Możliwość dofinansowania

Szkolenie SOC-200 Security Operations and Defensive Analysis - kompleksowy kurs e-learningowy

Numer usługi 2026/05/27/142469/3590752

7 870,77 PLN brutto
6 399,00 PLN netto
21,04 PLN brutto/h
17,11 PLN netto/h
261,33 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

189 ocen

Usługa szkoleniowa
zdalna
374:00 h
20.07.2026 do 17.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie SOC-200 Security Operations and Defensive Analysis jest skierowane do osób, które chcą zdobyć podstawowe umiejętności wykrywania, analizowania i obrony przed cyberatakami. Kurs nie tylko przygotowuje uczestników do certyfikacji, ale także wspiera długoterminową karierę w dziedzinie cyberbezpieczeństwa, budując umiejętności niezbędne do pracy wykwalifikowanego analityka ds. bezpieczeństwa informacji. Szkolenie przygotowuje uczestnika do pełnienia roli analityka Security Operations Center (junior/mid), który potrafi monitorować środowisko, analizować zdarzenia bezpieczeństwa i wspierać proces reagowania na incydenty. Szkolenie w języku angielskim.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	30-06-2026
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 praktycznej obrony systemów i sieci przed zagrożeniami cybernetycznymi poprzez monitorowanie środowiska, analizowanie zdarzeń bezpieczeństwa i wspieranie procesu reagowania na incydenty.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje metodykę działania atakujących	omawia etapy typowej metodyki ataku	Test teoretyczny z wynikiem generowanym automatycznie
	wyjaśnia zachowania i cele atakujących w różnych scenariuszach	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje ślady działań atakujących w logach i artefaktach	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje zależności między technikami ataku a skutkami w systemie.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje podatności i wektory ataku w środowisku Windows	opisuje typowe podatności stacji roboczych Windows	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje ataki po stronie klienta i serwera	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje techniki utrzymania dostępu w systemie	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje logi systemowe pod kątem incydentów bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje podatności i incydenty bezpieczeństwa w środowisku Linux	omawia najczęstsze wektory ataku na systemy Linux,	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje metody eskalacji uprawnień	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje podatności usług serwerowych,	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje nieprawidłowości w logach systemowych Linux.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykrywa zdarzenia sieciowe związane z incydentami bezpieczeństwa.	opisuje działanie zapór sieciowych i systemów wykrywania włamań	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje ruch sieciowy pod kątem anomalii	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje symptomy działań złośliwych w komunikacji sieciowej	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje alerty bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje alerty antywirusowe i techniki ukrywania aktywności.	wyjaśnia mechanizmy działania oprogramowania antywirusowego,	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje techniki omijania detekcji i przypadki zaciemniania ładunków	Test teoretyczny z wynikiem generowanym automatycznie
	ocenia ryzyko wynikające z ukrytej aktywności w systemie	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje techniki ukrytej komunikacji i przemieszczania się w sieci.	opisuje metody tunelowania i ukrytej komunikacji	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje lateral movement w środowisku sieciowym	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje ślady pivotowania w logach,	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje strukturę i bezpieczeństwo środowiska Active Directory.	opisuje strukturę i elementy Active Directory	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje potencjalne ścieżki ataku	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje uprawnienia użytkowników i grup	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje mechanizmy utrzymania dostępu w domenie.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Analizuje przemieszczanie się atakującego w środowisku Windows	opisuje techniki wykorzystania przejętych poświadczeń	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje metody zdalnego wykonywania poleceń	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje ślady pivotowania w środowisku	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje i wykorzystuje system SIEM do analizy bezpieczeństwa.	opisuje architekturę rozwiązania SIEM	Test teoretyczny z wynikiem generowanym automatycznie
	konfiguruje zbieranie logów z różnych źródeł	Test teoretyczny z wynikiem generowanym automatycznie
	normalizuje i analizuje dane zdarzeń	Test teoretyczny z wynikiem generowanym automatycznie
	tworzy dashboardy i alerty bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje dane SIEM w kontekście incydentów.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje logi systemowe w środowiskach Windows i Linux	identyfikuje źródła logów systemowych	Test teoretyczny z wynikiem generowanym automatycznie
	stosuje techniki filtrowania i korelacji zdarzeń	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje anomalie i wzorce incydentów	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 **Security Operations and Defensive Analysis (SOC-200)** to szkolenie o charakterze obronnym, którego celem jest nauka podstawowych umiejętności niezbędnych do obrony sieci i systemów przed cyberzagrożeniami. Uczestnicy zdobędą dogłębną wiedzę na temat procesów SOC, w tym monitorowania, wykrywania zagrożeń, selekcji alertów i eskalacji incydentów. Kurs kładzie nacisk na podejście praktyczne, umożliwiając uczestnikom efektywne analizowanie logów na dużą skalę, a jednocześnie rozwijając intuicję niezbędną do zrozumienia, w jaki sposób logi i artefakty są generowane zarówno w środowiskach Windows, jak i Linux.

