Możliwość dofinansowania

Microsoft Security Operations Analyst - forma zdalna w czasie rzeczywistym

Numer usługi 2024/06/28/120967/2200988

4 059,00 PLN brutto
3 300,00 PLN netto
144,96 PLN brutto/h
117,86 PLN netto/h

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
05.11.2024 do 08.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Docelowa grupa odbiorców: • **Administrator** • **Specjalista IT** • **Specjalista ds. bezpieczeństwa** • **Inżynier ds. bezpieczeństwa** Oczekiwane przygotowanie słuchaczy • Podstawowa znajomość platformy Microsoft 365 • Podstawowa wiedza na temat produktów firmy Microsoft związanych z zabezpieczeniami, zgodnością i tożsamością • Średnio zaawansowana znajomość systemu Windows 10 • Znajomość usług platformy Azure, w szczególności Azure SQL Database i Azure Storage • Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych • Podstawowe rozumienie koncepcji skryptowych • Umiejętność korzystania z anglojęzycznych materiałów
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	29-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28

Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie Uczestnika do szybkiego korygowania aktywnych ataków w środowisku, doradzania w zakresie doskonalenia praktyk ochrony przed zagrożeniami i umiejętności kierowania naruszeń polityk organizacyjnych do odpowiednich interesariuszy. Dzięki nabyciu tych umiejętności Uczestnik zwiększy bezpieczeństwo systemów informatycznych w swojej organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje zabezpieczenia przed zagrożeniami i incydentami za pomocą usługi Microsoft 365 Defender	- charakteryzuje sposoby ochrony przed zagrożeniami na platformie Microsoft 365 - definiuje sposoby ograniczenia incydentów za pomocą usługi Microsoft 365 Defender - definiuje sposoby wykorzystania Microsoft Defender dla tożsamości - charakteryzuje sposoby ochrony swojej tożsamości za pomocą usługi Azure AD Identity Protection - definiuje sposoby wykorzystania Microsoft Defender dla aplikacji w chmurze - charakteryzuje sposoby reakcji na alerty zapobiegania utracie danych przy użyciu Microsoft 365 - definiuje sposoby zarządzania ryzykiem wewnętrznym na platformie Microsoft 365	Test teoretyczny
Ogranicza zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych	- charakteryzuje zasady ochrony przed zagrożeniami za pomocą usługi Microsoft Defender dla punktów końcowych - charakteryzuje zasady implementacji zabezpieczeń systemu Windows - charakteryzuje zasady konfiguracji i zarządzania automatyzacją - charakteryzuje zasady konfiguracji alertów i wykryć	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Ogranicza zagrożenia za pomocą usługi Microsoft Defender for Cloud	- charakteryzuje zasady ochrony obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud - charakteryzuje zasady zarządzania stanem bezpieczeństwa w chmurze - charakteryzuje zasady zabezpieczania obciążeń w usłudze Microsoft Defender for Cloud - charakteryzuje zasady korygowania alertów zabezpieczeń za pomocą usługi Microsoft Defender for Cloud	Test teoretyczny
Konfiguruje środowisko Microsoft Sentinel	- charakteryzuje zasady zarządzania obszarami roboczymi Microsoft Sentinel - charakteryzuje dzienniki zapytań w Microsoft Sentinel - charakteryzuje listy obserwacyjne w Microsoft Sentinel	Test teoretyczny
Tworzy wykrywanie i prowadzi dochodzenie przy użyciu programu Microsoft Sentinel	- charakteryzuje zasady wykrywania zagrożeń za pomocą analiz Microsoft Sentinel - charakteryzuje zasady zarządzania incydentami bezpieczeństwa w Microsoft Sentinel - definiuje normalizację danych w Microsoft Sentinel - charakteryzuje zasady zarządzania zawartością w Microsoft Sentinel	Test teoretyczny
Wychwytuje zagrożenia w Microsoft Sentinel	- definiuje koncepcje wykrywania zagrożeń w programie Microsoft Sentinel - charakteryzuje funkcje wyszukiwania ofert pracy w programie Microsoft Sentinel	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

