

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup voucherów uprawniających do dostępu do usług szkoleniowych w zakresie wskazanym w opisie poszczególnych zadań produktów.

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. Szkolenia zostaną przeprowadzone na terenie Warszawy, po uzgodnieniu ich terminu z Zamawiającym.
2. Wykonawca przed zawarciem umowy przedstawi harmonogram szkoleń. Wykonawca zapewni co najmniej dwa terminy (oraz co najmniej cztery terminy dla zadania nr 5 temat nr 17, zadania nr 9 temat nr 7) szkoleń z każdego zakresu tematycznego. Dokładne terminy szkoleń zostaną uzgodnione między stronami.
3. W tym samym terminie może odbywać się tylko jedno z wymienionych w każdym zadaniu szkoleń.
4. Wykonawca zapewni salę szkoleniową wraz ze sprzętem niezbędnym do przeprowadzenia szkolenia oraz materiały dydaktyczne dla uczestników szkolenia, odzwierciedlające całość zagadnień poruszanych na szkoleniu.
5. Szkolenia muszą być przeprowadzane w języku polskim.
6. 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.
7. Poprzez pojęcie 1 dzień szkolenia należy rozumieć 8 godzin dydaktycznych gdzie każda godzina dydaktyczna stanowi 45 minut.
8. 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.
9. Termin wykonania usług szkoleniowych nastąpi nie później niż do dnia 31.12.2019 r.
10. Szkolenia wynikające z voucherów powinny być przeprowadzone przez wykładowców posiadających odpowiednie kwalifikacje zawodowe, doświadczenie i wykształcenie umożliwiające ich realizację.
11. Uczestnicy szkoleń wynikających z voucherów otrzymają imienny certyfikat ukończenia każdego szkolenia.
12. Wykonawca nie może powierzyć wykonania przedmiotu umowy osobie trzeciej bez uprzedniej zgody Zamawiającego wyrażonej na piśmie.

ZADANIE NR 5 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu produktów Microsoft:

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	MS-20483 Programming C# lub równoważne	5 dni	2
2	Programowanie .NET – kurs zaawansowany (wraz z rozszerzeniem o punkty opcjonalne) lub równoważne	4 dni	2
3	Understanding Windows Comunication Foundation (WCF) lub równoważne	2 dni	2
4	Wzorce projektowe w C# lub równoważne	3 dni	2
5	Warsztaty automatyzacji testów dot-net lub równoważne	3 dni	2
6	Programowanie WPF lub równoważne	3 dni	2
7	Programowanie w WPF MVVM lub równoważne	3 dni	2
8	MS-20761 Quering Data with T-SQL lub równoważne	5 dni	2
9	MS-20762 Developing SQL Databases lub równoważne	5 dni	3
10	MS-10987 Performance Tuning and Optimazing SQL Databases lub równoważne	4 dni	3
11	MS-20744 Securing Windows Server 2016 lub równoważne	5 dni	3
12	MS-20345-1 Administracja Exchange Server 2016 lub równoważne	5 dni	4
13	MS-20345-2 Projektowanie i wdrażanie	5 dni	4

	Exchange Server 2016 lub równoważne		
14	MS-10961 Automating Administration with Windows PowerShell lub równoważne	5 dni	1
15	MS-2810 Fundamentals of Network Security lub równoważne	4 dni	3
16	MS-2830 Designing Security for Microsoft Networks lub równoważne	3 dni	3
17	MS-20697-1 Implementing and Managing Windows 10 lub równoważne	5 dni	31
18	Microsoft Windows Server 2016 – kurs podstawowy lub równoważne	4 dni	2
19	Infrastruktura Klucza Publicznego (PKI) w Windows Server 2012, 2012 R2 i 2016 lub równoważne	4 dni	6

Szkolenia wymienione w pkt. 1,8-18 muszą być autoryzowane przez Microsoft oraz przeprowadzone przez wykładowców posiadających odpowiednie kwalifikacje zawodowe, doświadczenie i wykształcenie umożliwiające ich realizację, a także powinny być przeprowadzone na sprzęcie, którym dysponuje Wykonawca i w salach szkoleniowych Wykonawcy.

Po zakończeniu szkolenia uczestnicy otrzymają imienny certyfikat ukończenia kursu autoryzowany przez Microsoft.

Szczegółowy opis szkoleń:

Ad. 1. MS-20483 Programming C#

- Składnia C#
 - wprowadzenie do tworzenia aplikacji w C#
 - rodzaje danych, operatory i wyrażenia
 - konstrukcja języka C#
- Tworzenie metod, obsługa wyjątków oraz monitorowanie aplikacji
 - tworzenie i wywoływanie metod
 - tworzenie metod przeładowanych za pomocą parametrów opcjonalnych i wyjściowych
 - obsługa wyjątków
 - monitorowanie aplikacji
- Tworzenie kodu dla aplikacji graficznych
 - implementacja struktur i typów wyliczeniowych
 - organizacja danych w kolekcje

- obsługa zdarzeń
- Tworzenie klas i implementacja bezpiecznych kolekcji
 - tworzenie klas
 - definiowanie i implementacja interfejsów
 - implementacja bezpiecznych kolekcji
- Tworzenie hierarchii klas za pomocą dziedziczenia
 - tworzenie hierarchii klas
 - rozszerzanie klas .NET Framework
 - tworzenie typów rodzajowych
- Czytanie i zapisywanie danych lokalnie
 - czytanie i zapisywanie plików
 - szeregowanie i deszeregowanie danych
 - przygotowywanie strumieni I/O
- Dostęp do baz danych
 - tworzenie i wykorzystanie modeli Entity Data
 - odpytywanie danych za pomocą LINQ
 - aktualizowanie danych za pomocą LINQ
- Dostęp zdalny do danych
 - dostęp do danych poprzez Web
 - dostęp do danych w chmurze
- Projektowanie interfejsu użytkownika dla aplikacji graficznych
 - wykorzystanie XAML do projektowania interfejsu użytkownika
 - dowiązywanie kontrolek do danych
 - stylowanie interfejsu użytkownika
- Udoskonalanie wydajności aplikacji i odpowiedzi
 - implementacja wielowątkowości za pomocą wyrażeń Lambda i zadań
 - przygotowywanie operacji asynchronicznych
 - synchronizacja współbieżności dostępu do danych
- Integracja z kodem niezarządzalnym
 - tworzenie i wykorzystanie obiektów dynamicznych
 - zarządzanie czasem życia obiektów i kontrola zasobów niezarządzalnych
- Tworzenie typów wielokrotnych i zestawów
 - badanie obiektów metadanych
 - tworzenie i wykorzystanie atrybutów niestandardowych
 - generowanie kodu zarządzalnego
 - wersjonowanie, podpisywanie i wdrażanie zestawów
- Szyfrowanie i deszyfrowanie danych
 - implementacja szyfrowania symetrycznego
 - implementacja szyfrowania asymetrycznego.

Ad 2. Programowanie .NET-kurs zaawansowany (wraz z rozszerzeniem o punkty opcjonalne)

- Kolekcje
 - Podstawowe kolekcje: listy, słowniki
 - Kolejki, stosy
 - Kolekcje współbieżne – ConcurrentBag, ConcurrentQueue, ConcurrentDictionary
 - Definiowanie własnych kolekcji

- Typy generyczne
 - Tworzenie klas generycznych
 - Definiowanie metod generycznych
- Kowariancja i Kontrawariancja
- Typy anonimowe
 - Delegaty
 - Wyrażenia lambda
 - Anonimowe delegaty i domknięcia w C#
 - Tworzenie anonimowych obiektów
 - Func / Action
- Typ dynamic i Dynamic Language Runtime
- Metody rozszerzające
- Method Chaining
 - Wprowadzenie do wzorca Method Chaining
 - Definiowanie własnych interfejsów Fluent.
 - Omówienie zalet interfejsów Fluent i przypadków zastosowania
- LINQ
 - Czym jest LINQ
 - Przegląd podstawowych operatorów LINQ
 - LINQ to Objects
 - Łączenie wyrażeń LINQ z wykorzystaniem Method Chaining
 - Operatory projekcji
 - Agregacja
 - Grupowanie
 - Złączenia
 - Zalety stosowania LINQ
 - Własne operatory i rozszerzenia
- Mechanizm refleksji
 - Idea stosowania refleksji
 - Pobieranie informacji o składowych typów
 - Tworzenie obiektów z wykorzystaniem mechanizmu refleksji
 - Wykorzystanie atrybutów
- Wielowątkowość
 - Zastosowanie wielowątkowości w aplikacjach
 - Zarządzanie cyklem życia wątku – tworzenie, usypianie, kończenie
 - Synchronizacja wątków:
 - lock (Monitor)
 - Semaphore
 - ReaderWriterLock
 - WaitEventHandle
 - Zakleszczenia
 - Pule wątków
 - Dobre praktyki związane z wielowątkowością
- Metody asynchroniczne
 - Wykorzystanie Task Parallel Library
 - Użycie async, await
- Wprowadzenie do przetwarzania współbieżnego
 - Idea przetwarzania współbieżnego
 - Instrukcje Parallel LINQ

