Szkolenie: Microsoft
Azure Security Bootcamp

Microsoft Partner

Cel szkolenia:

To szkolenie jest połączeniem kursów **SC-900T00: Introduction to Microsoft Security, Compliance, and Identity** i **SC-200T00: Defend against cyberthreats with Microsoft's security operations platform**.

Dowiedz się, jak badać zagrożenia, reagować na nie i polować na nie przy użyciu usługi Microsoft Sentinel, Microsoft Defender XDR i Microsoft Defender dla Chmury. W tym kursie dowiesz się, jak ograniczać cyberzagrożenia przy użyciu tych technologii. W szczególności skonfigurujesz i użyjesz usługi Microsoft Sentinel, a także użyjesz języka Kusto Query Language (KQL) do przeprowadzania wykrywania, analizy i raportowania. Kurs został zaprojektowany dla osób pracujących na stanowisku analityka operacji zabezpieczeń (Security Operations) i pomaga uczestnikom przygotować się do egzaminu SC-200: Microsoft Security Operations Analyst.

Profil odbiorców:
Analityk operacji zabezpieczeń Microsoft współpracuje z interesariuszami w organizacji w celu zabezpieczenia systemów informatycznych. Celem jest zmniejszenie ryzyka organizacyjnego poprzez szybkie korygowanie aktywnych ataków w środowisku, doradzanie w zakresie ulepszania praktyk ochrony przed zagrożeniami oraz przekazywanie informacji o naruszeniach zasad organizacyjnych odpowiednim stronom. Obowiązki obejmują zarządzanie zagrożeniami, monitorowanie i reagowanie na nie przy użyciu różnych rozwiązań zabezpieczeń w całym środowisku. Rola ta polega przede wszystkim na badaniu, reagowaniu i polowaniu na zagrożenia przy użyciu usług Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender dla Chmury i produktów zabezpieczających innych firm.

Umiejętności zdobyte po ukończeniu:

- Zarządzanie łagodzeniem zagrożeń przy użyciu usługi Microsoft Defender XDR
- Zarządzanie łagodzeniem zagrożeń przy użyciu usługi Microsoft Purview
- Zarządzanie łagodzeniem zagrożeń przy użyciu usługi Microsoft Defender for Endpoint
- Zarządzanie łagodzeniem zagrożeń przy użyciu usługi Microsoft Defender for Cloud
- Tworzenie zapytań KQL dla usługi Microsoft Sentinel
- Konfigurowanie środowiska w usłudze Microsoft Sentinel
- Zarządzanie połączeniem dzienników z usługą 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

- Wykrywanie zagrożeń i reagowanie na nie przy użyciu usługi Microsoft Sentinel
- Zarządzanie wyszukiwaniem zagrożeń w usłudze Microsoft Sentinel

Plan szkolenia:

- Wprowadzenie do pojęć związanych z bezpieczeństwem, zgodnością i tożsamością
  - Moduł 1: Opisanie koncepcji z zakresu bezpieczeństwa i zgodności
  - Moduł 2: Opisanie koncepcji związanych z tożsamościami
- Wprowadzenie do usługi Microsoft Entra
  - Moduł 1: Opisanie funkcji i typów tożsamości w usłudze Microsoft Entra ID
  - Moduł 2: Opisanie możliwości uwierzytelniania w usłudze Microsoft Entra ID
  - Moduł 3: Opisanie możliwości zarządzania dostępem w usłudze Microsoft Entra
  - Moduł 4: Opisanie możliwości ochrony tożsamości i ładu w usłudze Microsoft Entra
- Wprowadzenie do rozwiązań z zakresu zabezpieczeń firmy Microsoft
  - Moduł 1: Opisanie usługi Microsoft Security Copilot
  - Moduł 2: Opisanie podstawowych usług infrastruktury zabezpieczeń na platformie Azure
  - Moduł 3: Opisanie możliwości zarządzania zabezpieczeniami na platformie Azure
  - Moduł 4: Opisanie możliwości ochrony zapewnianych przez usługę Microsoft Sentinel
  - Moduł 5: Opisanie ochrony przed zagrożeniami przy użyciu usługi Microsoft Defender XDR
- Wprowadzenie do rozwiązania Microsoft Purview i zasad ochrony prywatności firmy Microsoft
  - Moduł 1: Opisywanie portalu zaufania do usług (Service Trust Portal) i zasad ochrony prywatności firmy Microsoft
  - Moduł 2: Opisywanie rozwiązań zabezpieczeń danych z rodziny Microsoft Purview
  - Moduł 3: Opisywanie rozwiązań zgodności danych z rodziny Microsoft Purview
  - Moduł 4: Opisywanie rozwiązań ładu danych z rodziny Microsoft Purview
- Łagodzenie zagrożeń przy użyciu usługi Microsoft Defender XDR
  - Moduł 1: Wprowadzenie do ochrony przed zagrożeniami w usłudze Microsoft Defender XDR
  - Moduł 2: Łagodzenie zdarzeń przy użyciu usługi Microsoft Defender
  - Moduł 3: Reagowanie na zagrożenia przy użyciu usługi Microsoft Defender
  - Moduł 4: Zarządzanie usługą Microsoft Entra Identity Protection
  - Moduł 5: Zabezpieczanie aplikacji i usług w chmurze za pomocą usługi Microsoft Defender for Cloud Apps
  - Moduł 6: Zarządzanie usługą Microsoft Defender for Office 365