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

AGENDA SZKOLENIA

Ścieżka szkoleniowa 01: Ogranicz zagrożenia za pomocą usługi Microsoft 365 Defender

- Wprowadzenie do ochrony przed zagrożeniami na platformie Microsoft 365
- Ogranicz incydenty za pomocą usługi Microsoft 365 Defender
- Eliminuj zagrożenia za pomocą usługi Microsoft Defender dla usługi Office 365
- Microsoft Defender dla tożsamości
- Chroń swoje tożsamości za pomocą usługi Azure AD Identity Protection
- Microsoft Defender dla aplikacji w chmurze
- Reaguj na alerty zapobiegania utracie danych przy użyciu Microsoft 365
- Zarządzaj ryzykiem wewnętrznym na platformie Microsoft 365

Ścieżka szkoleniowa 02: Ogranicz zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych

- Chroń się przed zagrożeniami za pomocą usługi Microsoft Defender dla punktów końcowych
- Wdróż środowisko usługi Microsoft Defender dla punktów końcowych
- Implementuj ulepszenia zabezpieczeń systemu Windows
- Wykonaj badania urządzeń
- Wykonaj czynności na urządzeniu
- Przeprowadzaj dochodzenia w sprawie dowodów i podmiotów
- Konfiguruj i zarządzaj automatyzacją
- Skonfiguruj alerty i wykrycia
- Wykorzystaj zarządzanie zagrożeniami i lukami w zabezpieczeniach

Ścieżka szkoleniowa 03 — ograniczaj zagrożenia za pomocą usługi Microsoft Defender for Cloud

- Zaplanuj ochronę obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud
- Połącz zasoby platformy Azure z usługą Microsoft Defender for Cloud
- Połącz zasoby spoza platformy Azure z usługą Microsoft Defender for Cloud
- Zarządzaj stanem bezpieczeństwa w chmurze
- Zabezpieczenia obciążeń w usłudze Microsoft Defender for Cloud
- Koryguj alerty zabezpieczeń za pomocą usługi Microsoft Defender for Cloud

Ścieżka szkoleniowa 04 — Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language

- Skonstruuj instrukcje KQL dla Microsoft Sentinel

- Analizuj wyniki zapytań za pomocą KQL
- Twórz wielotabelowe zestawienia przy użyciu języka KQL
- Praca z danymi łańcuchowymi przy użyciu instrukcji KQL

Ścieżka szkoleniowa 05 — Skonfiguruj swoje środowisko Microsoft Sentinel

- Wprowadzenie do Microsoft Sentinel
- Twórz i zarządzaj obszarami roboczymi Microsoft Sentinel
- Dzienniki zapytań w Microsoft Sentinel
- Użyj list obserwacyjnych w Microsoft Sentinel
- Wykorzystaj analizę zagrożeń w Microsoft Sentinel

Ścieżka szkoleniowa 06 — Połącz dzienniki z Microsoft Sentinel

- Połącz dane z Microsoft Sentinel za pomocą łączników danych
- Połącz usługi Microsoft z Microsoft Sentinel
- Połącz Microsoft 365 Defender z Microsoft Sentinel
- Połącz hosty Windows z Microsoft Sentinel
- Połącz dzienniki Common Event Format z Microsoft Sentinel
- Połącz źródła danych syslog z Microsoft Sentinel
- Połącz wskaźniki zagrożeń z Microsoft Sentinel

Ścieżka szkoleniowa 07 — Twórz wykrywanie i prowadź dochodzenia przy użyciu programu Microsoft Sentinel

- Wykrywanie zagrożeń za pomocą analiz Microsoft Sentinel
- Automatyzacja w Microsoft Sentinel
- Reaguj na zagrożenia za pomocą podręczników Microsoft Sentinel
- Zarządzanie incydentami bezpieczeństwa w Microsoft Sentinel
- Analityka behawioralna jednostek w Microsoft Sentinel
- Normalizacja danych w Microsoft Sentinel
- Wykonuj zapytania, wizualizuj i monitoruj dane w Microsoft Sentinel
- Zarządzaj zawartością w Microsoft Sentinel

