**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest zakup voucherów uprawniających do dostępu do usług szkoleniowych w zakresie wskazanym w opisie poszczególnych zadań produktów. Z uwagi
na specyfikę przedmiotu zamówienia, proponuje się podział zamówienia na zadania,
co pozwoli na sprawne przeprowadzenie procedury przetargowej i umożliwi wykonawcom łatwiejszy dostęp do zamówienia, a także pozwoli na uzyskanie jak najbardziej korzystnych ofert dla Zamawiającego.

Biorąc powyższe pod uwagę poniżej zawarto opisy przedmiotów zamówienia
dla poszczególnych zadań. Tytuły szkoleń w poszczególnych zadaniach zawierają kody szkoleń zgodne ze ścieżką standardową dla danych produktów.

**WARUNKI PRZEPROWADZENIA SZKOLEŃ**

1. Z uwagi na rozliczenie w formie przedpłaty oraz długi czas realizacji przedmiotu zamówienia Wykonawca przed zawarciem umowy wniesie zabezpieczenie należytego wykonania Umowy w wysokości stanowiącej równowartości wynagrodzenia Wykonawcy z tytułu wykonania umowy, w jednej z form określonych w ustawie „Prawo zamówień publicznych” (tj. Dz. U. z 2019 r. poz. 1843). Zamawiający zwróci zabezpieczenie zwrotu wynagrodzenia w terminie 30 dni od dnia zakończenia realizacji umowy. Za dzień zakończenia umowy Strony przyjmują dzień wydania wszystkich świadectw o ukończeniu szkoleń. W przypadku wniesienia zabezpieczenia w gotówce Zamawiający dopuszcza proporcjonalny zwrot wpłaconej kwoty po realizacji szkoleń o wartości stanowiącej co najmniej połowę wynagrodzenia.
2. Szkolenia zostaną przeprowadzone na terenie Warszawy, po uzgodnieniu ich terminu
z Zamawiającym.
3. Wykonawca przedstawi harmonogram szkoleń nie później niż 21 dni od daty dostarczenia voucherów szkoleniowych. Wykonawca zapewni co najmniej dwa terminy szkoleń z każdego zakresu tematycznego. Zamawiający może skorzystać z obu uzgodnionych terminów, dzieląc zgłaszanych uczestników na dwie grupy. Dokładne terminy szkoleń zostaną uzgodnione między stronami.
4. W tym samym terminie może odbywać się tylko jedno z wymienionych w każdym zadaniu szkoleń.
5. Wykonawca zapewni salę szkoleniową wraz ze sprzętem niezbędnym do przeprowadzenia szkolenia oraz materiały dydaktyczne dla uczestników szkolenia, odzwierciedlające całość zagadnień poruszanych na szkoleniu.
6. Szkolenia muszą być przeprowadzane w języku polskim.
7. Wykonawca zapewni realizację usług szkoleniowych wynikających z voucherów, zgodnie ze szczegółowym opisem poszczególnych szkoleń lub kodem/nazwą katalogową szkolenia (jeśli taki istnieje) i dla określonej do każdego rodzaju szkolenia liczby uczestników.
8. Poprzez pojęcie 1 dzień szkolenia należy rozumieć 8 godzin dydaktycznych gdzie każda godzina dydaktyczna stanowi 45 minut.
9. Za równoważne Zamawiający uzna szkolenia obejmujące co najmniej przedmiot zawarty
w szkoleniach o wymienionych nazwach katalogowych, taką samą tematykę przedmiotowych szkoleń, taki sam czas wymagany do ich przeprowadzenia.
10. Termin wykonania usług szkoleniowych nastąpi nie później niż do dnia 31.12.2020 r.
11. Szkolenia wynikające z voucherów powinny być przeprowadzone przez wykładowców posiadających odpowiednie kwalifikacje zawodowe, doświadczenie i wykształcenie umożliwiające ich realizację.
12. Uczestnicy szkoleń wynikających z voucherów otrzymają imienny certyfikat ukończenia każdego szkolenia.
13. Wykonawca nie może powierzyć wykonania przedmiotu umowy osobie trzeciej bez uprzedniej zgody Zamawiającego wyrażonej na piśmie.
14. Przedmiot zamówienia stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego zgodnie z art. 43 ust. 1 pkt 29 c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2017 r., poz. 1221 z późn. zm.).
15. Zamawiający dopuszcza formę otwartą realizacji szkoleń tj. realizację szkoleń w grupach składających się z osób delegowanych przez Zamawiającego oraz komercyjnych Klientów wykonawcy, w ilości do 15 osób łącznie z osobami delegowanymi przez Zamawiającego. Zaproponowanie większej liczy uczestników szkolenia będzie wymagało indywidualnego ustalenia przedmiotowej kwestii w trybie „roboczym” z przedstawicielami Zamawiającego.
16. Zamawiający nie dopuszcza formy zdalnej realizacji szkoleń.
17. W przypadku przeprowadzenia szkoleń autoryzowanych, Zamawiający, zamiast przeniesienia autorskich praw majątkowych, o których mowa w § 7 umowy, wyrazi zgodę na udzielenie Zamawiającemu licencji (niewyłącznej, niezbywalnej, ograniczonej w czasie i na terytorium RP) na korzystanie z materiałów szkoleniowych i opracowań, które powstaną na potrzeby szkolenia.

**ZADANIE NR 1 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu produktów Microsoft:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | MS-10982 Supporting and Troubleshooting Windows 10 lub równoważne | 5 dni | 7  |
| **2.** | MS-10961 Automating Administration with Windows PowerShell lub równoważne | 5 dni | 4 |
| **3.** | Wdrażanie klienckich systemów operacyjnych z wykorzystaniem Windows Deployment Services lub równoważne | 3 dni | 12 |
| **4.** | MS-20462 Administering Microsoft SQL Server Databases lub równoważne | 5 dni | 1 |
| **5.** | MS-20742 Identity with Windows Server 2016 lub równoważne | 5 dni | 1 |
| **6.** | MS-20740 Installation, Storage and Compute with Windows Server 2016 lub równoważne | 5 dni | 1 |
| **7.** | MS-10987 Performance Tuning and Optimizing SQL Databases lub równoważne | 4 dni | 4 |

Szkolenia wymienione w punktach 1, 2, 4 – 7 muszą być autoryzowane przez Microsoft oraz przeprowadzone przez wykładowców posiadających odpowiednie kwalifikacje zawodowe, doświadczenie i wykształcenie umożliwiające ich realizację. Po zakończeniu szkolenia uczestnicy otrzymają inmienny certyfikat ukończenia kursu autoryzowany przez Microsoft.

**Szczegółowy opis szkoleń:**

**Ad. 1** **MS-10982** **Supporting and Troubleshooting Windows 10**

1. Wdrożenie metodyki rozwiazywania problemów
	* Przegląd systemu Windows 10
	* Wprowadzenie do roli EDST
	* Przegląd kroków prowadzących do rozwiązania problemu
	* Narzędzia służące do rozwiazywania problemów
2. Rozwiazywanie problemów z uruchamianiem systemu
	* Przegląd procesu Windows 10 Startup Recovery Environment
	* Rozwiazywanie problemów ustawień uruchamiania
	* Rozwiazywanie problemów usług systemu operacyjnego
	* Odzyskiwanie dysków szyfrowanych BitLocker
3. Rozwiazywanie problemów związanych ze sprzętem i sterownikami urządzeń
	* Rozwiazywanie problemów błędów sterowników urządzeń
	* Przegląd rozwiazywania problemów sprzętu
	* Rozwiazywanie problemów uszkodzeń fizycznych
	* Monitorowanie niezawodności
	* Konfigurowanie rejestru
4. Rozwiazywanie problemów ze zdalnym zarzadzaniem komputerami
	* Wykorzystanie Pulpitu Zdalnego
	* Wykorzystanie Pomocy Zdalnej
	* Zarzadzanie zdalne z wykorzystaniem Windows PowerShell
5. Rozwiazywanie problemów związanych z połączeniami sieciowymi
	* Określanie ustawień sieciowych
	* Rozwiazywanie problemów połączeń sieciowych
	* Rozwiazywanie problemów rozwiazywania nazw
6. Rozwiazywanie problemów z zasadami grupy
	* Przegląd aplikacji Zasady Grupy
	* Rozwiazywanie błędów dotyczących konfiguracji klienta
7. Rozwiazywanie problemów ustawień użytkownika
	* Rozwiazywanie problemów logowania użytkownika
	* Rozwiazywanie problemów aplikacji ustawień użytkownika
8. Rozwiazywanie problemów połączenia zdalnego
	* Rozwiazywanie problemów połączeń VPN
	* Rozwiazywanie problemów DirectAccess
9. Rozwiazywanie problemów dostępu do zasobów w domenie
	* Rozwiazywanie problemów uprawnień do plików
	* Odzyskiwanie dostępu do plików zaszyfrowanych z wykorzystaniem EFS
	* Rozwiazywanie problemów dostępu do drukarek
10. Rozwiazywanie problemów dostępu do zasobów dla klientów niebędących członkami domeny
	* Konfiguracja i rozwiazywanie problemów rejestracji urządzenia
	* Konfiguracja i rozwiazywanie problemów folderów roboczych
	* Konfiguracja i rozwiazywanie problemów dostępu do usługi OneDrive
11. Rozwiazywanie problemów aplikacji
	* Rozwiazywanie problemów instalacji aplikacji desktopowych
	* Rozwiazywanie problemów aplikacji desktopowych
	* Zarzadzanie sklepem aplikacji Windows
	* Rozwiazywanie problemów dostępu do aplikacji Web firmy
12. Utrzymanie Windows 10
	* Zarzadzanie i rozwiazywanie problemów aktywacji systemu
	* Monitorowanie i rozwiazywanie problemów wydajności
	* Stosowanie aktualizacji dla aplikacji i systemu operacyjnego
13. Odzyskiwanie danych oraz systemu operacyjnego
	* Odzyskiwanie plików w Windows 10
	* Odzyskiwanie systemu operacyjnego

**Ad. 2 MS-10961Automating Administration with Windows PowerShell**

1. Początek pracy z PowerShell
	* informacje ogólne
	* składnia poleceń
	* wyszukiwanie i uruchamianie komend
2. Polecenia administracyjne
	* administracja AD przy pomocy PS
	* konfiguracja sieci
	* administracja serwerem Windows
3. Praca z Windows PowerShell Pipeline
	* zrozumienie Pipeline
	* wybieranie, sortowanie i mierzenie obiektów
	* filtrowanie obiektów
	* wyliczanie obiektów
	* eksport danych
4. Zrozumienie funkcjonowania pipeline w Windows PowerShell
	* przekazywanie danych za pomocą wartości
	* przekazywanie danych za pomocą nazwy właściwości
5. Używanie PSProviders i PSDrives
	* korzystanie z PSProviders
	* korzystanie z PSDrives
6. Zapytanie o informacje o systemie za pomocą WMI i CIM
	* zrozumienie WMI i CIM
	* zapytanie o dane za pomocą WMI i CIM
	* wprowadzanie zmian za pomocą WMI / CIM
7. Praca ze zmiennymi, tablicami i tabelami mieszania
	* używanie zmiennych
	* manipulowanie zmiennymi
	* manipulowanie tablicami i tabelami mieszającymi
8. Podstawowe skrypty
	* wprowadzenie do skryptowania
	* konstrukcje skryptów
	* importowanie danych z plików
9. Zaawansowane skrypty
	* akceptowanie danych wprowadzanych przez użytkownika
	* omówienie dokumentowania skryptów
	* rozwiązywanie problemów i obsługa błędów
	* funkcje i moduły
10. Administracja komputerami zdalnymi
	* korzystanie z podstawowego zdalnego zarządzania
	* korzystanie z zaawansowanych technik zdalnego zarządzania
	* korzystanie z PSSessions
11. Korzystanie z zadań wykonywanych w tle oraz zadań zaplanowanych
	* używanie zadań wykonywanych w tle
	* używanie zadań zaplanowanych
12. Stosowanie zaawansowanych technik i profili Windows PowerShell
	* tworzenie skryptów profilu
	* korzystanie z zaawansowanych technik