- Pętle współbieżne
- Wydajność przetwarzania współbieżnego
- Wprowadzenie do programowania sieciowego
 - Gniazda sieciowe
 - Wykorzystanie klas TcpClient i TcpListener do komunikacji sieciowej
 - Wykorzystanie wielowątkowości w programowaniu sieciowym
- Komunikacja http
 - Wykorzystanie komunikacji http w usługach sieciowych
 - Użycie HTTPWebRequest / HTTPWebResponse
 - Zastosowanie uproszczonego interfejsu obsługi http – WebClient
- Programowanie aspektowe (PostSharp)
 - Idea i zalety programowania aspektowego
 - Wprowadzenie do biblioteki PostSharp
 - Definiowanie własnych aspektów
- Kontener IoC (opcjonalne)
 - Wzorzec Inversion of Control
 - Wprowadzenie do kontenera Autofac
 - Rejestrowanie składowych kontenera
 - Rozwiązywanie zależności
 - Automatyczne wstrzykiwanie zależności
 - Zalety i przypadki użycia wzorca IoC
- Testy jednostkowe (opcjonalne)
 - Idea testów jednostkowych i ich wpływ na niezawodność kodu
 - Porównanie najpopularniejszych bibliotek do testów jednostkowych dostępnych w środowisku .NET – MS Test, NUnit, XUnit
 - Tworzenie testów jednostkowych, klasa Assert
 - Uruchamianie testów jednostkowych, wprowadzenie do Test Explorer
 - Użycia rozszerzeń FluentAssertions
 - Wprowadzenie do metodyki Test-driven development
- Biblioteka logująca NLog (opcjonalne)
 - Znaczenie modułu logowania w systemach produkcyjnych
 - Poziomy logowania
 - Tworzenie pliku konfiguracyjnego NLog
 - Definiowanie celów oraz reguł logowania
 - Formatowanie wyjściowe logów

Ad. 3 Understanding Windows Communication Foundation (WCF)

- Architektura zorientowana na usługi
 - SOA - definicja, scenariusze i korzyści
 - WCF i SOA
- Pierwsze kroki w Windows Communication Foundation
 - Umowa serwisowa i umowa danych
 - Realizacja umowy
 - Hostowanie usługi WCF: dlaczego i jak
 - Jak konsumować usługę
 - Punkty końcowe
 - ABC (adres, powiązanie, umowa)
 - Zachowania>

- Dzielenie się umową
 - Tworzenie proxy za pomocą Visual Studio
 - Kiedy i jak korzystać z Fabryki kanałów
- Hosting usługi WCF
 - Zrozumienie roli hosta
 - Dostępne opcje hostingu (niestandardowe a komercyjne) oraz sposób wyboru
 - Hosting w usługach IIS, WAS, AppFabric
 - Długie procesy i hosty usług Windows
 - Tworzenie niestandardowego hosta - dlaczego i jak
 - Konfiguracja i monitorowanie hosta usługi
- Kontrakty, punkty końcowe i zachowania
 - Typy umów
 - Główna rola wiązań
 - Dlaczego ma wiele punktów końcowych
 - Interoperacyjność
 - Domyślne punkty końcowe
- Model komunikacji
 - SOAP a REST
 - Wzorce przesyłania wiadomości, jak wybierać
 - Inicjowanie i współbieżność, łącząc opcje
- Protokoły
 - Zrozumienie stosu kanałów i protokołów
- Niezawodność
 - Zwiększ niezawodność usług, wykorzystując transakcje, kolejki i niezawodne przesyłanie wiadomości
 - Korzystanie z routingu
- Odkrywanie i ogłoszenia
 - Jak odkrywać i udostępniać usługi za pośrednictwem WS-Discovery
- Testowanie i rozwiązywanie problemów
 - Jak indywidualizować błędy i jak sobie z nimi radzić
 - Wyjątki vs Usterki
 - Korzystanie z umów o błędach
 - Jak pisać niestandardowe procedury obsługi błędów i dlaczego
 - Rejestrowanie i śledzenie wiadomości
- Usługi WCF i bezpieczeństwo
 - Holistyczny pogląd
 - Uwierzytelnianie i autoryzacja
 - Model bezpieczeństwa
 - Bezpieczeństwo transportu i wiadomości
- Rozszerzanie WCF
 - Jak i kiedy rozszerzyć WCF poprzez zachowania, inspektorów i rozszerzenia hosta

Ad. 4 Wzorce projektowe w C#

- Manifest Agile
- Reguły
 - DRY
 - KISS

- Prawo Demeter
- Worse is Better
- SOLID
 - Zasada pojedynczej odpowiedzialności
 - Zasada otwarte-zamknięte
 - Zasada podstawiania Liskov
 - Zasada segregacji interfejsów
 - Zasada odwracania zależności
- Wzorce (teoria i ćwiczenia) - Creational Design Patterns
 - Abstract Factory
 - Builder
 - Factory Method
 - Object Pool
 - Prototype
 - Singleton
- Wzorce (teoria i ćwiczenia) - Structural Design Patterns
 - Adapter
 - Bridge
 - Composite
 - Decorator
 - Facade
 - Flyweight
 - Private Class Data
 - Proxy
- Wzorce (teoria i ćwiczenia) - Behavioral Design Patterns
 - Chain of responsibility
 - Command
 - Interpreter
 - Iterator
 - Mediator
 - Memento
 - Null Object
 - Observer
 - State
 - Strategy
 - Template method
 - Visitor
- Wzorce złożone
 - MVC (Model - View - Controller)
 - MVP (Model - View - Presenter)
 - MVVM (Model -View -View Model)

Ad. 5 Warsztaty automatyzacji testów dot-net

- Podstawy programowania
 - Środowisko programistyczne i podstawowe narzędzia: IntelliJ IDEA, Maven, GitHub, JUnit
 - Podstawy programowania w języku Java
 - Praca z repozytorium kodu (na przykładzie Git)

- Zasady Clean Code, czyli tworzenie kodu czytelnego i łatwego w utrzymaniu
- Podstawy testowania
 - Pisanie unit testów
 - Omówienie konceptów Test F.I.R.S.T. oraz Test-Driven Development
 - Omówienie piramidy testów
 - Uruchamianie testów i analiza rezultatów, w tym debugowanie kodu
 - Parametryzacja testów i Data Driven Testing
- Continuous Integration
 - Tworzenie konfiguracji testów automatycznych (buildu) na zdalnym serwerze TeamCity
 - Refaktoryzacja testów i analiza rezultatów działania Continuous Integration
- Selenium WebDriver
 - Tworzenie, uruchomienie i refaktoryzacja testów aplikacji webowej
 - Testowanie aplikacji Web 2.0, korzystającej z technologii Ajax, JavaScript oraz JQuery
- Budowa frameworku testowego
 - Page Object Pattern
 - Techniki i praktyki pozwalające utrzymywać duże ilości testów
- Moduły dodatkowe
 - Selenium Grid, czyli równoległe uruchamianie testów aplikacji webowych
 - Wstęp do Behavior Driven Development na przykładzie SpecFlow
 - Omówienie Specification by Example

Ad.6 Programowanie WPF

- Wprowadzenie
 - Podstawy WPF
 - Podstawy XAML
 - Atrybuty i elementy
 - Markup Extensions
- Panele (LayoutControl)
 - Grid, StackPanel
 - DockPanel, WrapPanel
 - UniformGrid
 - Canvas
- Kontrolki (ContentControl)
 - Label, TextBox
 - Button
 - CheckBox, RadioButton
 - Slider
- Kontrolki wieloelementowe (ItemsControl)
 - ListBox, ListView
 - DataGrid
- Style (Styles)
 - Utworzenie stylu
 - Dziedziczenie stylu
- Szablony (Templates)
 - Szablon danych (DataTemplate)
 - Szablon kontrolki (ControlTemplate)

- Zasoby (Resources)
 - Zasoby statyczne i dynamiczne
 - Zasoby okna i aplikacji
- Wiązanie danych (Binding)
 - Wiązanie kontroltek między sobą (Element Binding)
 - Wiązanie kontroltek z danymi (DataBinding)
 - Kontekst danych (DataContext)
 - Typy wiązania danych
 - Implementacja notyfikacji (INotifyPropertyChanged)
- Konwentery
 - Konwerter wartości (IValueConverter)
 - Konwerter wielowartościowy (IMultiValueConverter)
- Wyzwalacze (Triggers)
 - Wyzwalacze właściwości
 - Wyzwalacze danych

Ad. 7 Programowanie WPF MVVM

- Wprowadzenie
 - Podstawy WPF
 - Podstawy XAML
 - Atrybuty I element
 - Markup Extensions
- Panele (LayoutControl)
 - Grid, StackPanel
 - DockPanel, WrapPanel
 - UniformGrid
 - Canvas
- Kontrolki (ContentControl)
 - Label, TextBox
 - Button
 - CheckBox, RadioButton
 - Slider
- Kontrolki wieloelementowe (ItemsControl)
 - ListBox, ListView
 - DataGrid
- Style (Styles)
 - Utworzenie stylu
 - Dziedziczenie stylu
- Szablony (Templates)
 - Szablon danych (Data Template)
 - Szablon kontroltek (ControlTemplate)
- Zasoby (Resources)
 - Zasoby statyczne I dynamiczne
 - Zasoby okna i aplikacji
- Wiązanie danych (Binding)
 - Wiązanie kontroltek między sobą (Element Binding)
 - Wiązanie kontroltek z danymi (Databinding)
 - Kontekst danych (DataContext)

- Typy wiązania danych
- Implementacja notyfikacji (INotifyPropertyChanged)
- Konwentery
 - Konwerter wartości (IValueConverter)
 - Konwerter wielowartościowy (IMultiValueConverter)
- Wyzwalacze (triggers)
 - Wyzwalacze właściwości
 - Wyzwalacze danych

Wzorzec MVVM

- Wprowadzenie
 - Model View-ViewModel
 - Utworzenie modelu
 - Utworzenie modelu widoku
 - Utworzenie widoku
- Komendy (Command)
 - Implementacja RelayCommand
 - Użycie RelayCommand
- Zachowania
 - Zasada działania
 - Implementacja własnego behavior
 - Komendy do zdarzeń (EventToCommand)