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

- Łagodzenie zagrożeń przy użyciu rozwiązania Microsoft Security Copilot
  - Moduł 1: Wprowadzenie do generatywnej sztucznej inteligencji i agentów
  - Moduł 2: Opisywanie rozwiązania Microsoft Security Copilot
  - Moduł 3: Opisywanie podstawowych funkcji rozwiązania Microsoft Security Copilot
  - Moduł 4: Opisywanie wbudowanych środowisk rozwiązania Microsoft Security Copilot
  - Moduł 5: Poznaj rozwiązanie Security Copilot za pomocą symulacji z przewodnikiem
- Łagodzenie zagrożeń przy użyciu usługi Microsoft Purview
  - Moduł 1: Badanie alertów dotyczących ochrony przed utratą danych w usłudze Microsoft Purview i reagowanie na nie
  - Moduł 2: Badanie alertów o ryzyku wewnętrznym i powiązanych z nimi działań
  - Moduł 3: Wyszukiwanie i badanie za pomocą funkcji Audit (Wersja Premium) usługi Microsoft Purview
  - Moduł 4: Wyszukiwanie zawartości przy użyciu zbierania elektronicznych materiałów dowodowych w usłudze Microsoft Purview
- Łagodzenie zagrożeń przy użyciu usługi Microsoft Defender for Endpoint
  - Moduł 1: Ochrona przed zagrożeniami za pomocą usługi Microsoft Defender for Endpoint
  - Moduł 2: Wdrażanie środowiska usługi Microsoft Defender for Endpoint
  - Moduł 3: Wdrażanie ulepszeń zabezpieczeń systemu Windows za pomocą usługi Microsoft Defender for Endpoint
  - Moduł 4: Przeprowadzanie badań urządzeń w usłudze Microsoft Defender for Endpoint
  - Moduł 5: Wykonywanie akcji na urządzeniu przy użyciu usługi Microsoft Defender for Endpoint
  - Moduł 6: Przeprowadzanie badań dowodów i jednostek przy użyciu usługi Microsoft Defender for Endpoint
  - Moduł 7: Konfigurowanie automatyzacji i zarządzanie nią przy użyciu usługi Microsoft Defender for Endpoint
  - Moduł 8: Konfigurowanie alertów i wykrywania w usłudze Microsoft Defender for Endpoint
  - Moduł 9: Korzystanie z funkcji Vulnerability Management w usłudze Microsoft Defender for Endpoint
- Łagodzenie zagrożeń przy użyciu usługi Microsoft Defender for Cloud
  - Moduł 1: Planowanie ochrony obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud
  - Moduł 2: Łączenie zasobów platformy Azure z usługą Microsoft Defender for Cloud
  - Moduł 3: Łączenie zasobów spoza platformy Azure z usługą Microsoft Defender for Cloud
  - Moduł 4: Zarządzanie stanem zabezpieczeń w chmurze
  - Moduł 5: Objaśnianie ochrony obciążeń w chmurze w usłudze Microsoft Defender for Cloud
  - Moduł 6: Rozwiązywanie problemów z alertami zabezpieczeń przy użyciu usługi Microsoft Defender for Cloud

