Możliwość dofinansowania

Szkolenie SC-200T00 Microsoft Security Operations Analyst

Numer usługi 2024/05/14/142469/2148380

4 255,80 PLN brutto
3 460,00 PLN netto
151,99 PLN brutto/h
123,57 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
28.10.2024 do 31.10.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie jest skierowane do osób, które chcą zdobyć wiedzę z zakresu badania zagrożeń, odpowiadania na nie i ich wyszukowania za pomocą platformy Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Kurs jest przeznaczony dla inżynierów IT, którzy będą odpowiedzialni na łagodzenie cyberzagrożeń za pomocą tych technologii, którzy będą zajmowali się konfiguracją i korzystaniem z Azure Sentinel, będą używali języka Kusto Query Language (KQL) do wykrywania, analizy i raportowania. Kurs został zaprojektowany z myślą o osobach, które pracują na stanowisku Security Operations i pomaga uczestnikom przygotować się do egzaminu SC-200: Microsoft Security Operations Analyst.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	14-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28
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

Usługa przygotowuje Uczestnika do ograniczania zagrożeń przy wykorzystaniu z usługi Microsoft 365 Defender dla punktów końcowych oraz dla chmury, do tworzenia zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language (KQL), konfigurowania środowiska Microsoft Sentinel, łączenia dzienników z Microsoft Sentinel, tworzenia, wykrywania i przeprowadzania dochodzenia za pomocą programu Microsoft Sentinel oraz do wyszukiwania zagrożeń w Microsoft Sentinel.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
- ogranicza zagrożenia dla punktów końcowych i dla chmury przy wykorzystaniu z usługi Microsoft 365 Defender, - tworzy zapytania dla Microsoft Sentinel przy użyciu języka Kusto Query Language (KQL), - konfiguruje środowisko Microsoft Sentinel, - łączy dzienniki z Microsoft Sentinel,	Pre-test Post-test	Test teoretyczny
		Test teoretyczny
- tworzy, wykrywa i przeprowadza dochodzenia za pomocą programu Microsoft Sentinel - wyszukuje zagrożenia w Microsoft Sentinel.	Pre-test Post-test	Test teoretyczny
		Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, Uczestnik szkolenia, poza certyfikatem, otrzymuje zaświadczenie o ukończeniu szkolenia z zawartym opisem efektów uczenia się.

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

Szkolenie **SC-200T00 Microsoft Security Operations Analyst** jest przeznaczone dla analityków IT którzy chcą zdobyć wiedzę z zakresu badania zagrożeń, odpowiadania na nie oraz ich wyszukowania za pomocą platformy Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Kurs jest przeznaczony dla inżynierów IT, którzy będą odpowiedzialni na łagodzenie cyberzagrożeń za pomocą tych technologii, którzy będą zajmowali się konfiguracją i korzystaniem z Azure Sentinel, będą używali języka Kusto Query Language (KQL) do wykrywania, analizy i raportowania. Kurs został zaprojektowany z myślą o osobach, które pracują na stanowisku Security Operations i pomaga uczestnikom przygotować się do egzaminu SC-200: Microsoft Security Operations Analyst.

W celu przystąpienia do szkolenia Uczestnik powinien znać w stopniu podstawowym platformę Microsoft 365, produkty firmy Microsoft związane z zabezpieczeniami, zgodnością i tożsamością. Powinien również posiadać znajomość systemu Windows 10, usług platformy Azure, w szczególności Azure SQL Database i Azure Storage, maszyn wirtualnych platformy Azure i sieci wirtualnych. Uczestnik powinien również rozumieć podstawowe pojęcia związane ze skryptami.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy Uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności. W trakcie szkolenia omawiane jest również studium przypadków, w którym Uczestnicy wspólnie wymieniają się doświadczeniami. Nad case-study czuwa autoryzowany Trener, który przekazuje informację na temat przydatnych narzędzi oraz najlepszych praktyk do rozwiązania omawianego zagadnienia.

