Szkolenie: Microsoft
SC-200T00 Microsoft Security Operations Analyst

Gold Microsoft Partner

Cel szkolenia:

Uczestnicy tego szkolenia dowiedzą się, jak badać zagrożenia, reagować i pozbywać się ich za pomocą usługi Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Podczas szkolenia, omówione zostaną sposoby ograniczania zagrożenia cybernetycznego za pomocą tych technologii, w szczególności jak skonfigurować i używać usługę Azure Sentinel, a także korzystać z języka KQL (Kusto Query Language) do wykrywania, analizowania i raportowania. Szkolenie zostało zaprojektowane dla osób, które chcą się przygotować do egzaminu SC-200: Microsoft Security Operations Analyst.

Po ukończeniu szkolenia, uczestnik będzie potrafił:

- Wyjaśnić, w jaki sposób program Microsoft Defender może korygować zagrożenia w danym środowisku
- Tworzyć środowisko usługi Microsoft Defender
- Konfigurować reguły Attack Surface Reduction na urządzeniach z systemem Windows 10
- Wykonywać czynności na urządzeniu przy użyciu usługi Microsoft Defender
- Badać domeny i adresy IP w usłudze Microsoft Defender
- Badać konta użytkowników w usłudze Microsoft Defender
- Konfigurować ustawienia alertów w usłudze Microsoft Defender
- Wyjaśnić, jak rozwijają się zagrożenia cybernetyczne
- Prowadzić zaawansowane operacje neutralizacji zagrożeń w usłudze Microsoft 365 Defender
- Zarządzać zdarzeniami w usłudze Microsoft 365 Defender
- Wyjaśnić, jak usługa Microsoft Defender for Identity może korygować zagrożenia w danym środowisku.
- Badać alerty DLP w usłudze Microsoft Cloud App Security
- Wyjaśnić różne rodzaje działań, które można podjąć w przypadku zarządzania ryzykiem poufnym.
- Konfigurować automatyczne inicjowanie obsługi administracyjnej w usłudze Azure Defender
- Korygować alerty w usłudze Azure Defender
- Konstruować instrukcje KQL
- Filtrować wyszukiwanie na podstawie czasu zdarzenia, priorytetu, domeny i innych istotnych danych przy użyciu funkcji KQL
- Wyodrębniać dane z nieustrukturyzowanych pól ciągów przy użyciu funkcji KQL

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Zarządzać obszarem roboczym usługi Azure Sentinel
- Konfigurować dostęp do listy obserwowanych w usłudze Azure Sentinel za pomocą funkcji KQL
- Zarządzać wskaźnikami zagrożeń w usłudze Azure Sentinel
- Wyjaśnić różnice w formacie typowym i łączniku Syslog w usłudze Azure Sentinel
- Łączyć maszyny wirtualne systemu Azure z usługą Azure Sentinel
- Konfigurować agenta usługi Log Analytics do zbierania zdarzeń Sysmon
- Tworzyć nowe reguły i zapytania analityczne za pomocą kreatora reguł analizy
- Tworzyć zasady działania w celu automatyzacji reagowania na incydenty
- Używać zapytania do pozbywania się zagrożeń
- Monitorować zagrożenia w czasie za pomocą transmisji na żywo

Grupa docelowa:

Security Operations Analyst współpracuje z zainteresowanymi stronami organizacyjnymi w celu zabezpieczenia systemów informatycznych w firmie. Ich celem jest zmniejszenie ryzyka organizacyjnego poprzez szybkie korygowanie aktywnych ataków w środowisku, doradzanie w zakresie ulepszeń praktyk ochrony przed zagrożeniami i kierowanie naruszeń zasad organizacyjnych do odpowiednich zainteresowanych stron. Obowiązki obejmują zarządzanie zagrożeniami, monitorowanie i reagowanie przy użyciu różnych rozwiązań zabezpieczeń w całym środowisku. Rola dotyczy przede wszystkim pozbywania się zagrożeń korzystając z usługi Microsoft Azure Sentinel, Azure Defender, Usługi Microsoft 365 Defender i produktów zabezpieczeń innych firm. Ponieważ Security Operations Analyst zużywa dane wyjściowe operacyjne tych narzędzi, są one również kluczowym elementem w konfiguracji i wdrażaniu tych technologii.