**Ad. 3 Wdrażanie klienckich systemów operacyjnych z wykorzystaniem Windows Deployment Services**

1. Projektowanie, konfiguracja i zarządzanie środowiskiem klienckim:
	* omówienie planowania środowiska klienckiego
	* zdefiniowanie wymań konfiguracyjnych i przygotowanie standardowych ustawień systemowych
2. Przegląd i konfiguracja roli Windows Deployment Services:
	* konfiguracja PXE i ustawień bootowania:
	* konfiguracja ustawień instalacyjnych
	* zarządzanie pakietami sterowników w WDS
	* instalacja z wykorzystaniem multiemisji;
3. Projektowanie obrazów Windows:
	* przegląd architektury instalacji Windows, rodzaje obrazów
	* przegląd procesu tworzenia obrazu Windows
	* wybór strategii tworzenia obrazu;
4. Wdrażanie Windows z wykorzystaniem Windows Assessment and Deployment Kit:
	* przegląd narzędzi Windows ADK w zarządzaniu obrazami
	* budowanie obrazu Windows z wykorzystaniem Windows SIM i Sysprep, ImageX
	* opracowanie i modyfikacje pliku odpowiedzi
	* zarządzanie środowiskiem prenstalacyjnym
	* przechwytywanie, zastosowanie i utrzymanie obrazu Windows z zastosowaniem narzędzia DISM i dedykowanego modułu PowerShell
	* Implementowanie sterowników do obrazów instalacyjnych
	* Przygotowanie pakietów konfiguracyjnych dla Windows 10 z wykorzystaniem Windows Configuration Designer
5. Wdrażanie Windows z wykorzystaniem Zero Touch Installation:
	* projektowanie środowiska Zero Touch Installation
	* wykonanie Zero Touch Installation z wykorzystaniem Microsoft Deployment Toolkit 2013;
6. Zarządzanie aktualizacjami systemu Windows:
	* Implementowanie poprawek Windows Update do obrazów Instalacyjnych
	* Implementowanie poprawek Windows Update używając Windows Update Standalone Installer;
7. Scentralizowane zarządzanie stacjami roboczymi w celu ujednolicenia ustawień systemów klienckich przy użyciu zasad polityk grupowych (GPO):
	* Modyfikacja wybranych ustawień systemowych z poziomu GPO
	* centralna instalacja, modyfikacja ustawień, aktualizacja popularnych aplikacji na przykładzie Adobe Reader i środowiska Java;
8. Elementy wirtualizacji stanu użytkownika
	* profile mobilne
	* Folder Redirection
	* User Experience Virtualization (UE-V)
	* pliki trybu offline
9. Wirtualizacja aplikacji z użyciem platformy Microsoft APP-V:
	* przegląd technologii związanych z wirtualizacją aplikacji
	* planowanie i implementacja App-V
	* zarządzanie i administrowanie wirtualizacją aplikacji
	* planowanie i wdrożenie klienta App-V

**Ad. 4** **MS-20462 Administering Microsoft SQL Server Databases**

1. Wprowadzenie do administracji Microsoft SQL Server 2014
	* omówienie administracji danych
	* wprowadzenie do platformy SQL Server
	* narzędzia i techniki zarządzania bazą danych
2. Instalacja i konfiguracja SQL Server 2014
	* planowanie instalacji SQL Server
	* instalacja SQL Server 2014
	* konfiguracja po instalacyjna
3. Praca z bazami danych i przechowywaniem
	* wprowadzenie do przechowywania danych z SQL Server
	* zarządzanie przechowywaniem w bazach systemowych
	* zarządzanie przechowywaniem w bazach użytkowników
	* przenoszenie plików bazy danych
	* konfigurowanie rozszerzenia puli buforów
4. Planowanie i implementacja strategii dotyczącej kopii zapasowej
	* zrozumienie modeli odzyskiwania w SQL Server
	* planowanie strategii kopii zapasowych
	* tworzenie kopii zapasowej baz danych i logów transakcji
	* opcje tworzenie kopii zapasowej
	* zapewnienie stabilności kopii zapasowej
5. Odtwarzanie baz danych SQL Server 2014
	* zrozumienie procesu odtwarzania
	* odtwarzanie baz danych
	* zaawansowane scenariusze odtwarzania
	* odtwarzanie do określonego momentu w przeszłości
6. Importowanie i eksportowanie danych
	* wprowadzenie do transferu danych
	* importowanie i eksportowanie danych tabelarycznych
	* kopiowanie i przenoszenie bazy danych
7. Monitorowanie SQL Server 2014
	* wprowadzenie do zagadnień monitorowania SQL Server
	* dynamiczne zarządzanie widokami i funkcjami (DMV i DMF)
	* monitorowanie wydajności
8. Śledzenie aktywności w SQL Server
	* śledzenie obciążenia w SQL Server
	* wykorzystanie śladów
9. Zarządzanie bezpieczeństwem w SQL Server
	* wprowadzenie do zagadnień bezpieczeństwa w SQL Server
	* zarządzanie bezpieczeństwem z poziomu serwera
	* zarządzanie zabezpieczeniami z poziomu bazy danych
	* zarządzanie dostępem do bazy danych
10. Audyt dostępu do danych i szyfrowanie danych
	* audytowanie dostępu do danych w SQL Server
	* implementacja audytu SQL Server
	* szyfrowanie baz danych
11. Obsługa bieżąca bazy danych
	* integralność baz danych
	* zarządzanie indeksami
	* automatyzacja bieżącej obsługi baz danych
12. Automatyzacja zarządzania SQL Server 2014
	* automatyzacja zarządzania SQL Server
	* implementacja zadań agenta SQL Server
	* zarządzanie zadaniami agenta SQL Server
	* zarządzanie zadaniem kontekstów bezpieczeństwa
	* zarządzanie zadaniami na wielu serwerach
13. Monitorowanie SQL Server 2014 z wykorzystaniem alarmów i powiadomień
	* monitorowanie błędów SQL Server
	* konfiguracja wiadomości pocztowych
	* konfiguracja operatorów, alarmów i powiadomień

**Ad. 5 MS-20742 Identity with Windows Server 2016**

1. Instalacja i konfiguracja kontrolerów domeny
	* wprowadzenie do usługi AD DS
	* wprowadzenie do kontrolerów domeny usługi AD DS
	* wdrożenie dkontrolera domeny
2. Zarządzanie obiektami w AD DS
	* zarządzanie kontami użytkowników
	* zarzadzanie grupami w AD DS
	* zarządzanie obiektami typu komputer w AD DS
	* wykorzystywanie PowerShell do zarządzania AD DS
	* wdrażanie i zarządzanie OU
3. Zarzadzanie zaawansowaną infrastrukturą AD DS
	* wprowadzenie do zaawansowanych wdrożeń AD DS
	* wdażanie rozproszoneo środowiska AD DS
	* konfiguracji relacji zaufania AD DS
4. Wdrażanie i zarządzanie lokacjami i replikacją AD DS
	* wprowadzenie do replikacji AD DS
	* konfiguracja lokacji AD DS
	* konfiguracja i monitorowanie replikacji AD DS
5. Wdrażanie zasad grupowych (Group Policy)
	* wprowadzenie do zasad grupowych
	* wdrażanie i zarzadzanie obiektami GPO (Group Policy Object)
	* konfiguracja zakresu i przetwarzania obiektów GPO
	* rozwiązywanie problemów z GPO
6. Zarzadzanie ustawieniami użytkownika za pomocą zasad grupowych
	* wdrażanie szablonów administracyjnych
	* konfiguracja przekierowania folderów (Folder Redirection), instalacji oprogramowania i skryptów
	* konfiguracja preferencji zasad grupowych
7. Zabezpieczanie usług AD DS
	* zabezpieczanie kontrolerów domeny
	* wdrażanie bezpieczeństwa kont
	* wdrożenie inspekcji uwierzytelnienia
	* konfiguracja zarządzanych kont usług
8. Wdrażanie i zarządzanie AD CS
	* wdrożenie urzędów CA
	* zarządzanie urzędami CA
	* rozwiązywanie problemów i utrzymanie urzędów CA
9. Wdrażanie i zarzadzanie certyfikatami
	* wdrożenie i zarzadzanie szablonami certyfikatów
	* zarządzanie wdrożeniem, odrzuceniem i odzyskiwaniem certyfikatów
	* wykorzystanie certyfikatów w środowisku biznesowym
10. Wdrażanie i zarządzanie AD FS
	* wprowadzenie do usługi AD FS
	* planowanie i wymagania usługi AD FS
	* wdrożenie i konfiguracja usługi AD FS
	* wprowadzenie do Web Application Proxy
11. Wdrażanie i zarządzanie usługą AD RMS
	* wprowadzenie do AD RMS
	* wdrożenie i zarzadzanie infrastrukturą AD RMS
	* konfiguracja ochrony zawartości za pomocą AD RMS
12. Wdrażanie synchronizacji AD DS z Microsoft Azure AD
	* planowanie i przygotowanie synchronizacji usług katalogowych
	* wdrożenie synchronizacji usług katalogowych wykorzystując Azure AD Connect
	* zarzadzanie tożsamościami za pomocą synchronizacji usług katalogowych
13. Monitorowanie, zarządzanie i odzyskiwanie AD DS
	* monitorowanie AD DS
	* zarzadzanie bazą Active Directory
	* Opcje wykonywanie kopii zapasowej Active Directory i jej dzyskiwania