Ścieżka szkoleniowa 08 — Polowanie na zagrożenia w Microsoft Sentinel

- Wyjaśnij koncepcje wykrywania zagrożeń w programie Microsoft Sentinel
- Polowanie na zagrożenia z Microsoft Sentinel
- Użyj funkcji wyszukiwania ofert pracy w programie Microsoft Sentinel
- Poluj na zagrożenia za pomocą notatników w Microsoft Sentinel

Oczekiwane przygotowanie słuchaczy

- Podstawowa znajomość platformy Microsoft 365
- Podstawowa wiedza na temat produktów firmy Microsoft związanych z zabezpieczeniami, zgodnością i tożsamością
- Średnio zaawansowana znajomość systemu Windows 10
- Znajomość usług platformy Azure, w szczególności Azure SQL Database i Azure Storage
- Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych
- Podstawowe rozumienie koncepcji skryptowych

- Umiejętność korzystania z anglojęzycznych materiałów

Efekty uczenia zostaną zweryfikowane przed szkoleniem i po szkoleniu poprzez pre i post testy w formie testu teoretycznego zamkniętego w formie online.

Harmonogram

Liczba przedmiotów/zajęć: 17

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 17 Ścieżka szkoleniowa 01: Ogranicz zagrożenia za pomocą usługi Microsoft 365 Defender ćwiczenia	Paweł Telbuch	05-11-2024	10:00	11:00	01:00
2 z 17 Ogranicz incydenty za pomocą usługi Microsoft 365 Defender ćwiczenia	Paweł Telbuch	05-11-2024	11:00	12:30	01:30
3 z 17 Reaguj na alerty zapobiegania utracie danych przy użyciu Microsoft 365 wykład	Paweł Telbuch	05-11-2024	12:30	14:30	02:00
4 z 17 Zarządzaj ryzykiem wewnętrznym na platformie Microsoft 365	Paweł Telbuch	05-11-2024	14:30	17:00	02:30
5 z 17 Ścieżka szkoleniowa 02: Ogranicz zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych ćwiczenia	Paweł Telbuch	06-11-2024	09:00	11:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 17 Chroń się przed zagrożeniami za pomocą usługi Microsoft Defender dla punktów końcowych ćwiczenia	Paweł Telbuch	06-11-2024	11:00	13:00	02:00
7 z 17 Konfiguruj i zarządzaj automatyzacją Skonfiguruj alerty i wykrycia ćwiczenia	Paweł Telbuch	06-11-2024	11:00	13:00	02:00
8 z 17 Wykonaj czynności na urządzeniu ćwiczenia	Paweł Telbuch	06-11-2024	13:00	14:00	01:00
9 z 17 Wykorzystaj zarządzanie zagrożeniami i lukami w zabezpieczeniach ćwiczenia	Paweł Telbuch	06-11-2024	14:00	16:00	02:00
10 z 17 Ścieżka szkoleniowa 03 — ograniczaj zagrożenia za pomocą usługi Microsoft Defender for Cloud ćwiczenia	Paweł Telbuch	07-11-2024	09:00	11:00	02:00
11 z 17 Połącz zasoby platformy Azure z usługą Microsoft Defender for Cloud ćwiczenia	Paweł Telbuch	07-11-2024	11:00	13:00	02:00
12 z 17 Zabezpieczenia obciążeń w usłudze Microsoft Defender for Cloud ćwiczenia	Paweł Telbuch	07-11-2024	13:00	14:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 17 Ścieżka szkoleniowa 04 — Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language ćwiczenia	Paweł Telbuch	08-11-2024	09:00	11:00	02:00
14 z 17 Ścieżka szkoleniowa 05 — Skonfiguruj swoje środowisko Microsoft Sentinel ćwiczenia	Paweł Telbuch	08-11-2024	11:00	13:00	02:00
15 z 17 Ścieżka szkoleniowa 06 — Połącz dzienniki z Microsoft Sentinel ćwiczenia	Paweł Telbuch	08-11-2024	13:00	14:00	01:00
16 z 17 Ścieżka szkoleniowa 07 — Twórz wykrywanie i prowadź dochodzenia przy użyciu programu Microsoft Sentinel ćwiczenia	Paweł Telbuch	08-11-2024	14:00	15:00	01:00
17 z 17 Ścieżka szkoleniowa 08 — Polowanie na zagrożenia w Microsoft Sentinel ćwiczenia	Paweł Telbuch	08-11-2024	15:00	16:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	4 059,00 PLN
Koszt przypadający na 1 uczestnika netto	3 300,00 PLN
Koszt osobogodziny brutto	144,96 PLN
Koszt osobogodziny netto	117,86 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Telbuch