Plan szkolenia:

- Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Endpoint
  - Ochrona przed zagrożeniami za pomocą programu Microsoft Defender for Endpoint
  - Wdrażanie środowiska usługi Microsoft Defender for Endpoint
  - Wdrażanie ulepszeń zabezpieczeń systemu Windows 10 za pomocą usługi Microsoft Defender for Endpoint
  - Zarządzanie alertami i zdarzeniami w usłudze Microsoft Defender for Endpoint
  - Wykonywanie dochodzeń dotyczących urządzeń w usłudze Microsoft Defender for Endpoint
  - Wykonywanie akcji na urządzeniu przy użyciu usługi Microsoft Defender for Endpoint
  - Wykonywanie dochodzeń w sprawie dowodów i jednostek przy użyciu usługi Microsoft Defender for Endpoint
  - Konfigurowanie automatyzacji i zarządzanie nią przy użyciu usługi Microsoft Defender for Endpoint
  - Konfigurowanie alertów i wykrywania w usłudze Microsoft Defender for Endpoint
  - Korzystanie z zarządzania zagrożeniami i lukami w zabezpieczeniach w programie

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

Microsoft Defender for Endpoint

- Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender
  - Wprowadzenie do ochrony przed zagrożeniami dzięki usłudze Microsoft 365
  - Ograniczanie zdarzeń przy użyciu usługi Microsoft 365 Defender
  - Ochrona tożsamości za pomocą usługi Azure AD Identity Protection
  - Korygowanie ryzyka związanego z programem Microsoft Defender dla usługi Office 365
  - Ochrona środowiska dzięki usłudze Microsoft Defender for Identity
  - Zabezpieczanie aplikacji i usług w chmurze za pomocą programu Microsoft Cloud App Security
  - Reagowanie na alerty dotyczące zapobiegania utracie danych przy użyciu usługi Microsoft 365
  - Zarządzanie ryzykiem niejawne informacji poufnych w usłudze Microsoft 365
- Ograniczanie zagrożeń przy użyciu usługi Azure Defender
  - Planowanie zabezpieczeń obciążeń w chmurze przy użyciu usługi Azure Defender
  - Wyjaśnianie zabezpieczenia obciążeń w chmurze w usłudze Azure Defender
  - Łączenie zasobów platformy Azure z usługą Azure Defender
  - Łączenie zasobów innych niż platforma Azure z usługą Azure Defender
  - Korygowanie alertów zabezpieczeń przy użyciu usługi Azure Defender
- Tworzenie zapytań dla usługi Azure Sentinel przy użyciu języka KQL (Kusto Query Language)
  - Konstruowanie instrukcji KQL dla usługi Azure Sentinel
  - Analizowanie wyników kwerend przy użyciu funkcji KQL
  - Tworzenie instrukcji wielospajowych przy użyciu funkcji KQL
  - Praca z danymi w usłudze Azure Sentinel przy użyciu języka zapytań Kusto
- Konfigurowanie środowiska wartownicze platformy Azure
  - Wprowadzenie do usługi Azure Sentinel
  - Tworzenie obszarów roboczych usługi Azure Sentinel i zarządzanie nimi
  - Dzienniki zapytań w usłudze Azure Sentinel
  - Używanie list obserwowanych w usłudze Azure Sentinel
  - Korzystanie z analizy zagrożeń w usłudze Azure Sentinel
- Łączenie dzienników z usługą Azure Sentinel
  - Łączenie danych z usługą Azure Sentinel przy użyciu łączników danych
  - Łączenie usług firmy Microsoft z usługą Azure Sentinel
  - Łączenie usługi Microsoft 365 Defender z usługą Azure Sentinel
  - Łączenie hostów systemu Windows z usługą Azure Sentinel
  - Łączenie dzienników wspólnego formatu zdarzeń z usługą Azure Sentinel
  - Łączenie źródeł danych syslogu z usługą Azure Sentinel
  - Łączenie wskaźników zagrożeń z usługą Azure Sentinel

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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 wykrywania i przeprowadzanie dochodzeń przy użyciu usługi Azure Sentinel
  - Wykrywanie zagrożeń za pomocą analizy azure sentinel
  - Reagowanie na zagrożenia za pomocą podręczników Azure Sentinel
  - Zarządzanie zdarzeniami zabezpieczeń w usłudze Azure Sentinel
  - Korzystanie z analizy zachowania jednostki w usłudze Azure Sentinel
  - Wysyłaj zapytania, wizualizuj i monitoruj dane w usłudze Azure Sentinel
- Neutralizacja zagrożeń w usłudze Azure Sentinel
  - Polowanie na zagrożenia za pomocą usługi Azure Sentinel
  - Polowanie na zagrożenia przy użyciu notesów w usłudze Azure Sentinel

Wymagania:

Przed uczestnictwem w tym szkoleniu, uczestnicy muszą posiadać:

- Podstawową wiedzę o usłudze Microsoft 365
- Podstawowe rozumienie zabezpieczeń, zgodności i tożsamości produktów firmy Microsoft
- Ogólne rozumienie systemu Windows 10
- Znajomość usług platformy Azure, w szczególności usługi Azure SQL Database i usługi Azure Storage
- Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych
- Podstawową wiedzę na temat pojęć skryptów.

Poziom trudności

Certyfikaty:

Certyfikat ukończenia autoryzowanego szkolenia Microsoft.

Prowadzący:

Certyfikowany trener Microsoft.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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