństwa i zgodności z przepisami
  - Moduł 1: Wymuszanie ładu za pomocą usługi Azure Policy i blokad zasobów
  - Moduł 2: Konfigurowanie kontroli bezpieczeństwa i korygowanie zaleceń w Defender for Cloud
  - Moduł 3: Ocena zgodności z przepisami przy użyciu Microsoft Defender for Cloud
  - Moduł 4: Zarządzanie przypisaniami kontroli dostępu opartej na rolach na platformie Azure
  - Moduł 5: Ochrona danych na platformie Azure za pomocą usługi Azure Backup
  - Moduł 6: Osadzanie zabezpieczeń w potokach Bicep dla DevOps
- Wdrażanie zabezpieczeń dla usługi Azure Storage dla inżyniera ds. bezpieczeństwa chmury i AI
  - Moduł 1: Opisywanie usług magazynowania Azure
  - Moduł 2: Wdrażanie zabezpieczeń i zarządzanie dostępem dla usługi Azure Storage
  - Moduł 3: Konfigurowanie zabezpieczeń sieciowych dla usługi Azure Storage
  - Moduł 4: Wdrażanie usługi Microsoft Defender for Storage
- Wdrażanie zabezpieczeń dla baz danych Azure SQL
  - Moduł 1: Konfigurowanie zabezpieczeń na poziomie platformy dla bazy danych Azure SQL
  - Moduł 2: Konfigurowanie inspekcji dla usługi Azure SQL Database i wystąpienia zarządzanego SQL
  - Moduł 3: Wdrażanie usługi Microsoft Defender for Databases
- Wdrażanie kontroli bezpieczeństwa sieci na platformie Azure
  - Moduł 1: Segmentowanie i izolowanie obciążeń platformy Azure przy użyciu kontroli bezpieczeństwa sieci
  - Moduł 2: Centralizacja i wymuszanie inspekcji ruchu przy użyciu usługi Azure Firewall
  - Moduł 3: Zabezpieczanie łączności zdalnej i wdrażanie usługi Microsoft Entra Private Access
  - Moduł 4: Eliminowanie ekspozycji publicznych punktów końcowych za pomocą usługi Private Link
- Wdrażanie zabezpieczeń dla AI
  - Moduł 1: Zabezpieczanie dostępu dla tożsamości agenta Microsoft Entra
  - Moduł 2: Analiza ryzyka związanego z tożsamościami AI za pomocą usługi Microsoft Defender XDR
  - Moduł 3: Włączanie ochrony dla agentów Copilot Studio za pomocą usługi Microsoft Defender for Cloud Apps

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Moduł 4: Zabezpieczanie ruchu modeli AI za pomocą bramy AI Gateway
- Moduł 5: Konfigurowanie i zarządzanie barierami ochronnymi w Microsoft Foundry
- Moduł 6: Ochrona obciążeń AI przy użyciu usługi Microsoft Defender for Cloud
- Moduł 7: Zarządzanie agentami Agent 365 przy użyciu usługi Microsoft Agent 365
- Moduł 8: Odkrywanie i ocena ryzyka danych AI za pomocą DSPM for AI
- Moduł 9: Zarządzanie zgodnością i przechowywaniem danych AI

