Możliwość dofinansowania

RH415 Red Hat Security: Linux in Physical, Virtual, and Cloud - Warszawa

Numer usługi 2025/03/13/7370/2620068

13 899,00 PLN brutto
11 300,00 PLN netto
448,35 PLN brutto/h
364,52 PLN netto/h

OSEC Spółka z ograniczoną odpowiedzialnością

★★★★★

Warszawa / stacjonarna
Usługa szkoleniowa
31 h
01.09.2025 do 04.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Administratorzy systemów - odpowiedzialni za wsparcie fizycznej i wirtualnej infrastruktury firmy, systemów i serwerów. • Specjaliści i Audytorzy ds. Bezpieczeństwa IT - odpowiedzialni za zapewnienie, że środowisko technologiczne jest chronione przed atakami i jest zgodne z zasadami i przepisami dotyczącymi bezpieczeństwa/prywatności. • Architekci automatyzacji - inżynier lub architekt odpowiedzialny za rozwój automatyzacji w firmie oraz optymalizację narzędzi i infrastruktury chmurowej w celu osiągnięcia celów automatyzacji. *** • System Administrator – responsible for supporting the company's physical and virtual infrastructure, systems, and servers. • IT Security Practitioner / Compliance & Auditor – responsible for ensuring the technology environment is protected from attacks and is in compliance with security/privacy rules and regulations. • Automation Architect – Engineer or architect responsible for the company's automation development and optimizing cloud tools.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	25-08-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	31

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 szkolenia jest rozwój umiejętności związanych z zarządzaniem bezpieczeństwem systemów opartych na Red Hat Enterprise Linux, zarówno w środowiskach fizycznych, wirtualnych, jak i chmurowych. Uczestnicy nauczą się zarządzać ryzykiem, stosować narzędzia do audytów bezpieczeństwa, monitorować zgodność systemów oraz implementować techniki ochrony danych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik demonstruje umiejętności opisane poniżej: **- Zarządzanie zgodnością z OpenSCAP.** **- Włączanie SELinux na serwerze w stanie wyłączonym, przeprowadzanie podstawowej analizy polityki systemu oraz łagodzenie ryzyka za pomocą zaawansowanych technik SELinux.** **- Proaktywne identyfikowanie i rozwiązywanie problemów za pomocą Red Hat Insights.** **- Monitorowanie aktywności i zmian na serwerze za pomocą Linux Audit i AIDE.** **- Ochrona danych przed naruszeniem za pomocą USBGuard i szyfrowania pamięci masowej.** **- Zarządzanie kontrolami uwierzytelniania za pomocą PAM.** **- Ręczne stosowanie dostarczonych Ansible Playbooków do automatyzacji łagodzenia problemów związanych z bezpieczeństwem i zgodnością.** **- Skalowanie zarządzania OpenSCAP i Red Hat Insights za pomocą Red Hat Satellite i Red Hat Ansible Automation Platform.**	**Proges w porównaniu do pre testu.**	**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

1. Zarządzanie bezpieczeństwem i ryzykiem

- Definiowanie i wdrażanie strategii zarządzania bezpieczeństwem w systemach Red Hat Enterprise Linux.

1. Automatyzacja konfiguracji i naprawy za pomocą Ansible

- Automatyczne naprawianie błędów konfiguracji i bezpieczeństwa za pomocą Ansible Playbooks.

1. Ochrona danych za pomocą LUKS i NBDE

- Szyfrowanie danych na urządzeniach pamięci masowej za pomocą LUKS i używanie NBDE do zarządzania automatycznym odszyfrowywaniem po uruchomieniu serwerów.

1. Ograniczanie dostępu do urządzeń USB

- Ochrona systemów przed nieuczciwym dostępem do urządzeń USB za pomocą USBGuard.

1. Kontrolowanie uwierzytelniania za pomocą PAM

- Zarządzanie uwierzytelnianiem, autoryzacją, ustawieniami sesji i kontrolą haseł poprzez konfigurację wtykowych modułów uwierzytelniania (PAM).

1. Rejestrowanie zdarzeń systemowych za pomocą Audytu

- Rejestrowanie i sprawdzanie zdarzeń systemowych istotnych dla bezpieczeństwa przy użyciu systemu Audytu jądra Linux i narzędzi pomocniczych.