Ad.8 MS-20761 Querying Data with T-SQL

- Wprowadzenie do Microsoft SQL Server 2016
 - podstawowa architektura SQL Server
 - wersje i edycje SQL Server
 - rozpoczęcie pracy z SQL Server Management Studio
- Wprowadzenie do zapytań T-SQL
 - wprowadzenie do T-SQL
 - operacje na zbiorach
 - omówienie logiki predykatów
 - kolejność operacji w składni SELECT
- Tworzenie zapytań SELECT
 - tworzenie prostych składni SELECT
 - usuwanie duplikatów za pomocą DISTINCT
 - wykorzystanie kolumn i aliasów tabel
 - tworzenie prostych wyrażeń CASE
- Tworzenie zapytań do wielu tabel
 - omówienie sprzężeń
 - sprzężenia wewnętrzne
 - sprzężenia zewnętrzne
 - sprzężenia krzyżowe i samosprzężenia
- Sortowanie i filtrowanie danych
 - sortowanie danych
 - filtrowanie danych z wykorzystaniem WHERE
 - filtrowanie z wykorzystaniem opcji TOP oraz OFFSET-FETCH

- praca z wartościami nieznanymi
- Typy danych w SQL Server 2016
 - wprowadzenie do typów danych
 - dane znakowe
 - dane Data i Czas
- Wykorzystanie Data Manipulation Language (DML) do modyfikacji danych
 - wstawianie danych
 - modyfikowanie i usuwanie danych
- Stosowanie funkcji wbudowanych
 - tworzenie zapytań z wykorzystaniem funkcji wbudowanych
 - wykorzystanie funkcji konwersji
 - wykorzystanie funkcji logicznych
 - wykorzystanie funkcji do pracy z NULL
- Grupowanie i agregacja danych
 - wykorzystanie funkcji agregacji
 - wykorzystanie klauzuli GROUP BY
 - filtrowanie grup za pomocą HAVING
- Wykorzystanie podkwerend
 - tworzenie podkwerend z zawartością
 - tworzenie podkwerend skorelowanych
 - wykorzystanie predykcji EXISTS z podkwerendami
- Wykorzystanie wyrażeń tabelowych
 - widoki
 - wbudowane funkcje o wartościach tablicowych
 - tabele pochodne
 - wspólne wyrażenia tabelowe
- Wykorzystanie operatorów na zbiorach
 - tworzenie zapytań z operatorem UNION
 - wykorzystanie EXCEPT oraz INTERSECT
 - wykorzystanie APPLY
- Wykorzystanie funkcji Ranking, Aggregate oraz Offset
 - tworzenie okienek z wykorzystaniem klauzuli OVER
 - przegląd funkcji
- Przystawianie i grupowanie
 - tworzenie zapytań za pomocą PIVOT oraz UNPIVOT
 - praca ze zbiorami grup
- Wykonywanie procedur składowanych
 - odpytywanie danych z wykorzystaniem procedur składowanych
 - przekazywanie parametrów
 - tworzenie prostych procedur składowanych
 - praca z Dynamic SQL
- Programowanie w T-SQL
 - elementy programistyczne T-SQL
 - sterowanie wykonaniem instrukcji programu
- Implementacja obsługi błędów
 - obsługa błędów w T-SQL
 - praca z obsługą wyjątków
- Implementacja transakcji
 - transakcje i silnik bazodanowy

- kontrolowanie transakcji

Ad. 9 MS-20762 Developing SQL Databases

- Wprowadzenie do procesu programowania rozwiązań bazodanowych
 - omówienie platformy SQL Server
 - zadania programisty baz danych SQL Server
- Projektowanie i tworzenie tabel
 - przygotowanie projektu
 - wykorzystanie typów danych
 - praca ze schematami
 - tworzenie i modyfikowanie tabel
- Zaawansowane cechy tabel
 - partycjonowanie danych
 - kompresja danych
 - tabele tymczasowe
- Kontrola poprawności danych z użyciem ograniczników (Constraints)
 - wymuszanie integralności danych
 - spójność domenowa
 - reguły dla encji oraz integralność referencyjna
- Wprowadzenie do indeksowania danych
 - podstawowe pojęcia
 - typy danych a indeksy
 - fizyczna organizacja danych (Heap, Clustered Index, Nonclustered Indexes)
 - indeksy dla pojedynczych kolumn i indeksy złożone
- Strategie optymalnego indeksowania zawartości
 - typowe strategie indeksowania
 - zarządzanie indeksami
 - plany wykonawcze
 - wykorzystanie DTE
 - praca z magazynem zapytań (Query Store)
- Indeksy kolumnowe
 - wprowadzenie
 - budowanie indeksów kolumnowych
 - praca z indeksami kolumnowymi
- Projektowanie i tworzenie widoków
 - wprowadzenie do budowania widoków
 - tworzenie i zarządzanie widokami
 - rozważania wydajnościowe dla konstrukcji wykorzystujących widoki
- Projektowanie i tworzenie procedur składowanych
 - wprowadzenie do procedur składowanych
 - wykorzystanie procedur
 - budowanie sparametryzowanych procedur
 - kontrola kontekstu uruchamiania
- Projektowanie i tworzenie funkcji użytkownika
 - przegląd funkcji
 - projektowanie i tworzenie funkcji skalarnych
 - projektowanie i tworzenie funkcji zwracających dane tabelaryczne
 - zagrożenia w pracy z funkcjami

- konstrukcje alternatywne do użycia funkcji
- Reagowanie na modyfikacje danych poprzez wyzwalacze (Triggers)
 - projektowanie wyzwalaczy
 - tworzenie wyzwalaczy
 - zaawansowane zastosowania wyzwalaczy
- Praca z tabelami pamięciowymi
 - tworzenie tabel typu in-memory
 - tworzenie procedur składanych kompilowanych do kodu maszynowego
- Wykorzystanie kodu zarządzalnego w SQL Server
 - integracja środowiska SQL z CLR
 - tworzenie i publikowanie konstrukcji dla SQL Server w kodzie zarządzalnym
- Składowanie i odpytywanie danych XML
 - wprowadzenie do XML i schematów XML
 - składowanie dokumentów i schematów XML w SQL Server
 - wykorzystanie typu danych XML
 - składnia polecenia FOR XML
 - wprowadzenie do stosowania xQuery
 - praca z fragmentami XML (shredding)
- Praca z danymi przestrzennymi (Spatial Data)
 - wprowadzenie do składowania danych lokalizacyjnych
 - charakterystyka typów danych lokalizacyjnych
 - wykorzystanie danych lokalizacyjnych w aplikacjach
- Składowanie i odpytywanie dużych obiektów binarnych i znakowych
 - uwagi do wykorzystania dużych danych binarnych (BLOB)
 - praca ze strumieniami plikowymi (FILESTREAMS)
 - zapotrzebowanie na zewnętrzną usługę full-text search
- Konkurencyjny dostęp do danych
 - wykorzystanie izolacji migawkowej (Snapshot Isolation)
 - wykorzystanie blokad na poziomie partycji
- Wydajność i monitorowanie rozwiązań
 - system zdarzeń rozszerzonych
 - praca ze zdarzeniami rozszerzonymi
 - bieżące statystyki zapytań
 - dostrajanie konfiguracji plików bazy danych
 - praca z metrykami

Ad. 10 MS-10987 Performance Tuning and Optimizing SQL Databases

- 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
- SQL Server I/O
 - pojęcia podstawowe w operacjach wejścia/wyjścia
 - rozwiązania przechowujące dane
 - konfiguracja i testowanie wejścia/wyjścia
- Struktury baz danych
 - struktura wewnętrzna bazy danych
 - struktura plików danych

- struktura bazy TempDB
- Obsługa pamięci w SQL Server
 - pamięć systemu operacyjnego
 - wykorzystanie przydzielonej pamięci przez SQL Server
 - konstrukcje In-Memory OLTP
- Konkurencyjny dostęp do danych i obsługa transakcji
 - konkurencyjność i transakcje
 - system blokad dostępu
- Konstrukcja statystyk i indeksów
 - wewnętrzna struktura statystyk i ich wykorzystanie w planach realizacji
 - budowa indeksów
 - indeksy kolumnowe
- Uruchamianie zapytań i analiza planu wykonawczego
 - optymalizacja i wykonanie zapytań SQL
 - plany wykonawcze
- Składowanie planów wykonawczych i rekompilacja
 - struktura cache dla planów wykonawczych
 - diagnostyka problemów powstałych przy wykorzystaniu cache
 - składowanie zapytań
- Rozszerzone zdarzenia
 - pojęcia podstawowe
 - wykorzystanie systemu rozszerzonych zdarzeń
- Monitorowanie, śledzenie i zestawianie podstawowych wartości parametrów wydajnościowych
 - monitorowanie i śledzenie wskaźników wydajnościowych
 - baseline - zaakceptowane wartości wskaźników wydajnościowych oraz porównywanie zestawień
- Diagnostowanie 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

Ad. 11 MS-20744 Securing Windows Server 2016

- Wykrywanie zagrożeń przy użyciu narzędzi Sysinternals
 - Przegląd zagadnień związanych z wykrywaniem zagrożeń
 - Narzędzia pakietu Sysinternals wykorzystywane do wykrywania zagrożeń
- Ochrona poświadczeń i dostępu uprzywilejowanego
 - Prawa użytkownika
 - Konta komputerów i usług
 - Ochrona poświadczeń
 - Stacje robocze uprzywilejowanego dostępu i serwery dostępu pośredniego
 - Konfiguracja i wdrożenie Local Administrator Password Solution (LAPS)
- Ograniczanie uprawnień administratora przy użyciu Just Enough Administration (JEA)
- Idea rozwiązania JEA
 - Konfiguracja i wdrożenie (JEA)