**AD.6** **MS-20740 Installation, Storage and Compute with Windows Server 2016**

1. Instalacja, uaktualnienie i migracja serwerów i obciążenia roboczego
	* Wstęp do Windows Server 2016
	* Przygotowanie oraz instalacja serwera w wersji Nano i Core
	* Przygotowanie do uaktualnienia i migracji
	* Migracja ról serwera i obciążenia roboczego
	* Modele aktywacji serwera Windows
2. Konfiguracja lokalnego magazynu danych
	* Zarządzanie dyskami w Windows Server 2016
	* Zarządzanie wolumenami w Windows Server 2016
3. Wdrażanie rozwiązań magazynu danych typu „Enterprise”
	* Przegląd rozwiązań dyskowych typu DAS, NAS i SAN
	* Porównanie rozwiązań Fibre Channel, iSCSI oraz FCoE
	* Zrozumienie rozwiązań iSNS, DCP (Data Center Bridging) oraz MPIO
	* Konfiguracja udostępnień zasobów w Windows Server 2016
4. Wdrażanie rozwiązań „Storage Spaces” oraz deduplikacji danych
	* Wdrażanie przestrzeni magazynu dancyh „Storage Spaces”
	* Zarządzanie przestrzeniami dyskowymi
	* Wdrażanie deduplikacji danych
5. Instalacja i konfiguracja Hyper-V i maszyn wirtualnych
	* Przegląd funkcjonalności Hyper-V
	* Instalacja Hyper-V
	* Konfiguracja magazynu danych na serwerach Hyper-V
	* Konfiguracja usług sieciowych na serwerach Hyper-V
	* Konfiguracja maszyn wirtualnych Hyper-V
	* Zarządzanie maszynami wirtualnymi Hyper-V
6. Instalacja i zarządzanie kontenerami Windows Server i Hyper-V
	* Przegląd kontenerów w Windows Server 2016
	* Instalacja kontenerów w Windows Server 2016
	* Konfiguracja i zarządzanie kontenerami
7. Przegląd rozwiązań wysokodostępnych oraz odtwarzania danych
	* Definiowanie poziomów dostępności
	* Planowanie rozwiązań wysokodostępnych oraz odtwarzania danych dotyczących maszyn wirtualnych Hyper-V
	* Tworzenie kopii zapasowych i odtwarzanie systemu oraz danych za pomocą Windows Server Backup
	* Wysoka dostępność przy wykorzystaniu klastrów Windows Server 2016
8. Wdrożenie i zarządzanie klastrami
	* Planowanie usługi klastrów
	* Tworzenie i konfigurowania klastrów
	* Utrzymywanie klastrów
	* Rozwiązywanie problemów z usługą klastrów
	* Wdrażanie wysokiej dostępności lokacji za pomocą funkcjonalności „Strech clustering”
9. Wdrażanie usług klastrowych maszyn wirtualnych Hyper-V
	* Przegląd integracji Hyper-V w Windows Server 2016 z usługą klastrów
	* Wdrażanie i zarządzanie wirtualnymi maszynami w klastrze
	* Kluczowe cechy maszyn wirtualnych w środowisku klastrowym
10. Wdrażanie usługi równoważenia obciążenia sieciowego NLB
	* Przegląd klastrów NLB
	* Konfigurowanie klastra NLB
	* Planowanie wdrożenia NLB
11. Tworzenie i zarządzanie instalacją opartą na obrazach dyskowych
	* Wprowadzenie do instalacji opartej na obrazach dyskowych
	* Tworzenie i zarządzanie instalacją opartą na obrazach dyskowych przy użyciu MDT
	* Środowisko maszyn wirtualnych dla różnych obciążeń roboczych
12. Zarządzanie, monitorowanie i utrzymanie wdrożeń opartych na maszynach wirtualnych
	* Przegląd usługi WSUS i możliwości instalacji
	* Zarządzanie procesem uaktualnień za pomocą WSUS
	* Przegląd funkcjonalności PowerShell DSC
	* Przegląd narzędzi monitorowanie Windows Server 2016
	* Wykorzystanie monitora wydajności
	* Monitorowanie logów wydarzeń

**Ad. 7 MS-10987 Performance Tuning and Optimizing SQL Databases**

1. Architektura środowiska SQL Server, harmonogramowanie i obsługa blokad
	* komponenty składowe SQL Server i system SQL OS
	* harmonogramy zadań w systemie Windows i w środowisku SQL Server
	* system blokad i kolejek
2. SQL Server I/O
	* pojęcia podstawowe w operacjach wejścia/wyjścia
	* rozwiązania przechowujące dane
	* konfiguracja i testowanie wejścia/wyjścia
3. Struktury baz danych
	* struktura wewnętrzna bazy danych
	* struktura plików danych
	* struktura bazy TempDB
4. Obsługa pamięci w SQL Server
	* pamięć systemu operacyjnego
	* wykorzystanie przydzielonej pamieci przez SQL Server
	* konstrukcje In-Memory OLTP
5. Konkurencyjny dostęp do danych i obsługa transakcji
	* konkurencyjność i transakcje
	* system blokad dostępu
6. Konstrukcja statystyk i indeksów
	* wewnętrzna struktura statystyk i ich wykorzystanie w planach realizacji
	* budowa indeksów
	* indeksy kolumnowe
7. Uruchamianie zapytań i analiza planu wykonawczego
	* optymalizacja i wykonanie zapytań SQL
	* plany wykonawcze
8. Składowanie planów wykonawczych i rekompilacja
	* struktura cache dla planów wykonawczych
	* diagnostyka problemów powstałych przy wykorzystaniu cache
	* składowanie zapytań
9. Rozszerzone zdarzenia
	* pojęcia podstawowe
	* wykorzystanie systemu rozszerzonych zdarzeń
10. Monitorowanie, śledzenie i zestawianie podstawowych wartości parametrów wydajnościowych
	* monitorowanie i śledzenie wskaźników wydajnościowych
	* baseline - zaakceptowane wartości wskaźników wydajnościowych oraz porównywanie zestawień
11. Diagnozowanie najczęstszych przyczyn problemów wydajności
	* problemy wydajnościowe procesora
	* problemy wydajnościowe pamięci operacyjnej
	* problemy wydajnościowe systemu wejścia/wyjścia
	* problemy związane z konkurencyjnym dostępem do danych
	* wpływ wydajności bazy TempDB

**ZADANIE NR 2 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu produktów sieciowych:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania** | **Liczba uczestników** |
| **1.** | UCB11X Unified Communication Bootcamp v11.x lub równoważne | 5 dni | 1 |
| **2.** | NGFW Boot Next Generation firewall Bootcamp lub równoważne | 5 dni | 1 |

**Szczegółowy opis szkoleń:**

**Ad. 1 UCB11X Unified Communication Bootcamp v11.x**

1. Cisco Unified Communication Manager (CUCM)
	* Wirtualizacja, Prime License Manager
	* Dodawanie użytkowników i linii telefonów przy pomocy template’ow
	* Synchronizacja uzytkownikow z baza LDAP
	* Self-Provisioning
	* Voice-Gateway’e i protokoły sygnalizacyjne (H323, SIP, MGCP)
	* Zasady tworzenia dial-planu w voice-gateway’ach i CUCM (standard +E164, SIP URI, local route group, przywileje, manipulacje numeracja, CAC)
	* CUBE oraz SIP trunk do operatora telefonicznego
	* Media resources – transcoder, conference bridge, MOH
	* funkcjonalność Conference Now
	* Call Pickup, Hunt-group’y z Call Queing, Intercom
	* Extension Mobility, Device Mobility, Unified Mobility
2. VCS-C
	* rejestracja video-endpointów do VCS’a
	* integracja VCS’a z CUCM
	* routing połączeń pomiędzy VCS’em i CUCM
3. Cisco Unity Connection (CUC)
	* integracja CUC z CUCM
	* parametryzowanie systemu
	* konfiguracja użytkowników, synchronizacja z LDAP’em
	* dodatkowe funkcje CUC
4. Cisco Unified IM and Presence (IM&P)
	* integracja IM&P z CUCM
	* Cisco Jabber
	* integracja z LDAP’em
	* Mobile and Remote Access (MRA, "Collaboration Edge"), VCS-Expressway-C i VCS-Expressway-E
5. Cisco MediaSense
	* Integracja Cisco MS z CUCM i CUC
	* Video-on-Hold
	* Video greetings

**Ad. 2 NGFW Boot Next Generation firewall Bootcamp**

1. Cisco ASA jako firewall
	* Wstępna konfiguracja firewalla ASA
	* NAT i polityki dostępu
	* Inspekcja protokołów
	* Nowe funkcjonalności w oprogramowaniu ASA
2. Identity Based Firewall
	* Opis rozwiązania typu Cisco ASA Identity Firewall
	* Konfigurowanie Cisco CDA
	* Konfigurowanie Cisco ASA Identity Firewall
	* Weryfikacja i diagnozowanie Cisco ASA Identity Firewall
3. Cisco Firepower Threat Defense
	* Instalowanie Cisco Firepower na ASA i VM
	* Zarządzanie Cisco Firepower NGFW za pomocą Firepower Management Center (FMC)
	* Integracja z firewallami Cisco ASA oraz Firepower serii 2100/4100/9300
	* Budowanie polityk bezpieczeństwa warstwy L4-L7
	* Application Visibility and Control (AVC) oraz URL Filtering
	* AMP for Networks
	* Budowanie podstawowej polityki IPS
	* Zaawansowana konfiguracja IPS
	* Tuning reguł IPS w oparciu o Firepower Recommendations
	* Site-to-Site VPN oraz Remote Access VPN na FTD
	* SSL Decryption
	* Powiadamianie z zdarzeniach z wykorzystaniem Correlation Policy
	* Raportowanie
	* Budowanie własnych sygnatur IPS

**ZADANIE NR 3 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu produktów Hewlett Packard:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania** | **Liczba uczestników** |
| **1.** | HE646S HP BladeSystem Administration: c-Class lub równoważne | 3 dni | 4 |
| **2.** | HK 756S HP Insight Control: Management Fundamentals lub równoważne | 3 dni | 4 |

**Szczegółowy opis szkoleń:**

**Ad. 1 HE646S HP BladeSystem Administration: c-Class**

1. Wprowadzenie do infrastruktury Blade: Uproszczenie infrastruktury dzięki HP BladeSystem, HP CCI (Consolidated Client Infrastructure), Serwery klasy p i klasy c, Serwery pełnej wysokości i serwery połówkowe, Serwery pamięci masowej, Moduł Onboard Administrator, HP SIM 5.1 i serwery blade, HP BladeSystem Management Suite, Wykorzystanie RDP do instalacji , serwerów blade, Scenariusze wykorzystania serwerów blade, Wspierane rozwiązania klastrowe przez serwery blade
2. Zasilanie i chłodzenie serwerów klasy c: Projekt nowoczesnego centrum danych, Zasilanie zintegrowane w obudowie, Zasilacze, Moduły podłączeniowe zasilania, HP Dynamic Power Saver, Zaawansowane zarządzanie energią, Technologia Thermal Logic, Architektura PARSEC, Wentylatory HP Active Cool, Chłodzenie wielu obudów, HP Modular Coolling System
3. Serwery klasy c: Porównanie serwerów klasy p i klasy c, Cechy i korzyści, Procesory dwurdzeniowe, Pamięć masowa – rozwiązania szeregowe, Wewnętrzna pamięć masowa
4. Opcje podłączenia do sieci SAN dla serwerów klasy p: QLogic QMH2462 4Gb Fibre Channel HBA, Emulex 4Gb Fibre Channel HBA, Brocade 4Gb SAN Switch, Cisco MDS 9124e 4Gb SAN Switch, HP 4Gb Fibre Channel Pass-Thru Module
5. Instalacja infrastruktury do serwerów klasy c: Porównanie wymagań serwerów blade i tradycyjnych w zakresie miejsca instalacji, Planowanie systemu zasilania serwerów blade, Planowanie środowiska centrum danych, Przygotowanie obudowy, Przygotowanie i instalacji urządzeń sieciowych, Instalacja komponentów dystrybucji zasilania, Podłączenie modułów zarządzających, Instalacja zasilaczy
6. Instalacja i konfiguracja urządzeń SAN: Konfiguracja przełącznika Brocade 4Gb, Planowanie instalacji przełącznika, Instalacja przełącznika Brocade 4Gb, Sprawdzanie poprawności instalacji, Połączenie z Onboard Administrator, Weryfikacja i tworzenie kopii zapasowej konfiguracji
7. Zarządzanie serwerami klasy c: Zarządzanie obudową przy użyciu Onboard Administrator, HP BladeSystem Integrated Manager, Czym jest Insight Control, Insight Control i pakiety Essentials, Insight Control Data Center Edition, BladeSystem Automation Engine
8. Obudowa na serwery klasy c: Pozycjonowanie obudowy na serwery klasy c, Onboard Administrator
9. Zasilanie serwerów Blade: Komponenty systemu zasilania, Zasilanie jednofazowe i trzyfazowe, Zasilacze, System dystrybucji zasilania
10. Urządzenia aktywne i karty rozszerzeń (mezzanine): Sieć łącząca wiele potrzeb, Współdzielenie I/O, Kategorie sieciowych urządzeń połączeniowych, Karty mezzanine, Architektura Virtual Connect, Zarządzanie awarią serwera
11. Instalacja infrastruktury do serwerów klasy c: Porównanie wymagań serwerów blade i tradycyjnych w zakresie miejsca instalacji, Wykorzystanie narzędzi do konfiguracji systemów blade, Planowanie systemu zasilania serwerów blade, Rozpakowanie zestawu, Instalacja obudowy w szafie rack, Kontrola konfiguracji przeprowadzona przez Onboard Administrator, Insight Display Initial Setup Wizard, Onboard Administrator First Time Setup Wizard
12. Instalacja i konfiguracja urządzeń sieciowych dla serwerów klasy c: Czynności przed instalacją, Planowanie konfiguracji urządzeń sieciowych i zabezpieczeń, Logowanie do urządzeń sieciowych przez Onboard Administrator, Mapowanie portów przełączników, Konfiguracja przełączników nadmiarowych, Tworzenie kopii zapasowej konfiguracji, Instalacja modułu Pass-Thru
13. Wdrożenie serwerów klasy c: iLO 2, Rapid Deployment Pack 3.60, Ulepszenia dla infrastruktury blade, Tworzenie wirtualnych komputerów, Model „rip-and-replace”, Instalacja systemu na serwerze blade, Przechwytywanie obrazu serwera blade, Rekonfiguracja serwerów, Integracja z iLO, HP Control Tower – korzyści i instalacja, Podłączenie do sieci SAN
14. Wsparcie serwerów klasy c: Hardware and software support, Installation and Startup Service, Enhanced Network Installation and Startup, Service for BladeSystem Switches, Consulting and Implementation Services, Smart Cooling Services, Program napraw klienta, HP Instant Support Enterprise Edition, ISEE – konfiguracja i możliwości, Open Service Event Manager, Narzędzia diagnostyczne