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

- Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu języka Kusto Query Language (KQL)
  - Moduł 1: Konstruowanie instrukcji KQL dla usługi Microsoft Sentinel
  - Moduł 2: Analizowanie wyników zapytań przy użyciu języka KQL
  - Moduł 3: Tworzenie instrukcji wielotabelowych przy użyciu języka KQL
  - Moduł 4: Praca z danymi w usłudze Microsoft Sentinel przy użyciu języka Kusto Query Language
- Konfigurowanie środowiska usługi Microsoft Sentinel
  - Moduł 1: Wprowadzenie do usługi Microsoft Sentinel
  - Moduł 2: Tworzenie obszarów roboczych usługi Microsoft Sentinel i zarządzanie nimi
  - Moduł 3: Tworzenie zapytań w dziennikach w usłudze Microsoft Sentinel
  - Moduł 4: Używanie list obserwowanych w usłudze Microsoft Sentinel
  - Moduł 5: Wykorzystanie analizy zagrożeń w usłudze Microsoft Sentinel
  - Moduł 6: Integrowanie usługi Microsoft Defender XDR z usługą Microsoft Sentinel
- Łączenie dzienników z usługą Microsoft Sentinel
  - Moduł 1: Łączenie danych z usługą Microsoft Sentinel przy użyciu łączników danych
  - Moduł 2: Podłączanie usług firmy Microsoft do usługi Microsoft Sentinel
  - Moduł 3: Łączenie usługi Microsoft Defender XDR z usługą Microsoft Sentinel
  - Moduł 4: Łączenie hostów systemu Windows z usługą Microsoft Sentinel
  - Moduł 5: Łączenie dzienników Common Event Format z usługą Microsoft Sentinel
  - Moduł 6: Łączenie źródeł danych dziennika systemowego z usługą Microsoft Sentinel
  - Moduł 7: Podłączanie wskaźników zagrożeń do usługi Microsoft Sentinel
- Tworzenie wykrywania i przeprowadzanie badań przy użyciu usługi Microsoft Sentinel
  - Moduł 1: Wykrywanie zagrożeń za pomocą analizy w usłudze Microsoft Sentinel
  - Moduł 2: Automatyzacja w usłudze Microsoft Sentinel
  - Moduł 3: Reagowanie na zagrożenia za pomocą przewodników w usłudze Microsoft Sentinel
  - Moduł 4: Zarządzanie zdarzeniami związanymi z bezpieczeństwem w usłudze Microsoft Sentinel
  - Moduł 5: Identyfikowanie zagrożeń przy użyciu analizy behawioralnej
  - Moduł 6: Normalizacja danych w usłudze Microsoft Sentinel
  - Moduł 7: Tworzenie zapytań, wizualizowanie i monitorowanie danych w usłudze Microsoft Sentinel
  - Moduł 8: Zarządzanie zawartością w usłudze Microsoft Sentinel
- Wykonywanie wyszukiwania zagrożeń w usłudze Microsoft Sentinel
  - Moduł 1: Objaśnianie koncepcji wyszukiwania zagrożeń w usłudze Microsoft Sentinel
  - Moduł 2: Wyszukiwanie zagrożeń za pomocą usługi Microsoft Sentinel
  - Moduł 3: Korzystanie z zadań wyszukiwania 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 4: Poszukiwanie zagrożeń przy użyciu notesów w usłudze Microsoft Sentinel

Wymagania:

- Podstawowa wiedza na temat produktów Microsoft dotyczących zabezpieczeń, zgodności i tożsamości
- Podstawowa wiedza na temat usługi Microsoft Defender XDR
- Znajomość usług platformy Azure, w szczególności usługi Azure SQL Database i usługi Azure Storage (dla ścieżki szkoleniowej 5)
- Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych (dla ścieżki szkoleniowej 5)
- Podstawowa wiedza o sieciach komputerowych
- Zrozumienie użycia języka KQL w usłudze Microsoft Sentinel

Poziom trudności



Certyfikaty:

Uczestnicy otrzymają certyfikaty podpisane przez Microsoft (ukończenie kursu).

Ten kurs pomoże w przygotowaniu do egzaminu certyfikującego **Microsoft Certified: Security, Compliance, and Identity Fundamentals** (Egzamin SC-900) oraz do egzaminu certyfikującego **Microsoft Certified: Security Operations Analyst Associate** (Egzamin SC-200), oba są dostępne w centrach egzaminacyjnych Pearson VUE.

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