- Ograniczanie praw administratora i lasy administracyjne
 - Lasy Enhanced Security Administrative Environment (ESAE)
 - Przegląd rozwiązania Microsoft Identity Manager (MIM)
 - Wdrażanie Just In Time (JIT) and Privileged Access Management (PAM) z wykorzystaniem MIM
- Minimalizowanie zagrożeń związanych z działaniem złośliwego oprogramowania i innych zagrożeń
 - Konfiguracja Windows Defender
 - Wdrożenie AppLocker
 - Konfigurowanie i korzystanie z Device Guard
 - Wdrożenie i korzystanie z Enhanced Mitigation Experience Toolkit (EMET)
- Analiza aktywności z wykorzystaniem zaawansowanych zasad inspekcji oraz analiza zdarzeń
 - Przegląd zasad inspekcji
 - Idea zaawansowanego audytu
 - Konfigurowanie inspekcji i zbierania informacji przy użyciu Windows PowerShell
- Analiza aktywności z wykorzystaniem Microsoft Advanced Threat Analytics (ATA) i Operations Management Suite (OMS)
 - Przegląd funkcjonalności ATA
 - Idea rozwiązania OMS
- Zabezpieczanie infrastruktury wirtualizacji
 - Przegląd zabezpieczania maszyn wirtualnych z użyciem infrastruktury Guarded Fabric
 - Osłanianie i szyfrowane maszyny wirtualne
- Zabezpieczanie wdrażania oprogramowania i infrastruktury serwerowej
 - Korzystanie z Security Compliance Manager (SCM)
 - Wstęp do serwera w wersji Nano
 - Kontenery
- Szyfrowanie danych
 - Planowanie i wdrożenie Encrypting File System (EFS)
 - Planowanie i wdrożenie BitLocker
- Kontrola dostępu do plików i folderów
 - Wstęp do File Server Resource Manager (FSRM)
 - Implementacja zarządzania klasyfikacją i zadania związane z klasyfikacją plików
 - Dynamic Access Control (DAC)
- Wykorzystanie firewalla do kontroli ruchu sieciowego
 - Windows Firewall
 - Rozproszone programowe rozwiązania typu firewall
- Ochrona ruchu sieciowego
 - Zagrożenia wynikające z pracy w sieci i reguły bezpieczeństwa sieciowego
 - Konfiguracja zaawansowanych ustawień DNS
 - Analiza ruchu sieciowego z wykorzystaniem Microsoft Message Analyzer
 - Zabezpieczanie i analiza połączeń związanych z protokołem SMB
- Aktualizowanie Windows Server
 - Przegląd usługi WSUS
 - Wdrażanie poprawek systemowych za pomocą WSUS

Ad. 12 MS-20345-1 Administracja Exchange Server 2016

- Wdrażanie Microsoft Exchange Server 2016
 - wprowadzenie do Exchange Server 2016
 - wymagania i opcje wdrożeniowe Exchange Server 2016
- Zarządzanie serwerami Microsoft Exchange Server 2016
 - zarządzanie Exchange Server 2016
 - wprowadzenie do roli serwera Exchange 2016 Mailbox
 - konfiguracja serwerów roli Mailbox
- Zarządzanie obiektami odbiorców poczty
 - odbiorcy Exchange Server 2016
 - zarządzanie odbiorcami Exchange Server
 - konfiguracja list adresowych i polityk
- Zarządzanie środowiskiem Exchange Server 2016 oraz odbiorcami przy wykorzystaniu Exchange Management Shell
 - wprowadzenie do Exchange management Shell
 - zarządzanie Exchange Server 2016 wykorzystując Exchange Management Shell
 - zarządzanie Exchange Server 2016 wykorzystując skrypty Exchange Management Shell
 - rozwiązywanie problemów dotyczących zastosowania obiektów polityk grupowych
- Wdrażanie dostępu klientów
 - konfiguracja usług dostępu klientów w Exchange Server 2016
 - zarządzanie usługami klienckimi
 - usługi łączności klienckiej i publikacji Exchange Server 2016
 - konfiguracja usługi Outlook on the web
 - konfiguracja usług Exchange Server 2016 dla urządzeń mobilnych
- Zarządzanie wysoką dostępnością Exchange Server 2016
 - wysoka dostępność w Exchange Server 2016
 - konfiguracja wysokiej dostępności baz pocztowych
 - konfiguracja wysokiej dostępności usług Client Access
- Wdrażanie odzyskiwania danych po awarii w Microsoft Exchange 2016
 - wdrażanie usług kopii zapasowej Exchange Server 2016
 - wdrażanie odzyskiwania po awarii Exchange Server 2016
- Konfiguracja i zarządzanie transportem wiadomości
 - wprowadzenie do mechanizmów transportu wiadomości
 - konfiguracja transportu wiadomości
 - zarządzanie regułami transportowymi
- Konfiguracja ochrony antywirusowej, antyspamowej i oprogramowania złośliwego
 - wdrażanie i zarządzanie bezpieczeństwem wiadomości wykorzystując rolę Edge Transport
 - wdrażanie rozwiązań antywirusowych dla Exchange Server 2016
 - wdrażanie rozwiązań antyspamowych dla Exchange Server 2016
- Wdrażanie i zarządzanie wdrożeniem rozwiązań w chmurze: Microsoft Exchange Online
 - wprowadzenie do usług Exchange Online oraz Office 365
 - zarządzanie usługą Exchange Online

- wdrażanie procesu migracji do usług Exchange Online
- Monitorowanie i rozwiązywanie problemów z Microsoft Exchange Server 2016
 - monitorowanie Exchange Server 2016
 - rozwiązywanie problemów z Exchange Server 2016
- Bezpieczeństwo i utrzymanie Exchange Server 2016
 - ochrona Exchange Server 2016 za pomocą kontroli dostępu opartej na rolach (RBAC)
 - konfiguracja logowanej inspekcji na Exchange Server 2016
 - utrzymywanie Exchange Server 2016

Ad. 13 MS-20345-2 Projektowanie i wdrażanie Exchange SERVER

- Planowanie wdrożenia Exchange Server 2016
 - nowości w Exchange Server 2016
 - zbieranie wymagań biznesowych niezbędnych do wdrożenia Exchange Server 2016
 - planowanie wdrożenia Exchange Server
 - projektowanie wdrożenia usług głosowych (Unified Messaging)
- Planowanie i wdrażanie usług roli Mailbox Exchange Server 2016
 - planowanie wymagań sprzętowych na potrzeby Exchange Server
 - planowanie wirtualizacji Exchange Server oraz integracji z usługą Microsoft Azure
 - planowanie i wdrożenie folderów publicznych
- Planowanie i wdrażanie transportu wiadomości
 - projektowanie tras wiadomości
 - projektowanie usług transportowych
 - projektowanie granic routingu wiadomości
 - projektowanie i wdrażanie zgodności wiadomości z wybojami biznesowymi
- Planowanie i wdrażanie dostępu klientów
 - planowanie klientów Exchange Server 2016
 - planowanie dostępu klientów
 - planowanie i wdrażanie serwerów OOS (Office Online Server)
 - planowanie i wdrażanie współpracy SharePoint 2016 z Exchange
 - projektowanie dostępu dla klientów zewnętrznych
- Projektowanie i wdrażanie wysokiej dostępności
 - planowanie wysokiej dostępności dla Exchange Server 2016
 - planowanie równoważenia obciążenia
 - planowanie odporności na awarię lokalizacji
- Utrzymywanie Exchange Server 2016
 - wykorzystywanie aktywnego monitorowania (Managed Availability) do zwiększenia dostępności środowiska Exchange 2016
 - wdrażanie modułu PowerShell Desired State Configuration na potrzeby zarządzania Exchange Server 2016
 - projektowanie bezpieczeństwa wiadomości
 - planowanie bezpieczeństwa wiadomości
 - projektowanie i wdrażanie integracji z AD RMS i Azure RMS

- Projektowanie i wdrażanie retencji wiadomości
 - wprowadzenie do zarządzania rekordami wiadomości i archiwizacji
 - projektowanie kopii archiwalnej (In-Place Archiving)
 - projektowanie i wdrażanie retencji wiadomości
- Projektowanie zgodności wiadomości
 - projektowanie i wdrażanie zapobiegania utracie danych
 - projektowanie i wdrażanie usługi In-Place Hold
 - projektowanie i wdrażanie usługi In-Place eDiscovery
- Projektowanie i wdrażanie współpracy środowisk
 - projektowanie i wdrażanie usług federacyjnych
 - projektowanie współpracy pomiędzy organizacjami Exchange
 - projektowanie i wdrażanie migracji skrzynek między organizacjami Exchange
- Migracja do Exchange Server 2016
 - planowanie migracji z poprzednich wersji Exchange Server
 - przeprowadzenie migracji z poprzednich wersji Exchange Server
- Planowanie wdrożenia hybrydowego Exchange Server
 - podstawy wdrożenia hybrydowego
 - planowanie i przeprowadzenie wdrożenia hybrydowego
 - wykorzystanie zaawansowanej funkcjonalności przy wdrożeniach hybrydowych

Ad. 14 MS-10961 Automating Administration with Windows PowerShell

- Początek pracy z Windows PowerShell
 - informacje ogólne i historia
 - wyszukiwanie i uruchamianie komend
- Praca z Windows PowerShell Pipeline
 - praca z wykorzystaniem pipeline
 - eksport, import i konwertowanie danych
 - filtrowanie obiektów z pipeline
 - wyliczanie obiektów przy wykorzystaniu pipeline
- Zrozumienie funkcjonowania pipeline w Windows PowerShell
 - przekazywanie danych w pipeline wg wartości
 - przekazywanie danych w pipeline wg nazwy właściwości
- Używanie PSProviders i PSDrives
 - zrozumienie PSProviders i PSDrives
 - stosowanie PSDrives
- Formatowanie efektu wyjściowego
 - stosowanie formatowania podstawowego
 - stosowanie formatowania zaawansowanego
 - przekierowanie sformatowanego efektu wyjściowego
- Stosowanie Windows Management Instrumentation / Common Information Model (WMI/CIM)
 - zrozumienie WMI/CIM
 - wysyłanie kwerend dzięki WMI/CIM
 - dokonywanie zmian przy użyciu WMI/CIM
- Przygotowanie do wykonywania skryptów
 - wykorzystanie zmiennych