Aby Uczestnik osiągnął zamierzony cel szkolenia niezbędne jest wykonanie przez niego zadanych laboratoriów. Pomocne będzie również ugruntowanie wiedzy i wykonywanie ćwiczeń po zakończonej usłudze. Każdy Uczestnik dysponuje dostępem do laboratoriów przez okres 180 dni.

Szkolenie trwa 32 godziny dydaktyczne, realizowane w ciągu 4 następujących po sobie dni.
W trakcie każego dnia szkolenia przewidziane są dwie krótkie przerwy "kawowe" oraz przerwa lunchowa.

Program szkolenia:

Wprowadzenie do ochrony przed zagrożeniami na platformie Microsoft 365

Ograniczanie incydentów przy użyciu usługi Microsoft 365 Defender

Ochrona tożsamości za pomocą usługi Azure AD Identity Protection

Eliminowanie zagrożeń za pomocą usługi Microsoft Defender dla usługi Office 365

Ochrona infrastruktury dzięki usłudze Microsoft Defender for Identity

Zabezpieczanie aplikacji i usług w chmurze dzięki usłudze Microsoft Defender w Cloud Apps

Reagowanie na alerty dotyczące zapobiegania utracie danych przy użyciu platformy Microsoft 365

Zarządzanie ryzykiem wewnętrznym w usłudze Microsoft Purview

Badanie zagrożeń przy użyciu funkcji inspekcji w usługach Microsoft 365 Defender i Microsoft Purview Standard

Badanie zagrożeń przy użyciu inspekcji w usługach Microsoft 365 Defender i Microsoft Purview (Premium)

Badanie zagrożeń za pomocą funkcji wyszukiwania zawartości w usłudze Microsoft Purview

Ochrona przed zagrożeniami za pomocą usługi Microsoft Defender for Endpoint

Wdrażanie Microsoft Defender dla punktów końcowych

Wdrażanie ulepszeń zabezpieczeń systemu Windows za pomocą programu Microsoft Defender Endpoint

Przeprowadzanie badań urządzenia w programie Microsoft Defender w Endpoint

Wykonywanie działań na urządzeniu przy użyciu usługi Microsoft Defender w Endpoint

Wykonywanie analiz elementów i podmiotów przy użyciu usługi Microsoft Defender for Endpoint

Konfigurowanie automatyzacji i zarządzanie nią przy użyciu programu Microsoft Defender for Endpoint

Konfigurowanie alertów i wykrywania w usłudze Microsoft Defender w Microsoft Defender for Endpoint

Wykorzystanie zarządzania podatnościami na zagrożenia w usłudze Microsoft Defender Endpoint

Planowanie ochrony obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud

Podłączanie elementów Azure do usługi Microsoft Defender for Cloud

Łączenie elementów spoza platformy Azure z usługą Microsoft Defender for Cloud

Zarządzanie poziomem zabezpieczeń w chmurze

Wyjaśnienie ochrony obciążeń w chmurze w usłudze Microsoft Defender for Cloud

Korygowanie alertów zabezpieczeń przy użyciu usługi Microsoft Defender for Cloud

Konstruowanie instrukcji KQL dla usługi Microsoft Sentinel

Analizowanie wyników zapytań przy użyciu języka KQL

Tworzenie instrukcji wielu tabel przy użyciu języka KQL

Praca z danymi w usłudze Microsoft Sentinel przy użyciu języka zapytań Kusto

Wprowadzenie do Microsoft Sentinel

Tworzenie obszarów roboczych Microsoft Sentinel i zarządzanie nimi

Rejestry zapytań w Microsoft Sentinel

Używanie obserwowanych list w Microsoft Sentinel

Wykorzystywanie analizy zagrożeń w usłudze Microsoft Sentinel

Podłączanie danych do platformy Microsoft Sentinel przy użyciu łączników danych

Nawiązywanie połączeń między usługami firmy Microsoft a usługą Microsoft Sentinel

Nawiązywanie połączenia między usługą Microsoft 365 Defender a usługą Microsoft Sentinel

