Możliwość dofinansowania

Szkolenie TH-200 Foundational Threat Hunting - kompleksowy kurs e-learningowy

Numer usługi 2026/07/20/142469/3697879

7 870,77 PLN brutto
6 399,00 PLN netto
145,76 PLN brutto/h
118,50 PLN netto/h
261,33 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

197 ocen

Usługa szkoleniowa
zdalna
54:00 h
21.09.2026 do 19.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie TH-200 Foundational Threat Hunting jest skierowane do wszystkich, którzy chcą zbudować solidne podstawy w zakresie wykrywania zagrożeń, w tym analityków SOC, specjalistów ds. bezpieczeństwa IT oraz osób planujących przejście na wyspecjalizowane stanowiska w dziedzinie cyberbezpieczeństwa. Szkolenie w języku angielskim.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	01-09-2026
Forma prowadzenia usługi	zdalna
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

Celem kursu jest przygotowanie uczestników do działania w defensywnym wymiarze cyberbezpieczeństwa, tj. do wyszukiwania i identyfikacji zagrożeń.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia koncepcje i etapy procesu threat hunting.	omawia cele i znaczenie proaktywnego threat huntingu w cyberbezpieczeństwie	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia etapy procesu threat hunting	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje typy threat hunting stosowane w organizacjach	Test teoretyczny z wynikiem generowanym automatycznie
	wyjaśnia podstawowe pojęcia i praktyki związane z wykrywaniem zagrożeń	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje krajobraz aktorów zagrożeń.	rozróżnia typy aktorów zagrożeń w cyberprzestrzeni	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje specyfikę działania grup ransomware	Test teoretyczny z wynikiem generowanym automatycznie
	omawia cechy zaawansowanych trwałych zagrożeń (APT)	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje przykłady znanych aktorów zagrożeń i ich techniki działania.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady komunikacji i raportowania w threat huntingu.	wyjaśnia zasady działania Traffic Light Protocol (TLP)	Test teoretyczny z wynikiem generowanym automatycznie
	klasyfikuje informacje zgodnie z poziomami TLP	Test teoretyczny z wynikiem generowanym automatycznie
	przygotowuje raport z działań threat huntingowych	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje dane wywiadowcze w kontekście raportowania zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie
Wykorzystuje dane sieciowe do wykrywania zagrożeń.	identyfikuje sieciowe wskaźniki kompromitacji (IoC)	Test teoretyczny z wynikiem generowanym automatycznie
	konfiguruje narzędzia IDS/IPS do monitorowania ruchu sieciowego	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje zdarzenia sieciowe pod kątem aktywności podejrzanej	Test teoretyczny z wynikiem generowanym automatycznie
	wykrywa oznaki kompromitacji infrastruktury sieciowej.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykrywa zagrożenia na stacjach końcowych.	identyfikuje endpointowe wskaźniki kompromitacji	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje dane wywiadowcze do planowania działań	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje artefakty systemowe w celu wykrycia zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie
Wykrywa zagrożenia bez użycia znanych wskaźników kompromitacji.	opisuje metody wykrywania oparte na analizie zachowań	Test teoretyczny z wynikiem generowanym automatycznie
	koreluje dane z różnych źródeł w celu identyfikacji anomalii	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje symptomy zaawansowanych zagrożeń	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje narzędzia do analizy behawioralnej w procesie threat hunting.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Kurs **TH-200 Foundational Threat Hunting** to kompleksowy kurs, który wprowadza uczestników w zaawansowane techniki aktywnego wyszukiwania zagrożeń w sieciach i systemach. Uczestnicy uczą się identyfikować, analizować i neutralizować zagrożenia zanim wyrządzą szkody, korzystając z narzędzi Kali Linux oraz systemów SIEM i EDR. Kurs łączy teorię z praktyką poprzez realistyczne laboratoria i ćwiczenia, co pozwala zdobyć praktyczne umiejętności niezbędne w pracy analityka SOC lub threat hunter.