- aspekty bezpieczeństwa podczas wykonywania skryptów
- praca z poświadczeniami alternatywnymi
- Przejście od komendy do skryptu do modułu
 - przejście od komendy do skryptu
 - przejście od skryptu do funkcji do modułu
 - dołączenie podstawowej obsługi błędów
 - stosowanie podstawowych konstrukcji skryptowych
 - głębsze poznanie metod skryptowych
- Administracja komputerami zdalnymi
 - podstawowe funkcje zdalne
 - używanie sesji zdalnych
 - funkcje zdalne dla administracji delegowanej
- Połączenie wszystkich poznanych elementów
 - planowanie skryptu
- Korzystanie z zadań wykonywanych w tle oraz zadań zaplanowanych
 - używanie zadań wykonywanych w tle
 - używanie zadań zaplanowanych
- Stosowanie zaawansowanych technik i profili Windows PowerShell
 - zaawansowane techniki PowerShell
 - tworzenie profili skryptowych

Ad. 15 MS-2810 Fundamentals of Network Security

- Zapoznanie z typowymi atakami przeciwko urządzeniom sieciowym, zagrożeniami i podatnościami na ataki oraz poznanie działań wykonywanych przez personel, odpowiedzialny za bezpieczeństwo do zabezpieczenia urządzeń sieciowych.
- Zapoznanie ze sposobami wykorzystania kryptografii do zabezpieczania informacji i nabycie umiejętności wyboru odpowiedniej dla organizacji metody szyfrowania.
- Zabezpieczanie informacji w organizacji przy użyciu uwierzytelniania oraz kontroli dostępu.
- Dystrybucja i zarządzanie certyfikatami.
- Zabezpieczanie transmisji danych poprzez identyfikację zagrożeń dla urządzeń sieciowych oraz implementacja zabezpieczeń dla typowych metod transmisji danych, zdalnego dostępu i sieci bezprzewodowych.
- Zabezpieczanie serwerów WWW przeciwko typowym atakom i konfiguracja zabezpieczeń przeglądarek internetowych.
- Zabezpieczanie wiadomości e-mail i komunikatorów internetowych przed typowymi zagrożeniami.
- Zapoznanie z typowymi zagrożeniami usług katalogowych i DNS oraz zastosowanie metod zabezpieczających te usługi.
- Zapoznanie z zagrożeniami dla peryferiów sieci i monitorowanie ich zabezpieczeń.
- Zapoznanie polis zabezpieczeń służących do zarządzania bezpieczeństwem wykonywanych operacji i wykorzystanie tych polis.
- Zapewnienie nieprzerwanego działania przez implementację bezpiecznej strategii odzyskiwania sprawności po awarii, minimalizacji zagrożeń w komunikacji oraz tworzenia bezpiecznych kopii bezpieczeństwa i ich odtwarzania.

- Identyfikacja, odpowiedź na incydenty oraz asystowanie przy formalnym śledztwie w przypadku włamania.

Ad. 16 MS-2830 Designing Security for Microsoft Network

- Wprowadzenie do projektowania bezpieczeństwa dla sieci Microsoft Networks.
- Wprowadzenie do projektowania bezpieczeństwa w zakresie wykorzystania polis grupowych oraz procedur.
- Zdefiniowanie modelu procesowego Microsoft Solutions Framework.
- Omówienie zasad tworzenie zespołu odpowiedzialnego za projektowanie bezpieczeństwa.
- Zapoznanie z elementami podatnymi na niebezpieczeństwo oraz metodami ich wykorzystywania przez intruza.
- Przewidywanie zagrożeń bezpieczeństwa na podstawie modelu STRIDE.
- Tworzenie planu zarządzania ryzykiem.
- Projektowanie zabezpieczeń dla zasobów fizycznych.
- Wyznaczenie zagrożeń i analiza ryzyka w sieci.
- Projektowanie zabezpieczeń komputerów.
- Wyznaczenie zagrożeń i analiza ryzyka dla kont w organizacji.
- Projektowanie zabezpieczeń kont.
- Wyznaczenie zagrożeń i analiza ryzyka dla procesu uwierzytelniania.
- Projektowanie zabezpieczeń dla procesu uwierzytelniania.
- Wyznaczenie zagrożeń i analiza ryzyka dla danych.
- Projektowanie zabezpieczeń danych.
- Wyznaczenie zagrożeń i analiza ryzyka dla transmisji danych.
- Projektowanie zabezpieczeń transmisji danych.
- Wyznaczenie zagrożeń i analiza ryzyka dla urządzeń sieci.
- Projektowanie zabezpieczeń urządzeń sieci.
- Projektowanie polis audytu.
- Projektowanie procedur reakcji na incydenty.
- Analiza ryzyka tworzonego przez użytkowników sieci.
- Projektowanie polityki bezpiecznego używania komputera.
- Analiza ryzyka zarządzania siecią.
- Projektowanie polityki bezpieczeństwa dla zarządzania siecią.

Ad. 17 MS-20697-1 Implementing and Managing Windows 10

- Przegląd Windows 10
 - Wprowadzenie do Windows 10
 - Poruszanie się po interfejsie
- Instalacja Windows 10
 - Przygotowania do instalacji Windows 10
 - Aktualizacja systemu do Windows 10
- Konfiguracja urządzenia
 - Przegląd narzędzi wykorzystywanych do konfiguracji Windows 10
 - Opcje konfiguracji
 - Zarządzanie kontami użytkownika

- Wykorzystanie OneDrive
- Konfiguracja połączenia sieciowego
 - Konfiguracja IP połączenia sieciowego
 - Wdrożenie procesu rozpoznawania nazw
 - Wdrożenie bezprzewodowego połączenia sieciowego
 - Przegląd zagadnień dotyczących dostępu zdalnego
- Zarządzanie magazynem
 - Przegląd opcji dotyczących magazynowania
 - Zarządzanie dyskami, partycjami i wolumenami
 - Utrzymywanie dysków i wolumenów
 - Zarządzanie miejscami do magazynowania
- Zarządzanie plikami i drukarkami
 - Przegląd systemów plików
 - Konfiguracja i zarządzanie dostępem do plików
 - Konfiguracja i zarządzanie folderami udostępnionymi
 - Foldery robocze
 - Zarządzanie drukarkami
- Zarządzanie aplikacjami w Windows 10
 - Przegląd sposobów dostarczania aplikacji do użytkownika
 - Sklep Windows
 - Przeglądarki internetowe
- Zarządzanie bezpieczeństwem danych
 - Przegląd zagrożeń powiązanych z bezpieczeństwem danych
 - Zabezpieczanie danych z wykorzystaniem EFS
 - Wdrażanie i zarządzanie szyfrowaniem dysków funkcją BitLocker
- Zarządzanie bezpieczeństwem urządzeń
 - Korzystanie z ustawień bezpieczeństwa w celu ograniczenia zagrożeń
 - Konfiguracja funkcji kontrola konta użytkownika
- Zarządzanie zabezpieczeniami sieci
 - Przegląd zagrożeń powiązanych z siecią
 - Zapora systemu Windows
 - Zasady zabezpieczeń połączeń
 - Windows Defender
- Zarządzanie Windows 10
 - Aktualizacja Windows 10
 - Monitorowanie Windows 10
 - Optymalizacja wydajności
- Rozwiązywanie problemów i przywracanie danych
 - Zarządzanie urządzeniami i sterownikami
 - Przywracanie plików
 - Przywracanie urządzeń

Ad. 18 Microsoft Windows Server 2016 – kurs podstawowy

Wprowadzenie do Windows Server 2016

- Wymagania sprzętowe Windows Server 2016
- Wersje Windows Server 2016, różnice pomiędzy nimi
- Omówienie podstawowych zadań administracyjnych

Instalacja Windows Server 2016

- Instalacja Windows Server 2016
- Konsola zarządzania serwerem (role, funkcje)
- Konsola mmc
- Tworzenie obrazu NanoServer

Zarządzanie Windows Server 2016

- Omówienie metod zarządzania serwerem lokalnym oraz zdalnym
- Server Manager
- Wstęp do PowerShell
- Zarządzanie środowiskiem NanoServer
- Konsola mmc

Konfiguracja sieci Windows Server 2016

- Konfiguracja sieci w Windows Server 2016
- Firewall systemowy
- Wstęp do IPv6

Aktualizacje - Windows update

- Konfiguracja aktualizacji

Użytkownicy i grupy na serwerze

- Użytkownicy i grupy - zakładanie i zarządzanie

Zarządzanie przestrzenią dyskową

- Narzędzie Disk Management
- Narzędzie diskpart
- Technologia Storage Spaces
- Dyski wirtualne - VHD, VHDX i VHDS

Podstawy wirtualizacji

- Omówienie wirtualizacji
- Zmiany w zakresie wirtualizacji w Windows 2016 (VBS, Nested Virtualization)
- System wirtualny vs maszyna fizyczna
- Konfiguracja usługi Hyper-V
- Rodzaje dysków
- Dodawanie i modyfikowanie maszyny wirtualnej