1. Monitorowanie zmian w systemie plików

- Wykrywanie i analizowanie zmian w systemach plików serwera i ich zawartości za pomocą AIDE.

1. Ograniczanie ryzyka za pomocą SELinux

- Poprawa bezpieczeństwa i ograniczeń między procesami przy użyciu SELinux oraz zaawansowanych technik i analiz SELinux.

1. Zarządzanie zgodnością z OpenSCAP

- Ocena i naprawa zgodności serwera z zasadami bezpieczeństwa przy użyciu OpenSCAP.

1. Analizowanie i naprawianie problemów za pomocą Red Hat Insights

- Identyfikowanie, wykrywanie i naprawianie typowych problemów i luk w zabezpieczeniach systemów Red Hat Enterprise Linux za pomocą Red Hat Insights.

1. Automatyzacja zgodności z Red Hat Satellite

- Automatyzacja i skalowanie kontroli zgodności OpenSCAP za pomocą Red Hat Satelli

---

1. Managing Security and Risk

- Define and implement strategies to manage security on Red Hat Enterprise Linux systems.

1. Automating Configuration and Remediation with Ansible

- Remediate configuration and security issues automatically with Ansible Playbooks.

1. Protecting Data with LUKS and NBDE

- Encrypt data on storage devices with LUKS, and use NBDE to manage automatic decryption when servers are booted.

1. Restricting USB Device Access

- Protect systems from rogue USB device access with USBGuard.

1. Controlling Authentication with PAM

- Manage authentication, authorization, session settings, and password controls by configuring Pluggable Authentication Modules (PAM).

1. Recording System Events with Audit

- Record and inspect system events relevant to security by using the Linux kernel's Audit system and supporting tools.

1. Monitoring File System Changes

- Detect and analyze changes to a server's file systems and their contents by using AIDE.

1. Mitigating Risk with SELinux

- Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analysis.

1. Managing Compliance with OpenSCAP

- Evaluate and remediate a server's compliance with security policies by using OpenSCAP.

1. Analyzing and Remediating Issues with Red Hat Insights

- Identify, detect, and correct common issues and security vulnerabilities with Red Hat Enterprise Linux systems by using Red Hat Insights.

1. Automating Compliance with Red Hat Satellite

- Automate and scale OpenSCAP compliance checks by using Red Hat Satellite.

1. Comprehensive Review

- Review tasks from Red Hat Security: Linux in Physical, Virtual, and Cloud.

Harmonogram

Liczba przedmiotów/zajęć: 11

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Managing Security and Risk	Dariusz Puchalak	01-09-2025	09:00	12:00	03:00
2 z 11 Automating Configuration and Remediation with Ansible	Dariusz Puchalak	01-09-2025	12:00	15:00	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 11 Protecting Data with LUKS and NBDE	Dariusz Puchalak	01-09-2025	15:00	17:00	02:00
4 z 11 Restricting USB Device Access	Dariusz Puchalak	02-09-2025	09:00	12:00	03:00
5 z 11 Controlling Authentication with PAM	Dariusz Puchalak	02-09-2025	12:00	15:00	03:00
6 z 11 Recording System Events with Audit	Dariusz Puchalak	02-09-2025	15:00	17:00	02:00
7 z 11 Monitoring File System Changes	Dariusz Puchalak	03-09-2025	09:00	12:00	03:00
8 z 11 Mitigating Risk with SELinux	Dariusz Puchalak	03-09-2025	12:00	15:00	03:00
9 z 11 Analyzing and Remediating Issues with Red Hat Insights	Dariusz Puchalak	03-09-2025	15:00	17:00	02:00
10 z 11 Automating Compliance with Red Hat Satellite	Dariusz Puchalak	04-09-2025	09:00	12:00	03:00
11 z 11 Comprehensive Review	Dariusz Puchalak	04-09-2025	12:00	16:00	04:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	13 899,00 PLN
Koszt przypadający na 1 uczestnika netto	11 300,00 PLN

Koszt osobogodziny brutto	448,35 PLN
Koszt osobogodziny netto	364,52 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Dariusz Puchalak

Red Hat Certified Architect - Red Hat Certification ID 110-254-448
https://rhtapps.redhat.com/verify/?certId=110-254-448

Wybrane certyfikaty:
• Red Hat Certified Specialist in Linux Diagnostics and Troubleshooting
• Red Hat Certified Specialist in High Availability Clustering
• Red Hat Certified Specialist in Services Management and Automation
• Red Hat Certified Specialist in Ansible Networking Automation
• Red Hat Certified Specialist in Gluster Storage Administration
• Red Hat Certified Specialist in Containers and Kubernetes
• Red Hat Certified Specialist in Ceph Cloud Storage
• Red Hat Certified Specialist in Advanced Automation: Ansible Best Practices
...

