Możliwość dofinansowania

Szkolenie IR-200 Foundational Incident Response - kompleksowy kurs e-learningowy

Numer usługi 2026/03/09/142469/3390968

7 870,77 PLN brutto
6 399,00 PLN netto
262,36 PLN brutto/h
213,30 PLN netto/h
196,00 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5
169 ocen

zdalna
Usługa szkoleniowa
30 h
30.04.2026 do 31.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie IR-200 Foundational Incident Response jest skierowane do analityków Centrum Operacji Bezpieczeństwa (SOC), specjalistów ds. bezpieczeństwa IT i wszystkich profesjonalistów planujących przejście na stanowiska specjalistyczne w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem zarządzania incydentami. Szkolenie w języku angielskim.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1
Data zakończenia rekrutacji	17-04-2026
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	30
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 kompleksowego planowania reagowania na incydenty oraz wykorzystywania narzędzi i technik do skutecznego wykrywania i analizy incydentów bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia podstawowe koncepcje reagowania na incydenty bezpieczeństwa.	omawia cykl życia reagowania na incydenty wg NIST SP 800-61	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia kluczowe pojęcia związane z reagowaniem na incydenty	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje znaczenie reagowania na incydenty w systemie bezpieczeństwa organizacji.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje role, odpowiedzialności i modele pracy zespołów reagowania na incydenty.	opisuje role członków zespołu reagowania na incydenty	Test teoretyczny z wynikiem generowanym automatycznie
	porównuje wybrane frameworki (CREST, SANS, NIST)	Test teoretyczny z wynikiem generowanym automatycznie
	wyjaśnia współpracę zespołów IR z SOC i innymi jednostkami	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje fazy procesu reagowania na incydenty w analizie zdarzeń bezpieczeństwa.	identyfikuje cztery fazy reagowania na incydenty	Test teoretyczny z wynikiem generowanym automatycznie
	przyporządkowuje działania do właściwej fazy	Test teoretyczny z wynikiem generowanym automatycznie
	uzasadnia wybór działań w zależności od etapu incydentu	Test teoretyczny z wynikiem generowanym automatycznie
Planuje komunikację podczas incydentu bezpieczeństwa.	rozpoznaje dobre i złe praktyki komunikacyjne	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje elementy planu komunikacji incydentowej	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera formę komunikacji do rodzaju incydentu.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje typowe techniki ataków cybernetycznych	rozróżnia ataki oportunistyczne i ukierunkowane	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje charakterystyczne symptomy ataków	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje potencjalne skutki ataków	Test teoretyczny z wynikiem generowanym automatycznie
Wykrywa i analizuje zdarzenia bezpieczeństwa.	rozpoznaje oznaki złośliwej aktywności	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje dane zdarzeń	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera działania reagowania adekwatne do zagrożenia	Test teoretyczny z wynikiem generowanym automatycznie
Zabezpiecza i analizuje dowody cyfrowe w kontekście incydentu.	identyfikuje źródła dowodów cyfrowych	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje procedury zabezpieczania danych	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje wyniki analizy dowodów	Test teoretyczny z wynikiem generowanym automatycznie
Zarządza przypadkiem incydentu bezpieczeństwa.	otwiera i dokumentuje przypadek incydentu	Test teoretyczny z wynikiem generowanym automatycznie
	tworzy oś czasu zdarzeń	Test teoretyczny z wynikiem generowanym automatycznie
	przypisuje zasoby do sprawy.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje techniki izolowania i ograniczania skutków incydentu.	dobiera metody izolacji zagrożenia	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje strategie containmentu	Test teoretyczny z wynikiem generowanym automatycznie
	uzasadnia wybór działań ograniczających skutki incydentu.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Realizuje działania eliminacji zagrożeń i przywracania operacyjności.	identyfikuje źródło zagrożenia	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje proces usuwania zagrożeń	Test teoretyczny z wynikiem generowanym automatycznie
	planuje przywrócenie działania systemu	Test teoretyczny z wynikiem generowanym automatycznie
Przeprowadza ocenę wpływu incydentu na organizację.	identyfikuje obszary dotknięte incydentem	Test teoretyczny z wynikiem generowanym automatycznie
	ocenia potencjalne skutki operacyjne	Test teoretyczny z wynikiem generowanym automatycznie
	formułuje wnioski dotyczące ryzyka.	Test teoretyczny z wynikiem generowanym automatycznie
Sporządza dokumentację i raport po incydencie	tworzy techniczny raport incydentu	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje rekomendacje zapobiegawcze	Test teoretyczny z wynikiem generowanym automatycznie
	uzasadnia znaczenie dokumentacji dla przyszłych działań.	Test teoretyczny z wynikiem generowanym automatycznie