Serwer plików

- Udostępnianie katalogów
- Systemy plików: rodzina FAT, NTFS, REFS

- Ograniczanie za pomoc File Server Resource Manager oraz Przydziałów NTFS („quota”)

DNS

- Omówienie DNS
- Zasady rozwiązywanie nazw
- Strefy i ich konfiguracja
- Rodzaje rekordów DNS
- Dodawanie i modyfikowanie rekordów DNS

DHCP

- Omówienie DHCP
- Zasada działania
- Adresy nadawane manualnie vs automatycznie
- Rezerwacje

Wprowadzenie do Active Directory

- Omówienie podstawowych zasad działania Active Directory
- Omówienie podstawowych pojęć związanych z Active Directory
- Korzyści płynące z zastosowania Active Directory
- Infrastruktura Active Directory – podział logiczny i fizyczny
- Kontrolery domeny – zadania i funkcje
- RODC - kontroler domeny tylko do odczytu
- Omówienie ról FSMO(Flexible Single Master of Operation /Operations Masters)
 - o Schema Master
 - o Domain Naming Master
 - o PDC Emulator
 - o RID (Relative ID Master)
 - o Infrastructure Master
- Planowanie Active Directory

Instalacja Active Directory

- Instalacja Active Directory
- Baza NTDS.dit
- Zmiana hasła odzyskiwania przy użyciu ntdsutil
- Lokalizowanie ról FSMO

Podstawowe narzędzia administracyjne dla Active Directory

- Omówienie podstawowych narzędzi administracyjnych dla Active Directory
- Wyszukiwanie obiektów w Active Directory

Użytkownicy i grupy w Active Directory

- Użytkownicy i grupy - tworzenie i zarządzanie
- Konfiguracja atrybutów użytkownika

Komputery w Active Directory

- Konta komputerów w domenie
- Dodawanie komputerów do domeny

Jednostki organizacyjne

- Omówienie jednostek organizacyjnych w domenie
- Organizacja kont i grup domenowych przy użyciu jednostek organizacyjnych
- Zastosowanie jednostek organizacyjnych
- Delegacja uprawnień

Polityki bezpieczeństwa

- Wprowadzenie do polityk bezpieczeństwa
- Zastosowania polityk bezpieczeństwa
- Rodzaje polityk bezpieczeństwa
- Kolejność przetwarzania polityk bezpieczeństwa
- Konfigurowanie polityk bezpieczeństwa
- Tworzenie i konfigurowanie GPO (Group Policy Objects)
- Konfigurowanie zakresu obowiązywania GPO
- Konfigurowanie środowiska pracy użytkownika przy użyciu GPO
- Instalacja aplikacji przy użyciu GPO

Monitorowanie pracy serwera

- Monitorowanie pracy serwera
- Narzędzia do monitorowania pracy serwera
- Logi systemowe (Event log)
 - o Filtrowanie zdarzeń w logu
 - o Tworzenie widoków
 - o Przypisywanie zadań do zdarzeń z logu systemowym

Kopia bezpieczeństwa

- Wprowadzenie do prawidłowego wykonywania kopii bezpieczeństwa
- Wykonywanie kopii bezpieczeństwa
- Odtwarzanie kopii bezpieczeństwa

Konfigurowanie shadow copy

Ad. 19 Infrastruktura Klucza Publicznego (PKI) w Windows Server 2012, 2012 R2 i 2016

- Metody kryptograficzne, przegląd, porównanie w poszczególnych wersjach Windows Server

- AD Certification Authorities, projektowanie i wdrażanie Urzędu Certyfikacji
- Zarządzanie i monitorowanie Centrum Certyfikacji
- Tworzenie, wykorzystanie szablonów certyfikatów
- Konfiguracja CRL i OCSP
- Wykorzystanie certyfikatów (SSL/TLS)
- Zabezpieczenie tunelowania VPN certyfikatem
- Agent odzyskiwania kluczy
- Szyfrowanie danych przy użyciu EFS
- Rejestracja urządzeń sieciowych NDES
- Wykorzystanie narzędzi certreq.exe oraz certutil.exe

ZADANIE NR 6 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu produktów sieciowych:

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	ADVRSCBC;Advanced Routing&switching Bootcamp lub równoważne	5 dni	1
2	CIPTV1; Implementing Cisco IP Telephony & Video, Part 1 lub równoważne	5 dni	1
3	CIPTV2; Implementing Cisco IP Telephony & Video, Part 2 lub równoważne	5 dni	1
4	CTCOLLAB; Troubleshooting Cisco IP Telephony&Video lub równoważne	5 dni	1
5	Implementing Cisco Nexus 5000 and 2000 (DCNX5K) lub równoważne	5 dni	1
6	Implementing Core Cisco ASA Security (SASAC) lub równoważne	5 dni	1
7	NGFW Boot; Next-Generation Firewall Bootcamp lub równoważne	5 dni	2
8	SASAA; Implementing Advanced Cisco ASA Security lub równoważne	5 dni	1
9	ARCH (Cisco Network Service Architectures v3.0) lub równoważne	5 dni	2

10	Interconnecting Cisco Networking devices: Accelerated v3.0 lub równoważne	5 dni	1
11	ROUTE; Implementing Cisco IP Routing v 2.0 lub równoważne	5 dni	1
12	SWITCH; Implementing Cisco Switched Networks v 2.0 lub równoważne	5 dni	1

Szkolenia muszą być autoryzowane przez Cisco oraz przeprowadzone przez wykładowców posiadających odpowiednie kwalifikacje zawodowe, doświadczenie i wykształcenie umożliwiające ich realizację, a także powinny być przeprowadzone na sprzęcie, którym dysponuje Wykonawca i w salach szkoleniowych Wykonawcy.

Po zakończeniu szkolenia uczestnicy otrzymają imienny certyfikat ukończenia kursu autoryzowany przez Cisco.

Szczegółowy opis szkoleń:

Ad. 1 ADVRSBC; Advanced Routing&Switching Bootcamp

- Podstawy sieci i urządzeń sieciowych
 - Transmisja sieciowe, dane pakietowe, unicast, multicast, anycast, broadcast, usługi połączeniowe i bezpołączeniowe, topologie
 - Modele ISO/OSI/Internet/warstwowe, enkapsulacja, PDU, SDU
 - Używanie poprawnej terminologii: bity, pakiety, ramki, datagramy, segmenty
 - Organizacje standaryzacyjne i inne: IETF, IEEE, IANA, RIPE, dokumenty RFC
 - Stosy IP Windows i Linux
 - Wgląd w pakiety: sniffery, analizatory, tcpdump, Wireshark
 - Dostęp do urządzeń Cisco poprzez IPv4 oraz IPv6
 - Podstawy protokołów IPv4/IPv6. Wymiana informacji, routing, przełączanie.
 - Protokoły TCP/UDP/inne
 - Metody dostępu do urządzeń Cisco, CLI/GUI/inne
 - Kontrola lokalna i zdalna dostępu Telnet/SSH, linie terminalowe i ich parametry
 - Zarządzanie użytkownikami lokalnymi, no aaa new-model, lokalne AAA
 - Praca z urządzeniami Cisco
 - Protokoły AAA: RADIUS i Tacacs
 - Efektywne CLI: filtry, aliasy, ranges, itp.
 - Systemy plików IOS, protokoły wymiany TFTP/FTP/SCP. Zarządzanie oprogramowaniem.
 - Zarządzanie konfiguracjami, config replace, funkcjonalność archive
 - Podstawy kryptografii: hashe MD5/SHA, szyfrowanie, klucze symetryczne i asymetryczne
 - Bezpieczeństwo konfiguracji, plain text, ochrona haseł
 - Opisywanie interfejsów
 - Właściwe logowanie: ustawienia syslog, NTP, Embedded Syslog Manager (ESM)
 - Bezpieczniki errdisable

- Wprowadzenie do architektur urządzeń sieciowych
- Control / Data / Management plane, dane tranzytowe i lokalne
- Podstawowa praca sieci Ethernet / IP
 - Ethernet i jego standardy: miedziane i optyczne, 10/100G, monitorowanie i diagnostyka, TDR
 - Struktura i adresacja ramek, unicast i multicast, bit U/L
 - Internet Protocol, adresy IPv4, IPv6, planowanie adresacji
 - Multicasty w L3, IPv4 i IPv6
 - IPv4 ARP kontra IPv6 Neighbor Discovery, funkcje ICMPv4 oraz ICMPv6
 - Bezstanowa konfiguracja IPv6 (SLAAC)
 - DHCP w IPv4 oraz IPv6
 - Opcje IPv4, nagłówki rozszerzeń IPv6
 - Praca protokołów TCP oraz UDP
 - Praca hosta w sieci IP, wiele interfejsów, interfejs źródłowy ruchu
 - Brama domyślna, redundancja bramy domyślnej, potrzeba FHRP (HSRP/GLBP/VRRP) w IPv4 and IPv6
 - Wpływ MTU na ruch, fragmentacja w IPv4 i IPv6, PMTUD
 - Znaczniki QoS w ramach i pakietach
 - Podstawy troubleshootingu i diagnostyki, metodologia
 - Narzędzia diagnostyczne IOS oraz Open Source
 - Przełączanie L2 i L3
 - Praca przełącznika Ethernet, tablica przełączania, implementacja, skalowalność
 - Praca routera, tablica routingu, metryka, admin distance, AD255, routing a przełączanie L3
 - Wiele podsieci IP: IPv4 secondary, kilka podsieci IPv6
 - Tablica przełączania: podział na RIB i FIB, przełączanie CEF (Cisco Express Forwarding)
 - Wirtualizacja przełączania L2 i L3, co to jest VPN, taksonomia VPN
 - Wirtualizacja przełączania L2 (VLANy, VLAN database, zarządzanie VLANami, VTP)
 - Wirtualizacja przełączania L3, VRF
 - Łączenie L2 i L3, trunki 802.1q
 - Praca współczesnych przełączników: multilayer i L3, porty switched, routed, subinterfejsy
 - Najprostsza wymiana informacji między tablicami urządzeń, VRF-Lite
 - Klasyczne brydżowanie na routerze
 - Sztuka rysunkowej dokumentacji sieci
 - Brama domyślna kontra trasa domyślna
 - Powiązanie między L2 i L3, timery ARP / ND / MAC
 - Interfejsy wirtualne: null, loopback, tunnel, SVI, virtual-template, NVI
 - Zarządzania VRF-aware, VRF i interfejs źródłowy ruchu wysyłanego przez urządzenie
 - Przeskakiwanie między urządzeniami
 - Networkers Nightmare
 - Podstawy IP multicast
 - Filozofia przełączania multicast
 - Kontrola dołączania do sieci multicast: IGMP/MLD. IGMP snooping.
 - Routing PIM
- Proste topologie sieciowe
 - Zarządzanie topologiami Ethernet/IP,