W trakcie szkolenia uczestnicy pogłębią swoją wiedzę na temat incydentów bezpieczeństwa sieci, technik wykrywania i analizy obronnej, zdobywając pewność siebie w identyfikowaniu, analizowaniu i łagodzeniu realnych zagrożeń. Obejmuje to wykorzystanie analizy zagrożeń i kontekstu operacyjnego w celu wsparcia lepszego wykrywania zagrożeń w dynamicznych środowiskach korporacyjnych.

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).

Security Operations and Defensive Analysis (SOC-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 SOC-200 składa się **z 19 modułów tematycznych**, obejmujących łącznie **374 godz**.

Każdy z modułów zawiera filmy, laboratoria i ćwiczenia praktyczne, a także laboratoria wirtualne, które pozwalają uczestnikom wykazać się zrozumieniem materiału. Po zapoznaniu się z materiałami kursu, wykonanie Challenge Labs pomaga uczestnikom wykorzystać swoje umiejętności w obronie infrastruktury w realistycznych symulacjach ataków.

Po ukończeniu kursu uczestnicy mogą przystąpić do egzaminu certyfikacyjnego OSDA, w którym wykażą się umiejętnością identyfikowania, analizowania i reagowania na zagrożenia w warunkach rzeczywistych.

Program szkolenia:

Wprowadzenie do metodyki ataku

Zbudowanie podstawowego zrozumienia zachowań atakujących, cyklu ataku oraz przewidywania kroków przeciwnika w ramach zleceń testów penetracyjnych.

Wprowadzenie do punktów końcowych Windows

Identyfikacja typowych podatności punktów końcowych Windows i wektorów ataku, które przeciwnicy wykorzystują do kompromitacji systemów użytkowników.

Ataki po stronie serwera Windows

Analiza metod wykorzystywanych do eksploatacji krytycznych usług i podatności na serwerach Windows oraz praktyczne testy w kontrolowanym środowisku.

Ataki po stronie klienta Windows

Badanie ataków opartych na przeglądarce, luk w oprogramowaniu klienckim i technik socjotechnicznych używanych do kompromitacji interfejsów użytkownika.

Eskalacja uprawnień w Windows

Wykrywanie i wykorzystanie błędów konfiguracji, wad oprogramowania i luk pozwalających na podniesienie poziomu uprawnień i zwiększenie kontroli w sieci.

Utrzymywanie dostępu w Windows (Persistence)

Przegląd technik trwałego utrzymania dostępu: mechanizmy w systemie plików, wpisy w rejestrze, zadania zaplanowane i inne metody zachowania obecności na systemie.

Wprowadzenie do punktów końcowych Linux

Zapoznanie z typowymi wektorami ataku na systemy Linux, mechanizmami obronnymi oraz najczęściej występującymi słabościami.

Ataki po stronie serwera Linux

Zrozumienie sposobów kompromitacji serwerów Linux poprzez eskalację uprawnień, eksploity usług i błędy konfiguracyjne.

Detekcja w sieci (Network Detections)

Doprecyzowanie strategii unikania wykrycia poprzez analizę działania zapór, systemów IDS/IPS i innych mechanizmów monitorujących aktywność sieciową.

Alerty antywirusowe i omijanie antywirusów

Praktyczne metody minimalizowania śladu operacji i omijania detekcji AV: zaciemnianie ładunków, dostosowanie exploitów i techniki zmniejszające wykrywalność.

Ewazja sieciowa i tunelowanie

Tworzenie ukrytych kanałów komunikacji, pivotowanie i techniki tunelowania w celu poruszania się po sieci bez wykrycia przez systemy obronne.

Enumeracja Active Directory

Zbieranie informacji o strukturze AD, użytkownikach, grupach i uprawnieniach przy użyciu narzędzi i technik, które ujawniają potencjalne ścieżki ataku.

Ruch lateralny w Windows

Wykorzystanie skompromitowanych poświadczeń, zdalnego wykonania poleceń i pivotowania sieciowego do poszerzenia kontroli w środowisku Windows.

Utrzymywanie dostępu w Active Directory (AD Persistence)

Badanie ukrytych kont, manipulacji usługami i innych sposobów wtapiania się w strukturę domeny w celu długotrwałego utrzymania dostępu.

SIEM — część I: Budowa ELK SIEM

Praktyczne wdrożenie podstaw SIEM z użyciem ELK (Elasticsearch, Logstash, Kibana): instalacja, konfiguracja i integracja komponentów do zbierania logów.

SIEM — część II: Operacjonalizacja SIEM

Zarządzanie i wykorzystanie wdrożonego SIEM: zbieranie i normalizacja logów, tworzenie dashboardów, reguł alertów i procedur detekcji incydentów.

Szkolenie przygotowuje do certyfikacji OSDA OffSec Defense Analyst .

Egzamin OffSec Defense Analyst (OSDA).

- • Certyfikacja OSDA — Egzamin praktyczny z bezpieczeństwa systemów (Defense Analyst)

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70%, możesz mieć możliwość skorzystania ze zwolnienia z podatku VAT, pod warunkiem spełnienia pozostałych wymogów, o których mowa w § 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

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	21,04 PLN
Koszt osobogodziny netto	17,11 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	374:00

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 uczestnicy powinni posiadać solidne podstawy z zakresu sieci TCP/IP, znajomość systemów operacyjnych Linux i Windows oraz podstawową wiedzę z zakresu 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