**AD. 2 HK 756S HP Insight Control: Management Fundamentals**

1. Ogólne informacje o produkcie
	* Opis pakietu HP Insight Control i oprogramowania HP Systems Insight Manager
	* Opis nowych funkcjonalności dostępnych w HP Insight Control oraz HP Systems Insight Manager
	* Sposoby wykorzystania funkcjonalności w zarządzaniu zdalnymi systemami
	* Komponenty i aplikacje wymagane do zarządzania systemem
	* Określenie dostępności oprogramowania
	* Określenie zasobów pakietu
	* Opis opieki gwarancyjnej dla systemów Windows, Linux and HP-UX
2. Podstawy zarządzania infrastruktura
	* Zdefiniowanie pojęcia zarządzania systemami
	* Kluczowe elementy zarządzania systemami
	* Możliwości i komponenty karty iLO
	* Komponenty SmartStart do zarządzania serwerami ProLiant
	* Opis funkcjonalności Smart Update Manager służącej do aktualizacji oprogramowania i sterowników
	* Porównanie komponentów ProLiant Support Pack i narzędzi wspomagających zarządzanie
	* Opis agentów Insight Management Agents
	* Rozwiązywanie problemów agentów
	* Wykorzystanie System Management Homepage do zarządzania pojedynczym serwerem
	* Komponenty i możliwości WBEM
	* Rola WMI i interakcja z WBEM
	* Komponenty i możliwości Version Control
	* Wykorzystanie Version Control Agent i Version Control Repository
3. Instalacja oprogramowania po przez Version Control
	* Architektura funkcjonalności Version Control
	* Wymagania niezbędne do instalacji repozytorium oprogramowania
	* Konfiguracja repozytorium oprogramowania
	* Opis kroków aktualizacji zarządzanego systemu
* Laboratorium: Zarządzanie systemem z perspektywy jednego systemu i pokazania wymagań jakie należy spełnić aby ręcznie wykonać zadania zarządzania bez oprogramowania HP Systems Insight Manager 7.0 i Insight Software.
1. Typowa Instalacja
	* Zadania podczas instalacji
	* Kroki instalacji pakietu HP Insight Control na centralnym serwerze zarządzania - Central Management Server (CMS)
	* Wyjaśnienie roli WMI Mapper i procesu konfiguracji
	* Wyjaśnienie procesu aktualizacji oprogramowania HP Systems Insight Manager
	* Kroki niezbędne do usunięcia oprogramowania HP Systems Insight Manager
2. Konfiguracja
	* Opis i konfiguracja strony domowej
	* Opis dodawania użytkowników i uprawnień
	* Opis ustawienia wykrywania sprzętu
	* Nawigacja poprzez strony zarządzanych systemów
	* Opis konfiguracji zadań odpowiedzialnych za weryfikację stanu sprzętu i oprogramowania
	* Opis konfiguracji powiadomień
* Laboratorium: Konfiguracja HP Insight Control
1. HP BladeSystem Integrated Manager
	* Opis funkcjonalności i korzyści płynących z wykorzystania HP BladeSystem Integrated Manager
	* Opis zmian i nowości w HP BladeSystem Integrated Manager
	* Wyjaśnienie jak używać BladeSystem Integrated Manager
* Laboratorium: Użytkowanie HP BladeSystem Integrated Manager, Nawigacja poprzez hierarchię logiczną i foldery użytkowe w HP Systems Insight Manager 7.0
1. Używanie zadań, kolekcji, narzędzi i zdarzeń
	* Wyjaśnienie w jaki sposób używać zadań do zarządzania zdalnym systemem
	* Wyjaśnienie w jaki sposób wykorzystać kolekcje do filtrowania i organizowania systemów
	* Wyjaśnienie jak tworzyć i uruchamiać narzędzia
	* Wyjaśnienie jak zdarzenia są generowane i jak nimi zarządzać
* Laboratorium: Tworzenie i uruchamianie zadań, Tworzenie spersonalizowanych folderów i kolekcji, Przegląd zdarzeń, Konfiguracja automatycznej obsługi zdarzeń
1. Raporty
	* Opis procesu dostępu do raportów
	* Opis procesu zarządzania raportami
	* Identyfikacja zaawansowanych możliwości raportowania

**ZADANIE NR 4 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu Linux:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | LFS301 Linux for System Administration lub równoważne | 4 dni | 4 |