Uprawnienia trenerskie :
• Red Hat RHCI - Red Hat Certified Instructor
• Red Hat RHCX - Red Hat Certified Examiner
• SUSE Certified Instructor
• Check Point Security Instructor
• Certified Novell Instructor
• Novell Open Enterprise Server, eDirectory, ZENworks
• NetIQ Identity Manager
• Microsoft Certified Trainer

Doświadczenie:
1. Zaawansowana znajomość systemów i usług Uniksowych, Windowsowych
2. Znajomość systemów bezpieczeństwa (firewall, VPN, klastry, endpoint, system nadzoru nad uprzywilejowanymi użytkownikami)
3. Znajomość softwarowych systemów pamięci masowych (technologie Novellowe, iSCSI)
4. Znajomość PKI, TCP/IP, ATM, VRRP, eDirectory, Active Directory
5. Znajomość języków skryptowych (sh, bash,perl)

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autoryzowane materiały szkoleniowe Red Hat w formie elektronicznej (PDF) - podręcznik w języku angielskim.

Samo szkolenie prowadzone jest w języku polskim.

Na kilka dni przed rozpoczęciem szkolenia, na adres e-mail przypisany do konta Uczestnika na redhat.com (RHN ID jest wymagane przy zgłoszeniu Uczestnika), Uczestnik otrzymuje link do podręcznika, do szkolenia oraz do platformy komunikacyjnej z Trenerem. Link pozostaje aktywny przez cały czas trwania szkolenia.

Uczestnik/cy szkolenia otrzymuje/ą dostęp do wirtualnych laboratoriów - praktyczne ćwiczenia na realnych systemach.

Warunki uczestnictwa

Wymagania wstępne:

- Certyfikat Red Hat Certified Engineer (EX294 / RHCE) lub równoważna wiedza i doświadczenie w zakresie systemu Red Hat Enterprise Linux.
- Skorzystaj z naszej bezpłatnej oceny, aby sprawdzić, czy ta oferta najlepiej pasuje do Twoich umiejętności. Ocena umiejętności - https://skills.ole.redhat.com/en?partner=OSEC_PL

- Red Hat Certified Engineer (EX294 / RHCE) certification or equivalent Red Hat Enterprise Linux knowledge and experience.
- Take our free assessment to gauge whether this offering is the best fit for your skills.

Informacje dodatkowe

Ten kurs jest oparty na RHEL 9.2, Ansible Core 2.14, Red Hat Ansible Automation Platform 2.4, Satellite 6.14 i OpenSCAP 1.3.7.

Po ukończeniu szkolenia laboratorium będzie dostępne przez maksymalnie 45 dni dla każdego szkolenia na żywo, które obejmuje środowisko wirtualne.

Uwaga: Szkolenie oferowane jest w formie czterodniowych zajęć stacjonarnych, pięciodniowych zajęć wirtualnych lub w trybie samodzielnym.

Kolejne kroki:

- Red Hat Certified Specialist in Security: Linux (EX415)
- Red Hat Satellite 6 Administration (RH403) - zalecane dla osób chcących dowiedzieć się więcej o Red Hat Satellite.
- Zalecane dla tych, którzy chcą korzystać z praktyk DevOps w celu zapewnienia bezpieczeństwa

Informacja o kompetencjach:

- certyfikat udziału w szkoleniu (do pobrania z indyw. konta Uczestnika na redhat.com)

Szkolenie w j. polskim (chyba, że wskazano inaczej).

Max 12, min - 4 os

Adres

ul. Zeusa 41
01-497 Warszawa
woj. mazowieckie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Artur Kozioł

E-mail artur.koziol@osec.pl

Telefon (+48) 503 004 798