Łączenie hostów Windows z usługą Microsoft Sentinel

Połączenie logów Common Event Format z usługą Microsoft Sentinel

Możliwość łączenia źródeł danych syslog z usługą Microsoft Sentinel

Łączenie z programem Microsoft Sentinel wskaźników zagrożeń

Wykrywanie zagrożeń za pomocą analizy Microsoft Sentinel

Automatyzacja w Microsoft Sentinel

Zarządzanie incydentami bezpieczeństwa w Microsoft Sentinel

Identyfikowanie zagrożeń za pomocą analizy behawioralnej

Normalizacja danych w usłudze Microsoft Sentinel

Zapytania, wizualizacja i monitorowanie danych w usłudze Microsoft Sentinel

Zarządzanie zawartością w usłudze Microsoft Sentinel

Wyjaśnienie koncepcji wykrywania zagrożeń w usłudze Microsoft Sentinel

Wykrywanie zagrożeń za pomocą Microsoft Sentinel

Używanie zadań wyszukiwania w usłudze Microsoft Sentinel

Wyszukiwanie zagrożeń przy użyciu notesów w usłudze Microsoft Sentinel

SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezebrania się minimalnej liczby Uczestników tj. 3 osób.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 255,80 PLN
Koszt przypadający na 1 uczestnika netto	3 460,00 PLN
Koszt osobogodziny brutto	151,99 PLN
Koszt osobogodziny netto	123,57 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Patryk Łączny

Patryk Łączny – Microsoft Certified Trainer. Absolwent Politechniki Poznańskiej ze specjalnością Matematyczne Metody Informatyki. Zdobył m.in. certyfikaty: Microsoft Certified Professional, Microsoft® Certified Solutions Associate, Microsoft Office Specialist, Microsoft Certified Systems Engineer, Microsoft® Certified IT Professional, Microsoft® Certified Technology Specialist Microsoft Certified Trainer oraz certyfikat ECDL. Specjalizuje się w prowadzeniu szkoleń z zakresu aplikacji Microsoft Office, Exchange, SharePoint, Windows Server, Office 365, które prowadzi w SOFTRONIC od 2006 roku. Posiada uprawnienia pedagogiczne. W zewnętrznym systemie ewaluacji szkoleń Metrics That Matter uzyskał wysoką średnią notę 8,8pkt/9.

Zrealizował szkolenia dla setek Klientów z sektora publicznego oraz prywatnego co potwierdzają liczne referencje. Trener jest również twórcą autorskich szkoleń z zakresu Windows Server oraz bezpieczeństwa IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe, które są dostępne na koncie Uczestnika na dedykowanym portalu. Uczestnik uzyskuje również 180-dniowy dostęp do laboratoriów Microsoft, z których korzysta w dowolny sposób i w dowolnym momencie, za pośrednictwem przeglądarki internetowej.
Poza dostępami przekazywanymi Uczestnikowi, w trakcie szkolenia, Trener przedstawia i omawia autoryzowaną prezentację.

Warunki uczestnictwa

W celu przystąpienia do szkolenia Uczestnik powinien znać w stopniu podstawowym platformę Microsoft 365, produkty firmy Microsoft związane z zabezpieczeniami, zgodnością i tożsamością. Powinien również posiadać znajomość systemu Windows 10, usług platformy Azure, w szczególności Azure SQL Database i Azure Storage, maszyn wirtualnych platformy Azure i sieci wirtualnych. Uczestnik powinien również rozumieć podstawowe pojęcia związane ze skryptami.

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniające rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział z każdego miejsca na świecie.

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, ktory potwierdzi swój udziałw szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:
- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.
- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/glosniki oraz mikrofon.
- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+
- aplikacja MS Teams może zostać zainstalowana na komputerze lub można z niej korzystać za pośrednictwem przeglądarki internetowej

Kontakt

Agata Wojciechowska

E-mail agata.wojciechowska@softronic.pl
Telefon (+48) 618 658 840