**Szczegółowy opis szkolenia:**

**Ad. 1 LFS301 Linux for System Administration**

1. Wprowadzenie
	* Linux Foundation
	* Linux Foundation Training
	* Linux Foundation Certifications
	* Laboratory Exercises, Solutions and Resources
	* E-Learning Course: LFS201
	* Szczegóły dystrybucji
	* Laboratoria
2. Rozkład drzewa systemu plików w Linuxie
	* One Big Filesystem
	* Rozróżnienie danych
	* Standardowe drzewo katalogów - FHS
	* root (/) directory
	* /bin
	* /boot
	* /dev
	* /etc
	* /home
	* /lib and /lib64
	* /media
	* /mnt
	* /opt
	* /proc
	* /sys
	* /root
	* /sbin
	* /srv
	* /tmp
	* /usr
	* /var
	* /run
	* Laboratoria
3. Procesy
	* Programy i procesy
	* Limity dla procesów
	* Tworzenie procesów
	* Stany procesów
	* Tryby procesów
	* Demony
	* Parametr nice
	* Biblioteki
	* Laboratoria
4. Sygnały
	* Sygnały
	* Rodzaje sygnałów
	* kill
	* killall i pkill
	* Laboratoria
5. Systemy zarządzania pakietami
	* Założenia pakietów oprogramowania
	* Dlaczego pakiety?
	* Rodzaje pakietów
	* Dostępne systemy zarządzania oprogramowaniem
	* Poziomy i różnorodność narzędzi do pakietów
	* Źródła pakietów oprogramowania
	* Tworzenie pakietów oprogramowania
	* Systemy kontroli wersji (Revision Control Systems)
	* Dostępne narzędzia typu Source Control System
	* Jądro Linuxa (kernel) i git
	* Laboratoria
6. RPM
	* RPM (Red Hat Package Manager)
	* Nazewnictwo pakietów
	* Baza RPM i program pomocnicze
	* Zapytania
	* Weryfikacja pakietów
	* Instalacja i usuwanie pakietów
	* Aktualizacja I odświeżanie pakietów RPM
	* Aktualizacja jądra Linuxa
	* rpm2cpio
	* Laboratoria
7. dpkg
	* DPKG (Debian Package)
	* Nazewnictwo pakietów i źródło
	* Zapytania DPKG
	* Instalacja/Usuwanie/Aktualizacja pakietów
	* Laboratoria
8. yum
	* Instalatory pakietów
	* yum
	* Zapytania
	* Weryfikacja pakietów
	* Instalacja/Usuwanie/Aktualizacja pakietów
	* Dodatkowe polecenia yum
	* dnf
	* Laboratoria
9. zypper
	* zypper
	* Zapytania
	* Instalacja/Usuwanie/Aktualizacja pakietów
	* Dodatkowe polecenia zypper
	* Laboratoria
10. APT
	* APT
	* apt
	* Zapytania
	* Instalacja/Usuwanie/Aktualizacja pakietów
	* Czyszczenie
	* Laboratoria
11. Kontrolowanie systemu
	* Kontrolowanie systemu
	* sar
	* Kontrolowanie sieci
	* Logi systemowe
	* Laboratoria
12. Kontrolowanie procesów
	* Kontrolowanie procesów
	* ps
	* pstree
	* top
	* Laboratoria
13. Kontrolowanie i użycie pamięci
	* Kontrolowanie i optymalizacja pamięci
	* /proc/sys/vm
	* vmstat
	* Out of Memory Killer (OOM)
	* Laboratoria
14. Kontrolowanie I optymalizacja I/O
	* Kontrolowanie I/O
	* iostat
	* iotop
	* ionice
	* Laboratoria
15. I/O Scheduling
	* I/O Scheduling
	* Wybór I/O Scheduler
	* Laboratoria
16. System plików Linuxa i VFS
	* Podstawy systemu plików
	* Założenia systemu plików
	* Wirtualny system plików (VFS)
	* Dostępne systemy plików
	* Systemy plików z księgowaniem
	* Specjalne systemy plików
	* Laboratoria
17. Partycjonowanie
	* Popularne rodzaje dysków
	* Geometria dysku
	* Partycjonowanie
	* Tablica partycji
	* Nazywanie dysków
	* Nazwy urządzeń SCSI
	* blkid i lsblk
	* Rozszerzanie partycji
	* Kopia zapasowa I przywracanie tablicy partycji
	* Edytory tablicy partycji
	* fdisk
	* Laboratoria
18. Funkcje systemu plików: Parametry, Tworzenie, Sprawdzanie, Montowanie
	* Rozszerzone parametry
	* Tworzenie i formatowanie systemów plików
	* Sprawdzanie i naprawianie systemów plików
	* Montowanie systemów plików
	* NFS
	* Montowanie przy starcie i /etc/fstab
	* automount
	* Laboratoria
19. Funkcje systemu plików: Swap, Kwoty dyskowe, Wykorzystanie
	* Swap
	* Kwoty dyskowe
	* Użycie systemu plików
	* Użycie dysku
	* Laboratoria
20. Systemy plików Ext2/Ext3/Ext4
	* Funkcje ext4
	* Układ, grupy bloków I superblock na ext4
	* dumpe2fs
	* tune2fs
	* Laboratoria
21. Systemy plików XFS and BTRFS
	* XFS
	* btrfs
	* Laboratoria
22. Szyfrowanie dysków
	* Szyfrowanie systemu plików
	* LUKS
	* cryptsetup
	* Używanie zaszyfrowanej partycji
	* Montowanie przy rozruchu
	* Laboratoria
23. Logical Volume Management (LVM)
	* Logical Volume Management (LVM)
	* Woluminy i grupy woluminów
	* Praca z woluminami logicznymi
	* Zmiana rozmiaru logicznych woluminów
	* Migawki LVM
	* Laboratoria
24. RAID \*\*
	* RAID
	* Poziomy RAID
	* Konfiguracja systemowego RAID
	* Kontrolowanie macierzy RAID
	* RAID Hot Spares
	* Laboratoria
25. Usługi i konfiguracja jądra
	* Przegląd jądra
	* Konfiguracja jądra
	* Opcje rozruchowe jądra
	* sysctl
	* Laboratoria
26. Moduły jądra
	* Moduły jądra
	* Narzędzia modułów
	* modinfo
	* Konfiguracja modułu
	* Laboratoria
27. Urządzenia i udev
	* udev i zarządzanie urządzeniami
	* Węzły urządzeń
	* Reguły
	* Labs
28. Przegląd wirtualizacji
	* Wprowadzenie do wirtualizacji
	* Gospodarz i gość
	* Emulacja
	* Hipernadzorcy
	* libvirt
	* QEMU
	* KVM
	* Laboratoria
29. Przegląd kontenerów
	* Kontenery
	* Wirtualizacja aplikacji
	* Kontenery a maszyny wirtualne
	* Docker
	* Polecenia Dockera
	* Laboratoria
30. Zarządzanie kontami użytkowników
	* Konta użytkowników
	* Zarządzanie kontami użytkowników
	* Zablokowane konta
	* Hasła
	* /etc/shadow
	* Zarzązdzanie hasłami
	* Czas ważności hasła
	* Zastrzeżone powłoki i konta
	* Konto root
	* SSH
	* Laboratoria
31. Zarządzanie grupami
	* Grupy
	* Zarządzanie grupami
	* Prywatne grupy użytkownika
	* Członkostwo w grupie
	* Laboratoria
32. Własność i uprawnienia do pliku
	* Własność i uprawnienia do pliku
	* Uprawnienia dostępowe pliku
	* chmod, chown i chgrp
	* umask
	* ACL
	* Laboratoria
33. Pluggable Authentication Modules (PAM)
	* PAM (Pluggable Authentication Modules)
	* Proces uwierzytelniania
	* Konfiguracja PAM
	* Uwierzytelnianie LDAP
	* Laboratoria
34. Adresy sieciowe
	* Adresy IP
	* Rodzaje adresów IPv4
	* Rodzaje adresów IPv6
	* Klasy adresów IP
	* Maski sieciowe
	* Hostname
	* Laboratoria
35. Urządzenia sieciowe i ich konfiguracja
	* Urządzenia sieciowe
	* ip
	* ifconfig
	* Przewidywalne nazwy interfejsów sieciowych
	* Pliki konfiguracyjne
	* Network Manager
	* Routing
	* DNS and rozwiązywanie nazw
	* Diagnostyka sieci
	* Laboratoria
36. Zapory sieciowe
	* Zapory sieciowe
	* Interfejsy
	* firewalld
	* Strefy
	* Source Management
	* Zarządzanie usługami i portami
	* Laboratoria
37. Uruchamianie i wyłączanie systemu
	* Wyjaśnienie sekwencji rozruchu
	* Programy rozruchowe
	* Pliki konfiguracyjne w /etc
	* Wyłączanie i restartowanie systemu
	* Laboratoria
38. GRUB
	* Grand Unified Boot Loader (GRUB)
	* Ineraktywny wybór w GRUB przy rozruchu
	* Instalacja GRUB
	* Dostosowanie konfiguracji GRUB
	* Laboratoria
39. Init, SystemV, Upstart, systemd
	* Proces init
	* Alternatywy
	* systemd
	* systemctl
	* Rozruch SysVinit
	* chkconfig i usługa
	* Upstart
	* Laboratoria
40. Metody kopii zapasowej i przywracania
	* Podstawy kopii zapasowej
	* Kopia zapasowa a archiwum
	* Strategie i metody kopii zapasowej
	* tar
	* Kompresja (gzip, bzip2 i xz) i kopie zapasowe
	* dd
	* rsync
	* cpio
	* dump i restore
	* mt \*\*
	* Programy do kopii zapasowej
	* Laboratoria
41. Moduły bezpieczeństwa Linuxa
	* Moduły bezpieczeństwa Linuxa
	* SELinux
	* AppArmor
	* Laboratoria
42. Lokalne bezpieczeństwo
	* Lokalne bezpieczeństwo
	* Tworzenie polityki bezpieczeństwa
	* Aktualizacje i bezpieczeństwo
	* Fizyczne bezpieczeństwo
	* BIOS
	* Bootloader
	* Bezpieczeństwo systemu plików
	* Bity setuid/setgid
	* Laboratoria
43. Podstawowe rozwiązywanie problemów
	* Poziomy rozwiązywania problemów
	* Techniki rozwiązywania problemów
	* Co sprawdzić: Sień
	* Co sprawdzić: Integralność plików
	* Błędy procesu rozruchu
	* Uszkodzenia systemu plików i odzyskiwanie
	* Wirtualne konsole
	* Laboratoria
44. Odzyskiwanie systemu
	* Nośnik odzyskiwania systemu i rozwiązywanie problemów
	* Używanie nośnika odzyskiwania systemu
	* Odzyskiwanie systemu
	* Nośnik trybu awaryjnego
	* Tryb awaryjny
	* Single User Mode
	* Laboratoria

**ZADANIE NR 5 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu bezpieczeństwa teleinformatycznego:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania** | **Liczba uczestników** |
| **1.** | Szkolenie z Informatyki Śledczej (computer forensics) lub równoważne | 2 dni | 2 |
| **2** | Testy penetracyjne: atakowanie i ochrona systemów informatycznych lub równoważne | 3 dni | 2 |
| **3.** | Wprowadzenie do zagadnień bezpieczeństwa IT lub równoważne | 3 dni | 2 |
| **4.** | Cyberbezpieczeństwo – warsztaty lub równoważne | 2 dni | 2 |
| **5.** | Warsztaty dla administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego, w tym nt. szacowania i zarządzania ryzykiem - proces analizy i oceny ryzyka lub równoważne | 3 dni | 2 |
| **6.** | Szacowanie złożoności oprogramowania i wycena poprzez zastosowanie analizy punktów funkcyjnych (standard IFPUG) lub równoważne | 2 dni | 2 |

**Szczegółowy opis szkoleń:**

**Ad. 1 Szkolenie z Informatyki Śledczej (computer forensics)**

1. Dowód elektroniczny
	* pojęcie dowodu elektronicznego
	* najlepsze praktyki informatyki śledczej
	* procedury i polityki w firmach
	* aspekty prawne
	* rola i zadania Forensics Analyst, Investigator, Examiner
2. Procesy i procedury w informatyce śledczej
* identyfikacja:
	+ planowanie i rozpoznanie możliwości dowodowych
	+ oględziny miejsca zdarzenia,
	+ identyfikacja sprzętu, urządzeń przenośnych, urządzeń mobilnych, analogowych dokumentów
	+ dokumentowanie miejsca zdarzenia
	+ łańcuch dowodowy
	+ Laboratorium: oględziny miejsca zdarzenia
* zabezpieczenie:
	+ ulotność danych
	+ zabezpieczenie „live” vs. post mortem
	+ klonowanie dysków (metody hardwareowe i softwareowe)
	+ sterylność dysków docelowych
	+ formaty obrazów
	+ funkcje skrótu (MD5, SHA256)LAB: permanentne czyszczenie dysku, wykonywanie kopii binarnej dysku
* analiza:
	+ rodzaje informacji przechowywanych na cyfrowych nośnikach informacji
	+ odzyskiwanie danych
	+ przeszukiwanie przestrzeni przydzielonej, nieprzydzielonej, slack space
	+ dokumentowanie przeprowadzonych badań
	+ korelacja artefaktów
	+ Laboratorium: rekonstrukcja przebiegu przykładowego nadużycia
* raportowanie:
	+ konstrukcja raportu
	+ raportowanie metodą KISS
	+ prezentacja dla Zarządu
	+ Laboratorium: ocena merytoryczna przykładowych raportów
1. Oprogramowanie (komercyjne i open-source)
	* funkcjonalność komercyjnych programów: FTK oraz X-Ways Forensic
	* funkcjonalności narzędzi open source (CAINE, DEFT, NirSoft, RegRipper)
2. Analiza śledcza systemu operacyjnego Windows
	* analiza artefaktów Windows
	* analiza logów systemowych
	* analiza wybranych elementów rejestrów systemowych
	* analiza skompresowanych plików
	* pliki i katalogi użytkownika
	* analiza zawartości kosza systemowego
	* analiza Thumbs.db oraz plików .lnk

**Ad. 2 Testy penetracyjne: atakowanie i ochrona systemów informatycznych**

1. Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?
	* metodyki i rodzaje pentestów
* OSSTMM / OWASP
* Dokumenty opisujące dobre praktyki (NIST/CIS)
	+ różnice pomiędzy pentestami a audytami
1. Organizacja testów penetracyjnych
	* prawne aspekty prowadzenia testów penetracyjnch
	* opracowanie planu testów penetracyjnych
	* popularne problemy spotykane podczas testów penetracyjnych
2. Poszczególne fazy testu penetracyjnego
» Rekonesans
	* pasywne metody zbierania informacji o celu
* wykorzystanie serwerów proxy
* zbieranie i analiza metadanych
* ataki typu social-engineering i APT
* profilowanie pracowników
	+ aktywne metody zbierania informacji o celu
	+ mapowanie sieci ofiary
	+ omijanie firewalli

» Enumeracja podatności

* + rodzaje podatności (buffer overflow, format string, etc.)
* czym jest shellcode?
* mechanizmy DEP/ASLR i ich omijanie
* ROP i heap spray’ing
	+ dopasowywanie kodu exploita do znalezionych podatności
* rodzaje exploitów
* wyszukiwanie exploitów
* analiza przykładowego exploita
* tworzenie własnego exploita
	+ wybór drogi wejścia do systemu

» Atak

* + przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe
* ataki w sieci LAN/WAN/Wi-Fi
* ataki na urządzenia sieciowe (routery, switche, IDS/IPS/WAF, firewalle, load balancery)
* ataki denial of service
* fuzzing
* łamanie haseł
	+ atak przy pomocy exploita zdalnego
* narzędzia wspomagające atak
	+ podniesienie uprawnień do poziomu administratora
* exploity lokalne
* łamanie hashy haseł

» Zacieranie śladów

* + backdoorowanie przejętego systemu
	+ zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej

» Sporządzenie raportu z testu penetracyjnego

* + budowa szczegółowego raportu technicznego
	+ raport dla zarządu
1. Metody ochrony przed atakami
	* idea honeypotów
	* systemy IDS/IPS
	* metody hardeningu systemów Windows
	* metody hardeningu systemów Linux

**Ad. 3 Wprowadzenie do zagadnień bezpieczeństwa IT**

1. Wprowadzenie do tematyki bezpieczeństwa
	* Czym jest bezpieczeństwo IT?
	* Terminologia
2. Organizacje i normy
	* Kryteria oceny poziomu bezpieczeństwa
3. Zarządzanie bezpieczeństwem
	* Inicjowanie procesów bezpieczeństwa IT
	* Tworzenie procedur bezpieczeństwa
	* Zagrożenia i zabezpieczenia rozważane przy tworzeniu polityki bezpieczeństwa
4. Kryptografia oraz środowisko PKI
	* Terminologia i organizacje standaryzujące
	* Algorytmy
	* Funkcje skrótu
5. Protokoły i mechanizmy zabezpieczające transmisję danych
	* SSH
	* PGP
	* SSL/TLS
	* Tunelowanie danych
6. Metody autentykacji użytkowników
	* LDAP
	* Kerberos
7. Sieć I TCP/IP
	* Wprowadzenie do TCP/IP
	* Metody uwierzytelniania w sieciach LAN
	* Bezpieczeństwo sieci bezprzewodowych
8. Skanowanie sieci
	* Mapowanie sieci
	* Skanowanie portów
	* Wykrywanie systemu operacyjnego
9. Opis typowych i aktualnych trendów ataków
	* Typy ataków
	* Zapobieganie
	* Źródła informacji o nowych typach ataków
10. Systemy wykrywania włamań IDS/IPS
	* Host IDS
	* Network IDS
	* Firewalle
	* Typy firewalli
	* Działanie i implementacje
11. Sieci VPN
	* SSL VPN
	* IPsec VPN
12. Dobre praktyki
	* Sposoby weryfikacji spójności sysytemów
	* Sposoby składowania i ochrona logów
	* Co i jak monitorujemy?