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

Kurs **IR-200 Foundational Incident Response** to kompleksowy kurs, który wprowadza uczestników w świat reakcji na incydenty bezpieczeństwa IT. Uczestnicy uczą się metodologii wykrywania, analizowania, reagowania i odzyskiwania po cyberatakach, korzystając z narzędzi cyfrowej analizy i technik post-mortem. Kurs łączy teorię z praktyką poprzez realistyczne laboratoria i ćwiczenia, co pozwala na efektywne przyswajanie wiedzy.

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 Incident Response (IR-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 IR-200 składa się **z ponad 10 modułów tematycznych**, obejmujących łącznie **30 godz**. Wiele modułów obejmuje ćwiczenia praktyczne i laboratoria, mające na celu zapewnienie uczestnikom praktycznego doświadczenia w zakresie reagowania na incydenty. Po ukończeniu modułów kursu uczestnicy mogą przystąpić do Challenge Lab, które odzwierciedla dokładną strukturę egzaminu certyfikacyjnego OSIR.

Program szkolenia:

Wprowadzenie do reagowania na incydenty

Poznanie podstawowych pojęć z zakresu Incident Response, w tym standardów NIST SP 800-61, oraz roli analityków i zespołów reagowania na incydenty.

Podstawy Incident Response

Omówienie odpowiedzialności analityków IR, zespołów reagowania na incydenty oraz wykorzystywanych ram i frameworków (CREST, SANS, NIST).

Fazy reakcji na incydent

Dogłębna analiza czterech faz Incident Response według NIST SP 800-61: przygotowanie, wykrywanie i identyfikacja, reakcja i przywracanie, post-mortem.

Plany komunikacji w IR

Przegląd przykładów skutecznej i nieskutecznej komunikacji zewnętrznej oraz znaczenie planów komunikacji w reagowaniu na incydenty.

Typowe techniki ataków

Identyfikacja i analiza najczęściej wykorzystywanych ataków, zarówno oportunistycznych, jak i ukierunkowanych, w celu zwiększenia efektywności reakcji.

Wykrywanie i identyfikacja incydentów

Rozpoznawanie i analiza złośliwych działań w celu określenia właściwych działań zaradczych i minimalizacji ryzyka.

Cyberforensics dla analityków IR

Zbieranie, analiza i zabezpieczanie cyfrowych dowodów z incydentów bezpieczeństwa.

Zarządzanie przypadkami incydentów

Praktyczne prowadzenie spraw: otwieranie przypadków, dodawanie zasobów, tworzenie osi czasu zdarzeń oraz analiza w środowisku laboratoryjnym IRIS.

Aktywne powstrzymywanie incydentów

Izolacja i neutralizacja wykrytych zagrożeń przy użyciu technik izolacji i strategii containment.

Eliminacja i odzyskiwanie po incydencie

Identyfikacja i usunięcie zagrożeń w celu przywrócenia normalnej pracy systemów.

Wstępna ocena wpływu

Opracowanie oceny skutków incydentu dla organizacji i określenie ryzyka dla działalności biznesowej.

Raportowanie post-mortem

Tworzenie technicznych raportów z incydentów w celu ulepszania przyszłych działań i zwiększenia efektywności usług bezpieczeństwa informacji.

Szkolenie przygotowuje do certyfikacji **OSIR** (**OffSec Incident Responder**).

Certyfikacja OSIR — Egzamin praktyczny z reagowania na incydenty

Egzamin OSIR potwierdza zdolność do reagowania na incydenty w realistycznych warunkach i skutecznego przeprowadzania analiz bezpieczeństwa w środowisku korporacyjnym.

Cennik

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	262,36 PLN
Koszt osobogodziny netto	213,30 PLN

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 podstawowej znajomości zagadnień sieciowych i systemów operacyjnych (Windows i Linux), a także znajomości podstawowych zasad cyberbezpieczeństwa.

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