Wykształcenie: Wyższe magisterskie
Wyższa Szkoła Menedżerska w Warszawie – Pedagogika wczesnoszkolna i przedszkolna z elementami informatyki
Specjalizacja:
Serwerowe systemy operacyjne Microsoft NT/2000/2003/2008/2012.2016
Usługi katalogowe Active Directory
Usługi sieciowe w systemach Microsoft
Bezpieczeństwo systemów Microsoft
Klienckie systemy operacyjne Microsoft NT/2000/Vista/7/8/10
System Center – private cloud.
Doświadczenie trenerskie: Obecnie trener Altkom Akademii. Doświadczenie w prowadzeniu autoryzowanych szkoleń Microsoft od 2001 roku.
Zakres tematyczny prowadzonych szkoleń:
Administracja, implementacja środowiska serwerowego MS Windows 2000/ 2003/2008/2012/2016
Zarządzanie i utrzymanie środowiska serwerowego MS Windows 2000/ 2003/2008/2012/2016
Planowanie i projektowanie środowiska serwerowego MS Windows 2000/ 2003/2008/2012/2016
Administracja, implementacja środowiska serwerowego MS Windows 2000/ 2003/2008/2012/2016
Zarządzanie i utrzymanie środowiska serwerowego MS Windows 2000/ 2003/2008/2012/2016
Planowanie i projektowanie środowiska serwerowego MS Windows 2000/ 2003/2008/2012/2016
Administracja i implementacja usług katalogowych MS Windows 2000/ 2003/2008/2012/2016
Administracja, implementacja infrastruktury sieciowej MS Windows 2000/ 2003/2008/2012/2016
Zarządzanie i utrzymanie infrastruktury sieciowej MS Windows 2000/ 2003/2008/2012/2016
Planowanie i projektowanie infrastruktury sieciowej MS Windows 2000/

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych, do którego składają Państwo dokumenty o dofinansowanie do usługi rozwojowej.

Ogólne warunki uczestnictwa w zajęciach zostały zamieszczone na stronie: https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/

Informacje dodatkowe

Po szkoleniu Uczestnik otrzyma zaświadczenie o ukończeniu szkolenia.

Trener podczas szkolenia będzie organizował krótkie przerwy. Informacja o przerwach będzie umieszczona na slajdzie.

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY:

- Podstawowa znajomość platformy Microsoft 365
- Podstawowa wiedza na temat produktów firmy Microsoft związanych z zabezpieczeniami, zgodnością i tożsamością
- Średnio zaawansowana znajomość systemu Windows 10
- Znajomość usług platformy Azure, w szczególności Azure SQL Database i Azure Storage
- Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych
- Podstawowe rozumienie koncepcji skryptowych
- Umiejętność korzystania z anglojęzycznych materiałów

Warunki techniczne

Wymagania ogólne realizacji szkolenia w formule distance learning (online): Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt

Adrianna Kukurudz

E-mail adrianna.kukurudz@altkom.pl
Telefon (+22) 801 258 566