**Ad. 4 Cyberbezpieczeństwo - warsztaty**

1. Wstęp
	* Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne
	* Ryzyko i zarządzanie ryzykiem - co to jest ryzyko, podstawowe pojęcia i zasady zarządzania ryzykiem
	* Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola
	* Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować
	* Normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001
2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)
	* Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców
	* Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty
	* Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego
	* Reakcja - jak prawidłowo reagować na ataki socjotechniczne
	* Jak i skąd atakujący zbierają dane na twój temat
	* Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci
3. Atak „na komputery” - demonstracje wraz z objaśnieniem metod ochrony
	* Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących
	* Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC)
	* Ataki przez pocztę e-mail (fałszywe e-maile)
	* Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony
	* Ataki przez komunikatory (Skype, Facebook)
	* Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
	* Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam
4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów
	* Polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych
	* Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko”
	* Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
	* Problem aktualnego oprogramowania i kopii zapasowych
	* Bezpieczna praca z pakietem biurowym Microsoft Office
	* Bezpieczna praca z programem pocztowym
	* Bezpieczna praca z przeglądarką internetową
	* Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty)
5. Aspekty prawne
	* Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
	* Nieautoryzowane użycie systemów komputerowych
	* Rażące zaniedbania związane z wykorzystywaniem sprzętu

**Ad. 5 Warsztaty dla administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego, w tym nt. szacowania i zarządzania ryzykiem - proces analizy
i oceny ryzyka**

1. Prawne aspekty ochrony informacji w systemach teleinformatycznych. Ogólne zasady organizacji systemu TI.
2. Bezpieczeństwo osobowe; Bezpieczeństwo fizyczne; Bezpieczeństwo elektromagnetyczne; Bezpieczeństwo kryptograficzne; Kontrola dostępu. Zakres obowiązków personelu bezpieczeństwa teleinformatycznego; obowiązki kierownika jednostki organizacyjnej oraz pełnomocnika ochrony; obowiązki IBTI oraz Administratora systemu.
3. Bezpieczeństwo teleinformatyczne. Przebieg akredytacji systemu TI: etap planowania; etap projektowania; etap wdrażania; etap eksploatacji; etap wycofywania.
4. Bezpieczeństwo teleinformatyczne. Zasady organizacji wynikające z rozporządzenia PRM z 20 lipca 2011 w sprawie wymagań BTI.
5. Zasady opracowania dokumentacji bezpieczeństwa. Opracowanie Szczególnych Wymagań Bezpieczeństwa (SWB) i Procedur Bezpiecznej Eksploatacji (PBE).
6. Zarządzanie konfiguracją i zabezpieczeniami systemu lub sieci teleinformatycznej. Zasady organizacji i funkcjonowania systemu reagowania na incydenty komputerowe.
7. Wybrane aspekty zarządzanie ryzykiem w systemach TI: Analiza Poziomu Zagrożeń; Szacowanie Ryzyka.
8. Szacowanie ryzyka oraz zarządzanie ryzykiem w świetle ustawy z dnia 5 sierpnia 2010 o ochronie informacji niejawnych – podstawowe wymagania
9. Bezpieczeństwo fizyczne: podstawowe kryteria i sposób określania poziomu zagrożeń; dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń.
10. Bezpieczeństwo fizyczne - ĆWICZENIE: metodyka doboru środków bezpieczeństwa fizycznego; klasyfikacja środków bezpieczeństwa fizycznego; Bezpieczeństwo teleinformatyczne: Systemy Zarządzania Bezpieczeństwem Informacji; Normy ISO 27001 oraz 27005; Bezpieczeństwo teleinformatyczne: Analiza ryzyka: wybór metody oraz etapy szacowania wartości informacji niejawnych i prawnie chronionych przetwarzanych w jednostce organizacyjnej.
11. Bezpieczeństwo teleinformatyczne - ĆWICZENIE: identyfikacja i szacowanie zasobów informacyjnych, identyfikacja zagrożeń i określenia ich poziomu, identyfikacja podatności na ryzyka.
12. Bezpieczeństwo teleinformatyczne - ĆWICZENIE: analiza i ocena ryzyka, dobór środków ochrony, akceptacja ryzyka szczątkowego; utrzymanie złożonego poziomu bezpieczeństwa informacji, przegląd ryzyk i ocena skuteczności wprowadzonego poziomu zabezpieczeń.

## Ad. 6 Szacowanie złożoności oprogramowania i wycena poprzez zastosowanie analizy punktów funkcyjnych (standard IFPUG)

1. Czym jest szacowanie?
* Typowe definicje „dobrego oszacowania”
* Prawdziwy cel szacowania
1. Sprawdzanie swoich umiejętności szacowania
* Prosty test szacowania
1. Wartość dokładnych oszacowań
* Czy lepsze jest oszacowanie za wysokie czy za niskie?
* Szczegółowe dane na temat skuteczności oszacowań w przemyśle oprogramowania
* Korzyści płynące z dokładnego szacowania
1. Wprowadzenie do punktów funkcyjnych
* Historia punktów funkcyjnych
* Sposoby wykorzystania punktów funkcyjnych
1. Podstawy szacowania za pomocą punktów funkcyjnych
* Typy PF
* Reguły zliczania PF
1. Proces zliczania Punktów Funkcyjnych
* Zliczenie zbiorów danych aplikacji
* Zliczenie funkcji transakcyjnych
* Określanie złożoności Punktów Funkcyjnych
1. Obliczenie współczynnika dopasowania wartości VAF (Value Adjustment Factor)
2. Wyliczanie końcowej wartości punktów funkcyjnych
3. Stosowanie metody punktów funkcyjnych do szacowania projektów realizowanych w zaawansowanych technologiach
4. Uproszczone techniki punktów funkcyjnych (metoda holenderska, elementy GUI)
5. Analiza Punktów Funkcyjnych dla rozwijającego się lub modyfikowanego oprogramowania – rozszerzenie metody IFPUG opracowane przez organizację NESMA
* Omówienie publikacji „Function Point Analysis for Software Enhancement”
* Modyfikacja istniejącej funkcjonalności dla funkcji danych
* Modyfikacja istniejącej funkcjonalności dla funkcji transakcyjnych
1. Naliczenie punktów funkcyjnych metodą COSMIC-FFP
* Faza strategii pomiaru
* Faza mapowania
* Faza pomiaru
* Raportowanie pomiaru
1. Szacowanie nakładu pracy
* Obliczanie nakładu pracy przy użyciu nauki szacowania
* Wykresy średniej branżowej nakładu pracy
* Metoda ISBSG
1. Szacowanie harmonogramu
* Podstawowe równanie harmonogramu
* Zasada szacowania pierwszego rzędu Jonesa
* Obliczanie oszacowania harmonogramu przy użyciu nauki szacowania
1. Szacowanie parametrów planowania
* Szacowanie podziału pracy nad projektem
* Szacowanie harmonogramu różnych działań
* Oszacowania kosztów
* Szacowanie powstawania usterek i ich usuwania
* Szacowanie ryzyka i marginesów bezpieczeństwa
1. Style prezentacji oszacowania
* Komunikowanie założeń oszacowania
* Wyrażanie niepewności
* Używanie przedziałów
1. Polityka, negocjacje i rozwiązywanie problemów
* Cechy kierownictwa
* Polityczne wpływy na oszacowanie
* Rozwiązywanie problemu i honorowe negocjacje
1. Warsztat z zakresu szacowania oprogramowania

**ZADANIE NR 6 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu MikroTik:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | MTCNA Mikrotik Certified Network Associate lub równoważne | 3 dni | 3 |
| **2.** | MTCRE MikroTik Certified Routing Engineer lub równoważne | 3 dni | 3 |
| **3.** | MTCSE Mikrotik Certified Security Engineer lub równoważne | 2 dni | 3 |

**Szczegółowy opis szkoleń:**

**Ad. 1 MTCNA Mikrotik Certified Network Associate**

1. TCP/IP – adresacja i podstawy działania
2. Konfiguracja Firewall
3. Konfiguracja prostych sieci bezprzewodowych
4. Kontrola przepływu pakietów (kolejki) – QoS
5. Podstawowa wiedza dotycząca routingu statycznego
6. Konfiguracja bezpiecznych tuneli

**Ad. 2 MTCRE MikroTik Certified Routing Engineer**

1. Routing statyczny
2. Protokoły routingu dynamicznego (OSPF)
3. Sieci VPN (konfiguracja zaawansowana)
4. VLAN

**Ad. 3 MTCSE Mikrotik Certified Security Engineer**

1. Przegląd zagrożeń i ataków na wybrane usługi
2. Omówienie najpopularniejszych ataków
3. Wykrywanie ataków
4. Filtrowanie L2
5. Zaawansowana konfiguracja IP->Firewall
6. Port knocking
7. Ataki typu brute-force
8. Wykrywanie skanowania portów
9. Kryptografia
	* rodzaje szyfrów
	* PKI
10. Tunele:
	* L2TP/IPsec,
	* IPSec
	* SSTP z certyfikatami
11. Omówienie ataków m.in. na:
	* MNDP
	* Winbox
	* DHCP
	* TCP sync
	* UDP
	* ICMP
	* FTP
	* SSH

**ZADANIE NR 7 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu usług programistycznych:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| 1 | NetProg Network Programmability Bootcamp lub równoważne | 5 dni | 3 |
| 2 | Zaawansowane programowanie w C# lub równoważne | 3 dni | 14 |
| 3 | Wzorce projektowe w C# lub równoważne | 4 dni | 12 |
| 4 | Java 8 and Spring lub równoważne | 5 dni | 4 |
| 5 | Spring Boot for Beginners lub równoważne | 2 dni | 4 |
| 6 | Aplikacje Web SPA z frameworkiem Angular lub równoważne | 3 dni | 4 |