Szkolenie realizowane jest w formule **e-learningu asynchronicznego** (self-paced) **w języku angielskim**.

Uczestnik otrzymuje dostęp do indywidualnie wygenerowanego konta **na platformie OffSec** na okres **90 dni.** W tym czasie może korzystać z materiałów bez narzuconych terminów i godzin nauki, dostosowując tempo oraz harmonogram nauki do własnej dyspozycyjności.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy (test teoretyczny z wynikiem generowanym automatycznie).

Foundational Threat Hunting (TH-200) e-learning

- 90 dni dostępu do kursu i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.
- Bonusowy dostęp do kursu PEN-103, umożliwiający zdobycie dodatkowego certyfikatu.

Struktura szkolenia:

Kurs TH-200 składa się **z 7 modułów tematycznych**, obejmujących łącznie **54 godz.**, którym towarzyszą praktyczne ćwiczenia laboratoryjne i pytania testowe. Po ukończeniu modułów merytorycznych i laboratoriów, uczestnicy mogą pracować nad kompleksowym modułem Challenge Lab, który łączy wszystkie umiejętności zdobyte na kursie i przygotowuje ich do egzaminu OSTH.

Program szkolenia:

Koncepcje i praktyki Threat Hunting

Poznanie etapów i typów polowań na zagrożenia w przedsiębiorstwach — cele, metodyka i najlepsze praktyki, które pozwalają efektywnie planować i prowadzić aktywne wykrywanie zagrożeń.

Przegląd krajobrazu aktorów zagrożeń

Analiza różnych grup zagrożeń (w tym grup ransomware i APT), ich motywacji, typowych technik i znanych przypadków, aby lepiej priorytetyzować i kontekstualizować wyniki polowań.

Komunikacja i raportowanie dla Threat Hunterów

Opracowanie jasnych raportów i procesów przekazywania informacji (m.in. Traffic Light Protocol), tak by wywiad i obserwacje szybko trafiały do zespołów SOC, IR i zarządu.

Polowanie z użyciem danych sieciowych

Wykorzystywanie sieciowych IoC, analiz ruchu i narzędzi IDS/IPS (np. Suricata) do wykrywania podejrzanej aktywności, identyfikacji kompromitacji i budowania praktycznych zdolności detekcyjnych.

Polowanie na punktach końcowych

Stosowanie wskaźników na końcówkach (Endpoint IoC) oraz podejść opartych na hipotezach i telemetrii, aby skutecznie wykrywać i śledzić atakujące zachowania na hostach.

Threat Hunting bez IoC (behawioralne)

Huntowanie z użyciem analizy zachowań i korelacji danych zamiast opierać się wyłącznie na znanych IoC — metody wykrywania zaawansowanych i wcześniej nieznanych zagrożeń, z wykorzystaniem narzędzi takich jak CrowdStrike Falcon i własnych pipeline'ów analitycznych.

Szkolenie przygotowuje do certyfikacji OSTH (OffSec Threat Hunter)

Certyfikacja OSTH

- Praktyczny egzamin z zakresu Threat Hunting, wymagający od uczestnika wykrywania i analizowania działań zagrożeń w środowisku korporacyjnym.

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 870,77 PLN
Koszt przypadający na 1 uczestnika netto	6 399,00 PLN
Koszt osobogodziny brutto	145,76 PLN
Koszt osobogodziny netto	118,50 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	54:00

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- **90 dni** dostępu do kursu (materiały do pobrania w pdf. oraz materiały video) i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.

Warunki uczestnictwa

Wymagana znajomość języka angielskiego na poziomie B1/B2 (średnio-zaawansowany)

Przed przystąpieniem do kursu zalecamy posiadanie pewnego doświadczenia w zakresie cyberbezpieczeństwa, solidnych podstawy w zakresie sieci TCP/IP oraz znajomości systemów operacyjnych Linux i Windows.

Warunki techniczne

Realizacja za pomocą platformy e-learningowej OffSec https://portal.offsec.com

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.

- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon.

- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+

Kontakt

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840