- Wdrażanie zabezpieczeń dla serwerów i maszyn wirtualnych
  - Moduł 1: Wdrażanie szyfrowania dysków dla maszyn wirtualnych platformy Azure
  - Moduł 2: Konfigurowanie funkcji zabezpieczeń zaufanego uruchamiania dla maszyn wirtualnych platformy Azure
  - Moduł 3: Planowanie i wdrażanie usługi Azure Bastion
  - Moduł 4: Zarządzanie zabezpieczeniami serwerów hybrydowych z obsługą usługi Arc
  - Moduł 5: Wdrażanie usługi Microsoft Defender for Servers
  - Moduł 6: Wdrażanie dostępu typu just-in-time do maszyn wirtualnych
  - Moduł 7: Konfigurowanie konfiguracji maszyn na platformie Azure pod kątem punktów odniesienia zabezpieczeń systemu operacyjnego
- Zabezpieczanie usług platformy aplikacji Azure dla inżyniera ds. bezpieczeństwa chmury i AI
  - Moduł 1: Wykrywanie ryzyka związanego z kontenerami przy użyciu usługi Microsoft Defender for Containers
  - Moduł 2: Wdrażanie kontroli bezpieczeństwa dla usługi Azure Kubernetes Service
  - Moduł 3: Wdrażanie zabezpieczeń dla usługi Azure Container Registry
  - Moduł 4: Zabezpieczanie usług Azure Functions i Logic Apps
  - Moduł 5: Zabezpieczanie usług Azure App Services i Web Application Firewall
  - Moduł 6: Zabezpieczanie usługi Azure API Management
- Zarządzanie stanem zabezpieczeń przy użyciu rozwiązania Microsoft Defender for Cloud
  - Moduł 1: Łączenie środowisk hybrydowych i wielochmurowych z usługą Microsoft Defender for Cloud
  - Moduł 2: Identyfikacja ryzyka bezpieczeństwa przy użyciu funkcji zarządzania stanem zabezpieczeń w chmurze
  - Moduł 3: Odkrywanie zewnętrznych powierzchni ataku i zarządzanie nimi za pomocą usługi Microsoft Defender EASM
  - Moduł 4: Ocena zgodności z przepisami przy użyciu usługi Microsoft Defender for Cloud
  - Moduł 5: Włączanie i konfigurowanie planów ochrony obciążeń w usłudze Microsoft Defender for Cloud
  - Moduł 6: Wdrażanie funkcji zarządzania podatnościami w usłudze Microsoft Defender
- Wdrażanie zbierania aktywności i zdarzeń w usłudze Microsoft Sentinel
  - Moduł 1: Tworzenie obszarów roboczych usługi Microsoft Sentinel i zarządzanie nimi
  - Moduł 2: Zarządzanie zawartością w usłudze Microsoft Sentinel

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Moduł 3: Łączenie usług firmy Microsoft z usługą Microsoft Sentinel
- Moduł 4: Zbieranie zdarzeń zabezpieczeń systemu Windows przy użyciu reguł zbierania danych
- Moduł 5: Zbieranie danych systemu Linux i dziennika systemowego za pomocą reguł zbierania danych
- Moduł 6: Wdrażanie zautomatyzowanego reagowania na zagrożenia za pomocą podręczników (playbooks)
- Moduł 7: Zarządzanie przechowywaniem i archiwizacją danych w usłudze Microsoft Sentinel
- Moduł 8: Zabezpieczanie dostępu do dzienników inspekcji w usłudze Microsoft Sentinel

- Wdrażanie i obsługa rozwiązania Microsoft Security Copilot
  - Moduł 1: Opisanie usługi Microsoft Security Copilot
  - Moduł 2: Konfigurowanie obszarów roboczych dla usługi Microsoft Security Copilot
  - Moduł 3: Zarządzanie agentami i wtyczkami usługi Security Copilot

Wymagania:

- Praktyczne doświadczenie w administracji platformą Microsoft Azure i środowiskami hybrydowymi, w tym zasobami obliczeniowymi, siecią i pamięcią masową
- Dobra znajomość usługi Microsoft Entra ID
- Znajomość administracji platformą Microsoft 365
- Praktyczna wiedza na temat usług Azure Key Vault, Azure Policy, Azure RBAC
- Znajomość rozwiązania Microsoft Defender for Cloud na poziomie podstawowym
- Zrozumienie koncepcji sieciowych platformy Azure, w tym sieci wirtualnych, podsieci i prywatnych punktów końcowych
- Doświadczenie w posługiwaniu się językiem Kusto Query Language (KQL) i obszarami roboczymi usługi Log Analytics

Poziom trudności



Certyfikaty:

Uczestnicy otrzymają certyfikaty podpisane przez Microsoft (ukończenie kursu).

Ten kurs pomoże w przygotowaniu do certyfikacji **Microsoft Certified: Cloud and AI Security Engineer Associate (beta)**, która jest dostępna w centrach egzaminacyjnych Pearson VUE.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Prowadzący:

Microsoft Certified Trainer (MCT)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001