**Szczegółowy opis szkoleń:**

**Ad. 1 NetProg Network Programmability Bootcamp**

1. Dlaczego Python
2. Interpretery
3. Podstawy – zmienne, typy, działania
4. IDLE
5. PyCharm
6. Liczby całkowite i zmiennoprzecinkowe (ang. Integers, Floats)
7. Łańcuchy (ang. Strings)
8. Wartości logiczne (ang. Booleans),
9. Instrukcje Warunkowe
10. Pętle, kontrolowanie pętli
11. Pliki
12. Listy
13. Funkcje
14. Moduły
15. Skrypty
16. Przetwarzanie argumentów
17. Krotki (ang. Tuples)
18. Zbiory (ang. Sets)
19. Słowniki (ang. Dictionaries)
20. Stosowanie Systemów Kontroli Wersji – GIT
21. Generatory – podstawy
22. Wyrażenia Regularne (ang. Regular Expressions)
23. Logowanie
24. Wprowadzenie do Obiektości (ang. Objects)
25. Wyjątki (ang. Exception Handling)
26. Przechowywanie danych – ang. Shelves
27. Skrypty expect w pythonie – jak to robić, gdzie są problemy
28. Natywna biblioteka ssh – Paramiko – stosowanie
29. Router Guestshells – jak konfigurować i do czego wykorzystać
30. Natywny Interpreter Pythona ‚on the box’
* stosowanie
* parsowanie zagnieżdżonych struktur – na przykładzie wyników clid()
* wbudowane biblioteki
* zastosowanie pythona do EEM
1. Biblioteka Netmiko – stosowanie
2. Równoległe przetwarzanie
* wprowadzenie do zagadnienia
* omówienie korzyści
* zastosowanie w praktyce (z wykorzystaniem Netmiko)
1. Obróbka konfiguracji urządzeń
* biblioteka NAPALM – stosowanie
* biblioteka CiscoConfParse – stosowanie
1. Współczesne API
* REST
1. NX-API
* Sandbox
* Postman – kolekcje, środowiska, wykorzystanie
* wykorzystanie w skryptach Python
* MIB – przeglądanie
1. YANG i NETCONF
* Teoria
* problemy przy stosowaniu
1. Wprowadzenie do Ansible – stosowanie
2. Kontrolery sieci – na przykładzie (ACI) APIC
* omówienie zasad
* programowanie z wykorzystaniem Python SDK

**Ad.2 Zaawansowane programowanie w C#**

1. Programowanie współbieżne
2. Wstep do wielowatkowosci
3. Klasa Thread
4. Mechanizmy async i await
5. Asynchroniczne wywoływanie metod
6. Synchronizacja dostępu
7. Wyrażenia regularne
8. Rodzaje wzorców
9. Biblioteka Regex
10. Przetwarzanie danych z użyciem wyrażeń regularnych
11. Wykorzystanie grup
12. Zastosowanie wyrażeń regularnych
13. Refleksje
14. Dostęp do klas i właściwości
15. Wykorzystanie refleksji w typach wyliczeniowych
16. Operacje na plikach wykonywalnych
17. Wykorzystanie własnych atrybutów
18. Zaawansowane delegaty
19. Wykorzystanie metod rozszerzeń
20. Drzewa wyrażeń
21. Wzorce projektowe i architektoniczne
22. Singleton
23. Obserwator
24. Fasada
25. Fabryka
26. Stan
27. Strategia
28. Polecenie
29. Iterator
30. MVC
31. MVP
32. MVVM
33. Zaawansowane elementy debuggowania kodu i diagnostyki
34. Klasa Trace
35. Klasa Debug
36. Klasa StackTrace
37. Klasa Stopwatch
38. Zaawansowane elementy Windows Forms
39. Kontrolki plikowe
40. WebBrowser
41. BackgroundWorker
42. Komunikacja sieciowa
43. Architektura Client-Server
44. Klasy WebRequest i WebResponse
45. Obsługa WebServices
46. Obsługa maila
47. Bezpieczeństwo w aplikacjach
48. Obsługa SSL/TLS
49. Szyfrowanie i hashowanie danych
50. Scalanie plików wykonywalnych
51. Dekompilacja plików wykonywalnych
52. Metody zabezpieczeń przed dekompilacją plików wykonywalnych

**Ad. 3** **Wzorce projektowe w C#**

1. Podstawy teoretyczne
	* Informacje ogólne o wzorcach projektowych
	* Zasady SOLID
	* Historia wzorców projektowych
	* Podział wzorców projektowych
2. Wzorce konstrukcyjne
	* Singleton
	* Prototype
	* Object Pool
	* Factory Method
	* Abstract Factory
	* Builder
3. Wzorce strukturalne
	* Proxy
	* Private Class Data
	* Facade
	* Composite
	* Adapter
	* Bridge
	* Decorator
	* Flyweight
4. Wzorce operacyjne
	* Null Object
	* Memento
	* State
	* Strategy
	* Template method
	* Command
	* Mediator
	* Observer
	* Chain of responsibility
	* Iterator
	* Visitor
	* Interpreter
5. Wzorce złożone
	* MVC (Model - View - Controller)
	* MVVM (Model - View - ViewModel)
6. Hands On Lab – projektowanie architektury systemu dla przedstawionego scenariusza, z jednoczesnym wykorzystaniem wielu, spośród poznanych wzorców.

**Ad. 4 Java 8 and Spring**

1. Java 8
* Wyrażenia Lambda
* Predykaty
* Generics
* Java Optional
* Strumienie
* Interfejs API daty i godziny
1. Spring Framework
* Zasady OO
* Wzorzec Odwrócenia Kontroli (Inversion of Control)
* Spring ApplicationContext
* BeanFactory
* Pliki konfiguracyjne XML
1. Wstrzykiwanie Zależności (Dependency Injection),
* Dlaczego Wstrzykiwanie Zależności?
* Wstrzykiwanie zależności przez setery
* Wstrzykiwanie zależności przez konstruktory
* Settery a konstruktory
1. Spring JDBC
* Wzorzec projektowy DAO
* POJO do mapowania bazy danych
* Zapytania do bazy danych
1. Spring MVC
* Wzorzec projektowy MVC
* DispatcherServlet
* Kontrolery
* Modele
* JSPs
1. Spring walidacja
* Mechanizmy walidacji
* Wyświetlanie komunikatów o błędach

**Ad. 5 Spring Boot for Beginners**

1. Wprowadzenie
* Spring Framework: od 2002 do teraz
* Spring Boot: budowanie na platformie Spring
1. Architektura i podstawy Spring Boot
2. Przegląd MVC
3. Inicjalizacja projektu
4. Używanie Groovy do Script Spring Boot
5. Korzystanie z interfejsu CLI Spring Boot
6. Budowanie i wdrażanie aplikacji
7. Używanie szablonów do dynamicznego HTML
8. Uruchamianie Spring Boot Application Starters
9. Dostęp do danych za pomocą Spring Data
10. Konfigurowanie właściwości Spring Boot
11. Spring Boot Metrics i Health Checks
12. Zabezpieczanie aplikacji z pomocą Spring Security
13. Uwierzytelnianie i autoryzacja
14. Interakcja z brokerem JMS

**Ad. 6 Aplikacje Web SPA z frameworkiem Angular**

1. Architektura aplikacji Web
	* Model tradycyjny, komponentowy, SPA
	* Standardy komunikacji z systemem backendowym
2. Platforma Node.js
	* Charakterystyka, architektura i zastosowania
	* Zarządzanie pakietami
	* Konfiguracja i użycie narzędzi do kompilacji, budowania i testowania
3. Studium porównawcze frameworków SPA
4. Angular
	* Wprowadzenie do języka TypeScript i standardu ES6+
	* Architektura frameworka
	* Instancja i konfiguracja frameworka
	* Generowanie artefaktów projektowych, CLI
	* Praca z komponentami ich stanem danych i zdarzeniami
	* Wykorzystanie metod cyklu życia
	* Definiowanie szablonów
	* Dynamiczna manipulacja stylami CSS
	* Komunikacja pomiędzy komponentami, relacja parent-child
	* Obsługa formularzy
	* Formatowanie tekstu z użyciem pipes
	* Routing, nawigacja pomiędzy komponentami
	* Wstrzykiwanie zależności, DI
	* Integracja z RxJS w kontekście komunikacji z API
5. Testowanie - wprowadzenie
	* Charakterystyka i porównanie dostępnych frameworków
	* Struktura testu, implementacja testów
	* Testowanie komponentów

**ZADANIE NR 8 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu metodyki projektów teleinformatycznych:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | Szkolenie SoapUI lub równoważne | 2 dni | 2 |

**Szczegółowy opis szkoleń:**

**Ad. 1 Szkolenie SoapUI**

1. Wprowadzenie
	* Praca z aplikacją SoapUI
	* Testy manualne w SoapUI
2. Podstawy automatyzacji testów
	* Elementy dobrego testu
	* Automatyzacja testów w projekcie
3. Testowanie usług SoapUI
	* Protokół SOAP i odkrywanie funkcji na podstawie WSDL
	* XPath i asercje w testach usług SOAP
	* Zmienne w SoapUI
4. Testowanie usług REST
	* Omówienie konwencji REST
	* Projekt usługi REST w soapUI
	* Asercje w testach REST
5. Symulacja aplikacji
	* Symulacja usług REST
	* Symulacja usług SOAP
	* Dynamiczne generowanie danych
6. Język Groovy
	* Podstawy języka Groovy
	* SoapUI Object Model
	* Generowanie danych z wykorzystaniem Groovy
	* JMS z Groovy
7. Wykorzystanie źródeł danych
	* Wykorzystanie baz danych
	* Wykorzystanie plików CSV
	* Wykorzystanie plików Excel
8. Testy wydajnościowe
	* Testowanie wydajności w SoapUI
	* Wykorzystanie Groovy w testach wydajnościowych
9. Testy bezpieczeństwa
	* Omówienie podstawowych typów ataków
	* Weryfikacja podatności na ataki w SoapUI
10. Dodatkowe aspekty automatyzacji testów
	* Uruchamianie testów poprzez serwer CI
	* Zarządzanie środowiskami
	* Utrzymanie testów (WSDL update)

**ZADANIE NR 9 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu usługi VEEM:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | VMCE Veeam Certified Engineer lub równoważne | 3 dni | 1 |

**Szczegółowy opis szkoleń:**

**Ad. 1 VMCE Veeam Certified Engineer**

* + 1. Wstęp
		2. Omówienie produktów Veeam
	+ Obsługa hypervisorów
	+ Najważniejsze cechy i funkcje rozwiązania Veeam Backup & Replication
	+ Najważniejsze cechy i funkcje rozwiżzania Veeam ONE
	+ Veeam Management Pack
	+ Obsługa oprogramowania vCloud Director
	+ Najważniejsze pojęcia
	+ Metody tworzenia kopii zapasowych
	+ Planowanie
	+ Śledzenie zmienionych bloków (Changed Block Tracking — CBT)
	+ Kompresja i deduplikacja
	+ Zasady przechowywania
		1. Funkcje i sposób działania rozwiazania Veeam ONE
	+ Automatyczne wykrywanie infrastruktury kopii zapasowych i wirtualnej
	+ Kategoryzacja biznesowa
	+ Gotowe alarmy
	+ Monitorowanie bezobsługowe
	+ Raportowanie i pulpity
	+ Gromadzenie danych bez udziału agentów
	+ Funkcje związane z platforma Hyper-V
	+ Wdrażanie rozwiązania Veeam ONE
	+ Narzędzie do oceny dostępne w rozwiązaniu Veeam ONE
		1. Wdrażanie
	+ Architektura rozwiązania
	+ Scenariusze wdrażania
	+ Wymagania wstępne
	+ Uaktualnianie rozwiązania Veeam Backup & Replication
		1. Pierwsza konfiguracja
	+ Dodawanie serwerów
	+ Dodawanie serwera proxy kopii zapasowych VMware
	+ Dodawanie serwera proxy kopii zapasowych Hyper-V typu off-host
	+ Dodawanie repozytoriów kopii zapasowych
	+ Tworzenie kopii zapasowej konfiguracji i jej przywracanie
		1. Wykonywanie kopii zapasowych
	+ Definiowanie zadań tworzenia kopii zapasowych
	+ Definiowanie zadań kopiowania maszyn wirtualnych
	+ Błyskawiczne odzyskiwanie maszyny wirtualnej
		1. Replikacja (zadania replikacji, przełączanie w tryb awaryjny, powrót po awarii)
	+ Omówienie replikacji
	+ Omówienie przełączania w tryb awaryjny
	+ Omówienie powrotu po awarii
		1. SureBackup, SureReplica
	+ Weryfikacja odzyskiwania za pomocą funkcji SureBackup
	+ SureReplica
		1. Przywracanie maszyn wirtualnych i obiektów
	+ Odzyskiwanie danych
	+ Przywracanie obiektów Microsoft Exchange i SharePoint
	+ Praca z programami narzędziowymi Veeam Backup & Replication
		1. Reguła 3-2-1 (kopie zapasowe na taśmie, WAN, dodatkowe egzemplarze kopii zapasowych)
	+ Akcelerator WAN
	+ Powielanie kopii zapasowych w lokalizacji zewnętrznej
	+ Zlecanie operacji przywracania plików i maszyn wirtualnych przy użyciu narzędzia Veeam Backup Enterprise Manager
	+ Interfejs RESTful API narzedzia Veeam Backup Enterprise Manager
	+ HP StoreVirtual VSA
		1. Wersje produktów
	+ Porównanie wersji produktów
	+ Wersje pełna i bezpłatna
		1. Rozwiazywanie problemów
	+ Jak sprawdzić i przeanalizować problem
	+ Szukanie dodatkowych informacji