- Topologie L1, L2, L3, inne
- Zarządzanie topologią L2 poprzez STP: PVSTP, PVRSTP, MST, narzędzia STP
- Architektura sieci kampusowej
- Interakcja między L2 i L3 oraz FHRP
- Topologie wirtualne L2, połączenia fizyczne, logiczne, kanały (PVC, SVC), NBMA
- Technologie starożytne: Frame Relay, ATM
- NBMA w Ethernet: private VLANs
- Ścieżki równoległe: ECMP (Equal-Cost MultiPath), ECMP CEF load-sharing
- Ścieżki równoległe: L2/L3 portchannel, 802.3ad/PAgP/LACP
- Wykrywanie topologii poprzez MAC/ARP/CDP/LLDP, ping, traceroute, STP, itp.
- Nowy paradygmat przełączania – wirtualizacja i tunelowanie
 - Tunelowanie L2: ukrywanie tagów, QinQ, 802.1ad
 - Globalna i lokalna pula VLANów
 - Tunelowanie MAC: Provider Backbone Bridging, 802.1ah
 - Infrastruktura Carrier Ethernet
 - Tunelowanie L3: GRE, non-IP, multipoint GRE, konieczność NHRP, tunele IPv6
 - Ukrywanie adresacji poprzez NATv4, NATv6, ALG, kontrola routingu poprzez NAT
 - Generyczny mechanizm tunelowania: labelki, wprowadzenie do filozofii i aplikacji MPLS
 - Wirtualizacja urządzeń, urządzenia logiczne, VDC, stakowanie, VSS, extenders, moduły wyniesione
 - Wpływ wirtualizacji na zagadnienia projektowe
- Opieka nad ruchem data plane
 - Walidacja ruchu wchodzącego: statyczna, anti-spoofing
 - ACLki na przełączniku L3: PACL, RACL, VACL, implementacja
 - Storm control
 - Prosta kontrola MAC: ACLki MAC, port-security
 - Dynamiczna kontrola, anti-spoofing, DHCP snooping, uRPF, source guard
 - Walidacja ARP
 - Zaawansowana kontrola: 802.1x / EAP / MAB
 - Podstawy QoS: klasyfikacja, oznaczanie, policing, wygładzanie, WRED, QoS na routerze i przełączniku
 - Monitorowanie ruchu tranzytowego
 - Statystyki, liczniki, NetFlow
 - Przechwyt ruchu, SPAN/RSPAN/ERSPAN, VLAN filters, Embedded Packet Capture
 - Budowa konfiguracji Data Plane, makra, wzorce, AutoConf
 - Tworzenie rekomendowanego wzorca konfiguracji Data Plane
 - Networkers Nightmare
- Opieka nad ruchem data plane (c.d.)
 - Podstawy technologii szyfrowania, IPSec (S2S, RA), GETVPN, SSL, Flex, MACSec, 802.3ae
 - Funkcje firewalli, IOS firewall
 - PoE i wsparcie dla telefonii IP, Voice VLAN
- Ruch control i management plane
 - Bardziej zaawansowane zarządzanie, SNMP
 - Automatyka: KRON, EEM (Embedded Event Manager)
 - Bezpieczeństwo infrastruktury, kontrola otwartych usług

- Control Plane Policing (CoPP)
- Budowa rekomendowanej konfiguracji Control i Management plane
- Zaawansowanie przychodzi wraz z dynamiką
 - Narzędzia dynamiki: IP SLA, Enhanced Object Tracking (EOT)
 - Omijanie tablicy routingu poprzez Policy-Based Routing (PBR)
 - Routing statyczny nie taki statyczny: opcje ,ip route' + EOT + IP SLA + EEM
 - Podstawy routingu dynamicznego, trzy źródła informacji routingowej
 - Osiągalność (reachability) kontra topologia (topology)
 - Klasy protokołów routingu: Distance-Vector / Link State / Path Vector
 - System Autonomiczny (AS), routing wewnątrz i pomiędzy AS
 - Co jest złego w RIPie?
 - Uruchamianie routingu EIGRP, OSPF, IS-IS, BGP
 - Użycie komendy ,network' i jej dwie funkcje, konfiguracje AF w OSPF i EIGRP
 - Uwierzytelnianie sąsiadów i informacji routingowej
 - Głębiej w protokoły, rozgłaszanie sieci, natywne i redystrybucja
 - Równoległe procesy routingu, ships in the night, IPv4/IPv6 dual stack, tablice protokołów
 - Kontrolowanie metryki, mechanizmy unikania pętli w protokołach routingu
 - Rozgłaszanie trasy domyślnej
 - Kontrolowanie topologii – segmentacja sieci, podział na regiony, obszary i systemy autonomiczne
 - Znakowanie informacji routingowej, tagi, community
 - Narzędzia kontroli routingu: prefix-listy, route-mapy, RPL (Route Policy Language)
 - Redystrybucja informacji między protokołami. Seed metric.
 - Redukcja prefiksów: sumaryzacja, agregacja, filtrowanie, routing stub (EIGRP, OSPF)
 - Anycast i jego usługi
 - Networkers Nightmare
 - Zaawansowanie przychodzi wraz z dynamiką (c.d.)
 - Więcej skalowalności: czego nie lubi EIGRP, BGP route-reflectors i peery dynamiczne
 - Który protokół routingu jest lepszy? Potrzeba stosowania inżynierii ruchowej.
- Kontrola ścieżki i topologii
 - Proces konwergencji: składowe, analiza procesu
 - Przyspieszanie konwergencji, tuning protokołów, BFD (Bidirectional Forwarding Detection)
 - Zarządzanie FIB: priorytetyzacja prefiksów, Prefix Independent Convergence (PIC)
 - Stabilizacja informacji: dampening
 - Budowa rekomendowanej konfiguracji routingu
 - Fałszywe ścieżki: blackholing
 - Pułapki FHRP: suboptymalny routing, pułapki agregacji prefiksów
 - Celowy blackholing: RTBH (Remote Triggered BlackHoling)
 - Pętle w sieci: informacji, danych, mikropętle, pętle sąsiedztwa, nieskończona rekurencja
 - Budowa ścieżek z wykorzystaniem MPLS: L2VPN, L3VPN, MPLS over GRE
 - Dobrze mieć ścieżkę zapasową: EIGRP feasible successor, IP LFA, BGP AddPath
 - Dodatkowe narzędzia do kontroli ścieżki w BGP: AS_PATH ACL, community lists

- Kontrola ruchu wchodzącego i wychodzącego
- Asymetria routingu, routing nieoptymalny
- Wzajemna redystrybucja, migracja protokołów routingu
- Automatyczna kontrola ścieżki z wykorzystaniem PfR (Performance Routing)
- Networkers Nightmare
- Współczesne sieci
 - Wiarygodne przełączanie: Stateful SwitchOver (SSO), NSF/GR, NSR
 - Nie tylko Ethernet
 - Topologie zaawansowane i sieci nakładkowe
 - VRF a VPN, złożone VPN, wymiana informacji między VPN
 - Proste sieci nakładkowe, L2TPv3, MPLS AToM
 - Sieci nakładkowe NVGRE, OTV, VxLAN
 - Matryce L2; FabricPath, TRILL
 - Aktualne trendy: converged access, Network Function Virtualization (NFV), IoT
 - Programowalność: SDN, REST API, OnePK, Cisco One, REST API
 - Q&A

Ad. 2 Implementing Cisco IP Telephony & Video, Part1 (CIPTV1)

- Wprowadzenie do telefonii IP, architektura środowiska Cisco Collaboration, potrzebne urządzenia, system licencjonowania
- Uruchomienie systemu – podstawowe zadania administracyjne po nowej instalacji
- Dodawanie użytkowników i przypisanie im ról, integracja z LDAP.
- Wprowadzenie do składników środowiska IP telefonii, Implementacja IP Telefonów i Wideotelefonów typu SCCP, SIP
- Konfiguracja elementów planu routingu telefonicznego (dial-plan) do połączeń z zewnętrznym operatorem PSTN za pomocą gateway'a MGCP, H323 lub SIP, nadawanie przywilejów IP Telefonom, implementacja SIP URI.
- Dodatkowe usługi związane z IP Telefonami np.: hunt grupy, kolejkowanie połączeń, przekierowania, przejmowanie połączeń.
- Działanie i konfiguracja voice-gateway'a typu H323 i MGCP
- Działanie i konfiguracja CUBE'a
- Rozszerzenie funkcjonalności systemu IP Telefonii o mostek CFB i serwer MoH, Annuncjator, MTP oraz określenie zasad dostępu do tych usług.
- Usługi typu IP Phone Services
- Urządzenia z rodziny TelePresence (TelePresence Server i TelePresence Conductor)
- Implementacja QoS'a

Ad. 3 Implementing Cisco IP Telephony & Video, Part2 (CIPTV2)

- Wprowadzenie do telefonii IP w środowisku typu multisite, problemy i sposoby ich rozwiązywania.
- Implementacja gateway'ów używając sygnalizacji H323 i MGCP oraz implementacja trunków H323 lub SIP.
- Zasady budowania i implementacja dial-plan'u w środowisku typu multisite z uwzględnieniem środowiska międzynarodowego, E.164 standard, SIP URI
- Wprowadzenie redundancji dla lokalizacji zewnętrznych przy pomocy funkcjonalności SRST, CUCME w trybie SRST.