**ZADANIE NR 10 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu usługi VMware:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | H2UX3S Vmware vSphere:Install, Configure, Manage (v6) lub równoważne | 5 dni | 2 |

**Szczegółowy opis szkoleń:**

**Ad. 1 H2UX3S Vmware vSphere:Install, Configure, Manage (v6)**

1. Centrum danych zdefiniowane programowo
	* Przedstawienie elementów zdefiniowanego programowo centrum danych
	* Gdzie vSphere pasuje do architektury chmury
	* Instalacja i użycie klienta vSphere
	* Przegląd ESXi
2. Tworzenie maszyn wirtualnych
	* Przedstawienie maszyn wirtualnych, sprzęt maszyny wirtualnej i pliki maszyn wirtualnych
	* Twórzenie i praca z maszynami wirtualnymi i szablonami
3. Serwer vCenter
	* Przedstawienie architektury vCenter Server
	* Wdrożenie i konfiguracja urządzenia vCenter Server
	* Użycie vSphere Web Client
	* Zarządzanie obiektami inwentaryzacyjnymi i licencjami serwera vCenter Server
4. Konfigurowanie i zarządzanie sieciami wirtualnymi
	* Tworzenie i zarządzanie standardowymi przełącznikami
	* Konfiguracja zabezpieczeń przełącznika wirtualnego i zasady równoważenia obciążenia
	* Tworzenie, konfiguracja i zarządzanie przełącznikami rozproszonymi vSphere, połączeniami sieciowymi i grupami portów
5. Konfigurowanie i zarządzanie pamięcią wirtualną
	* Protokoły i typy urządzeń pamięci
	* Omówienie hostów ESXi za pomocą pamięci iSCSI i NFS
	* Tworzenie i zarządzanie magazynami danych VMFS i NFS
	* VMware Virtual SAN ™
	* Wirtualne woluminy
6. Zarządzanie maszynami wirtualnymi
	* Używanie szablonków i klonowania do wdrożenia nowych maszyn wirtualnych
	* Modyfikacja i zarządzanie maszynami wirtualnymi
	* Wykonywanie migracji vSphere vMotion i vSphere Storage vMotion
	* Tworzenie migawek maszyn wirtualnych i zarządzanie nimi
	* Tworzenie vApps
	* Typy bibliotek treści oraz sposoby ich wdrażania i używania
7. Zarządzanie zasobami i monitorowanie
	* Wprowadzenie do koncepcji wirtualnego procesora i pamięci
	* Konfigurowanie i zarządzanie pulami zasobów
	* Metody optymalizacji wykorzystania procesora i pamięci
	* Narzędzia do monitorowania zużycia zasobów
	* Alarmy i ich używanie do zgłaszania określonych warunków lub zdarzeń
	* Identyfikacja i rozwiązywanie problemów z zasobami maszyny wirtualnej
	* vRealize Operations Manager do monitorowania i zarządzania centrum danych
8. vSphere HA i vSphere Fault Tolerance
	* Architektura vSphere HA
	* Konfiguracja i zarządzanie klasterem vSphere HA
	* Zaawansowane parametry vSphere HA
	* vSphere Fault Tolerance
	* Włączanie vSphere Fault Tolerance na maszynach wirtualnych
	* Wprowadzenie do replikacji vSphere
	* Używanie vSphere Data Protection do tworzenia kopii zapasowych i przywracania danych
9. Skalowalność hosta
	* Funkcje i zalety klastra vSphere DRS
	* Konfiguracja i zarządzanie klaster vSphere DRS
	* Regóły powinowactwa i anty-powinowactwa
	* Używanie vSphere HA i vSphere DRS razem, w celu zachowania ciągłość biznesowej
10. vSphere Update Manager i utrzymanie hosta
	* Używanie vSphere Update Manager do zarządzania łataniem ESXi
	* Instalacja vSphere Update Manager i wtyczki vSphere Update Manager
	* Tworzenie linii bazowych łatek
	* Używanie profili hosta do zarządzania zgodnością konfiguracji hosta
	* Skanowanie i naprawianie hostów
11. Instalowanie składników vSphere
	* Instalacja ESXi
	* Opcje wdrażania vCenter Server
	* Wymagania dotyczące sprzętu, oprogramowania i bazy danych vCenter Server
	* Instalacja urządzenia vCenter Server Appliance i instancji vCenter Server
	* Instalacja serwera vCenter Server

**ZADANIE NR 11 – opis przedmiotu zamówienia**

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu usługi SAP:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Tytuł szkolenia** | **Czas trwania**  | **Liczba uczestników** |
| **1.** | Introduction to Programming with ABAP lub równoważne | 2 dni | 2 |
| **2..** | ABAP Workbench Foundations lub równoważne | 5 dni | 2 |
| **3** | Programing ABAP Reports lub równoważne | 5 dni | 2 |

**Szczegółowy opis szkoleń:**

**Ad. 1 Introduction to Programming with ABAP**

1. Wprowadzenie do programowania strukturalnego
2. Tworzenie programów ABAP w edytorze ABAP (SE38)
3. Przetwarzanie tekstu źródłowego za pomocą edytora ABAP
4. Testowanie programów przy pomocy debugera
5. Praca z podstawowymi obiektami danych (proste zmienne)
6. Przypisania wartości, obliczenia i wyrażenia arytmetyczne
7. Instrukcje warunkowe, wyrażenia logiczne i warunki logiczne
8. Operacje na ciągach
9. Pętle
10. Implementacja prostego ekranu z polami wejściowymi i wyjściowymi
11. Definiowanie i używanie podprogramów (dlaczego warto przechowywać części programów w podprogramach?)

Kurs powinien być oparty na rozwiązaniach SAP NETWEAVER 200

**Ad. 2 ABAP Workbench Foundations**

1. Przebieg programu ABAP
	* Opis przetwarzania programów ABAP
2. ABAP Workbench Wprowadzenie
	* Przedstawienie środowiska programistycznego ABAP
	* Organizowanie opracowań ABAP
	* Opracowywanie programów
	* Finalizowanie rozwoju
3. Podstawowe elementy języka ABAP
	* Definiowanie elementarnych obiektów danych
	* Korzystanie z podstawowych instrukcji ABAP
	* Praca z debuggerem ABAP
4. Modularyzacja
	* Przedstawienie modularyzacji
	* Modularyzacja za pomocą podprogramów
	* Modularyzacja za pomocą modułów funkcyjnych
	* Implementowanie modułów funkcyjnych
	* Modularyzacja za pomocą BAPI
	* Modularyzacja za pomocą klas globalnych
	* Wdrażanie prostych klas globalnych i metod statycznych
	* Modułowość przy użyciu klas lokalnych
5. Złożone obiekty danych
	* Praca ze strukturami
	* Praca z tabelami wewnętrznymi
6. Modelowanie i odzyskiwanie danych
	* Dane modelowania
	* Odczytywanie rekordów pojedynczej bazy danych
	* Odczytywanie wielu rekordów bazy danych
	* Obsługa innych aspektów dostępu do bazy danych
	* Praca z kontrolami autoryzacji
7. Klasyczny raport ABAP
	* Wdrażanie list ABAP
	* Wdrażanie ekranów wyboru
	* Wdrażanie zdarzeń raportów ABAP
8. Ekran
	* Tworzenie ekranów
	* Tworzenie pól wejściowych / wyjściowych
	* Wdrażanie transportu danych
9. Przeglądarka list SAP
	* Korzystanie z przeglądarki list SAP
10. Web Dynpro ABAP
	* Opisanie Web Dynpro ABAP
	* Implementacja nawigacji w Web Dynpro
	* Wdrażanie transportu danych w sieci Dynpro
11. Narzędzia analizy programu
	* Korzystanie z Inspektora kodu
12. Narzędzia programistyczne ABAP dla SAP NetWeaver
	* Opis narzędzi programistycznych ABAP dla SAP NetWeaver
	* Tworzenie projektu ABAP w Eclipse
13. Standardowe korekty oprogramowania SAP
	* Dostosowywanie standardowego oprogramowania SAP

**Ad. 3 Programing ABAP Reports**

1. Wprowadzenie do raportów ABAP
	* Korzystanie ze standardowych raportów
	* Wdrożenie prostej listy
2. Ekrany wyboru
	* Wdrażanie ekranu wyboru
	* Wdrażanie ekranów wielokrotnego wyboru
	* Wdrażanie kontroli danych wejściowych i tworzenie wariantów
	* Modyfikowanie ekranu wyboru w czasie wykonywania
3. Tworzenie listy przeglądarek SAP (ALV)
	* Korzystanie z funkcji ALV
	* Przygotowanie ekranu kontenera do kontroli siatki ALV
	* Wyświetlanie danych za pomocą siatki ALV
4. Projekt ALV
	* Wariant programowania układu funkcji w siatce ALV
	* Zmiana układu siatki ALV
	* Dostosowanie wyglądu siatki ALV
	* Dostosowanie kontroli siatki ALV za pomocą Katalogu pól
5. Zdarzenia i metody ALV
	* Obsługa zdarzeń kontroli siatki ALV
	* Obsługa dodatkowych zdarzeń w sieci ALV
	* Wywoływanie dodatkowych metod siatki ALV
	* Wdrażanie menu kontekstowych dla siatki ALV
6. Pobieranie danych za pomocą logicznych baz danych
	* Wyjaśnienie funkcjonalności logicznych baz danych
	* Pobieranie danych za pomocą logicznych baz danych
	* Korzystanie z zaawansowanej funkcjonalności logicznych baz danych
7. Pobieranie danych bez logicznych baz danych
	* Odczytywanie danych z wielu tabel bazy danych
	* Implementowanie funkcji agregujących i grupowanie w instrukcji SELECT
	* Implementowanie klauzul HAVING i ORDER BY w instrukcjach SELECT
8. Zew innych programów z raportów ABAP
	* Wywoływanie programów i przekazywanie danych
9. Przetwarzanie w tle
	* Wykonywanie przetwarzania w tle
10. ALV Object Model (OM)
	* Wyświetlanie danych za pomocą modelu obiektowego ALV
	* Dostosowywanie danych wyjściowych modelu obiektu ALV
	* Dostosowanie właściwości ALV