- Zarządzanie pasmem w sieci WAN przez wdrożenie rozproszonego systemu urządzeń dodatkowych (transcoder'y, MoH, mostki konferencyjne)
- Zarządzanie pasmem w sieci WAN przy pomocy mechanizmów CAC oraz funkcjonalności Automated Alternate Routing (AAR)
- Wdrożenie Device Mobility, Extension Mobility oraz Unified Mobility.
- Cisco VCS i Cisco Expressway, dostęp dla klientów mobilnych typu Jabber
- Usługi Cisco Intercluster Lookup Service (ILS) oraz Global Dial Plan Replication (GDPR), omówienie i konfiguracja
- Cisco Service Advertisement Framework (SAF) oraz Cisco Call Control Discovery (CCD) – omówienie

AD. 4 Troubleshooting Cisco IP Telephony & Video (CTCOLLAB)

- Metodologia rozwiązywania problemów w środowisku Cisco Collaboration
- Narzędzia, raporty przydatne w rozwiązywaniu problemów
- Rozwiązywanie problemów z replikacją baz danych w ramach klastra CUCM
- Rozwiązywanie problemów z połączeniem z bazą LDAP
- Rozwiązywanie problemów z rejestracją IP Telefonów i współpracą CUCM'a z gateway'ami
- Rozwiązywanie problemów związanych z Cisco VCS i Cisco TelePresence (TMS)
- Rozwiązywanie problemów z zestawianiem połączeń wewnętrznych i zewnętrznych w sieci typu single-site
- Rozwiązywanie problemów z zestawianiem połączeń wewnętrznych i zewnętrznych w sieci typu multi-site.
- Problemy z funkcjonalnością ILS i GDPR oraz ich rozwiązywanie
- Problemy dotyczące jakości połączeń i ich rozwiązywanie – QoS
- Rozwiązywanie problemów związanych z funkcjonalnością Device Mobility, Extension Mobility oraz Unified Mobility

Ad. 5 Implementing Cisco Nexus 5000 and 2000 (DCNX5K)

- Architektura sprzętowa i programowa przełącznika Nexus 5500, 5600
- Architektura sprzętowa i cechy programowe przełącznika Nexus 2000
- Omówienie przełączników serii Nexus 3000,4000,6000
- Konfiguracja warstwy drugiej na przełącznikach Nexus 5000
- Diagnostowanie problemów w warstwie drugiej
- Łączenie przełączników Nexus 5000 i 2000
- Konfiguracja virtual Port-Channel (vPC), oraz Enhanced vPC (EvPC)
- Omówienie i konfiguracja protokołu FabricPath
- Omówienie protokołu Fibre Channel (FC)
- Omówienie protokołów FCoE i DCB oraz ich roli w sieciach konwergentnych
- Konfiguracja protokołu FCoE i DCB na przełączniku Cisco Nexus 5000
- Przyłączanie serwerów do sieci DCB/FCoE przy użyciu adapterów CNA
- Diagnostowanie problemów w sieci DCB/FCoE.
- Wstęp do zarządzania i konfigurowania sieciami SAN
- Korzystanie z graficznych narzędzi zarządzających
- Omówienie i konfiguracja przełączników w trybach NPV/NPIV
- Diagnostowanie problemów w sieciach SAN
- Zarządzanie systemem NX-OS i monitoring (System Management)

- Podwyższanie wersji systemu NX-OS (Upgrade)
- **Ćwiczenia**
 - Konfiguracja inicjalna przełącznika Nexus 5000
 - Konfigurowanie zarządzania systemem (System Management)
 - Podwyższanie wersji systemu NX-OS (ISSU)
 - Konfiguracja użytkowników oraz bezpieczeństwa sieciowego
 - Korzystanie z narzędzi graficznych do zarządzania przełącznikami
 - Korzystanie z narzędzi do wykrywania i usuwania problemów
 - Przyłączanie Cisco Nexus 2000 Fabric Extender (static & dynamic pinning mode)
 - Wybrane zagadnienia konfiguracji warstwy drugiej
 - Wykrywanie i usuwanie problemów w warstwie drugiej.
 - Konfiguracja Virtual Port-Channel, oraz Enhanced Virtual Port-channel (EvPC)
 - Konfiguracja Host Virtual Port-channel
 - Konfiguracja protokołu FabricPath
 - Konfiguracja przełącznika Nexus w sieci SAN, we współpracy z przełącznikami MDS
 - Konfiguracja przełącznika w trybach NPV, NPIV
 - Wykrywanie i usuwanie problemów w sieci SAN
 - Konfiguracja FCoE, przyłączanie serwerów do sieci DCB/FCoE przy użyciu adapterów CNA
 - Wykrywanie i usuwanie problemów w sieciach DCB, przy wykorzystaniu protokołu FCoE

Ad. 6 Implementing Core Cisco ASA Security (SASAC)

- Wprowadzenie do Cisco ASA:cechy funkcjonalne, modele, licencjonowanie
- Wdrożenie podstawowej konfiguracji Cisco ASA i zarządzania urządzeniami Cisco ASA za pomocą CLI i ASDM (poziomy bezpieczeństwa interfejsów,VLAN-y, ścieżka domyślna, serwer DHCP), diagnozowanie problemów
- Wdrożenie funkcjonalności typu NAT (object (auto) NAT, manual NAT), diagnozowanie problemów
- Konfiguracja ACL dowiązywanych do interfejsu i globalnie, konfiguracja grup obiektów (object group), konfiguracja serwerów publicznych (public servers), diagnoza problemów
- Konfiguracja routingu statycznego, dynamicznego i wsparcia dla multicastów
- Wdrożenie funkcjonalności kontroli dostępu za pomocą Cisco ASA (modularne podejście do polityki bezpieczeństwa MPF (Modular Policy Framework), inspekcja stanu połączeń, wdrożenie polityki inspekcji na poziomie L3/L4 i na poziomie warstwy aplikacji, jakość usług QoS, diagnozowanie problemów inspekcji na poziomie warstwy aplikacji
- Ocena rozwiązań VPN na Cisco ASA
- Omówienie funkcjonalności typu Connection Profiles, Group Policies, User Policies, VPN accounting i DAP dla SSL VPN
- Wdrażanie usług PKI
- Funkcjonalność i konfigurowanie dostępu typu Clientless SSL VPN na Cisco ASA, diagnozowanie problemów

- Konfiguracja mechanizmów typu AAA dla połączeń typu Clientless SSL VPN na Cisco ASA
- Konfiguracja pełnego dostępu do sieci z wykorzystaniem klienta typu Cisco AnyConnect
- Konfiguracja mechanizmów typu AAA dla połączeń klienta typu Cisco AnyConnect na Cisco ASA, diagnozowanie problemów
- Wdrożenie Cisco AnyConnect IPsec/IKEv2 VPN
- Wdrożenie funkcjonalności wirtualizacji i wysokiej dostępności za pomocą ASA (wirtualne firewalle, redundantne interfejsy, rozwiązanie typu ether-channel, redundancja typu active/standby i typu active/active)

Ad. 7 NGFW Boot; Next-Generation Firewall Bootcamp

- Cisco ASA jako firewall
 - Wstępna konfiguracja firewalla ASA
 - NAT i polityki dostępu
 - Inspekcja protokołów
 - Nowe funkcjonalności w oprogramowaniu ASA
- 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
- 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

Ad. 8 Implementing Advanced Cisco ASA Security v2.1 (SASAA)

Moduł 1: Rodzina produktów Cisco ASA

- Wprowadzenie do Cisco ASA 5500-X
- Wprowadzenie do Cisco ASA v
- Nowe cechy w ASA 9.3 and 9.4.1

Moduł 2: Firewall Cisco ASA typu Identity Based Firewall

- Opis rozwiązania typu Cisco ASA Identity Firewall
- Konfiguracja Cisco CDA
- Konfiguracja Cisco ASA Identity Firewall
- Weryfikacja i diagnoza Cisco ASA Identity Firewall

Moduł 3: Moduł Cisco ASA FirePOWER (SFR)

- Instalacja Cisco ASA FirePOWER Services Module
- Zarządzanie Cisco ASA FirePOWER Services Module za pomocą FirePower Management Center
- Opis usług Cisco ASA 5506-X, 5508-X, and 5516-X FirePOWER

Moduł 4: Integracja ASA z rozwiązaniem typu Cisco Cloud Web Security

- Wprowadzenie do Cisco ASA z Cisco Cloud Web Security
- Konfiguracja Cisco ASA z Cisco Cloud Web Security
- Weryfikacja działania Cisco ASA Cloud Web Security
- Opis polityk Web Filtering Policy w Cisco ScanCenter
- Opis Cisco ASA Cloud Web Security AMP i CTA

Moduł 5: Rozwiązanie typu Cisco ASA Cluster

- Opis cech rozwiązania typu Cisco ASA Cluster
- Opis terminologii Cisco ASA Cluster i przepływ danych
- Konfiguracja Cisco ASA Cluster za pomocą CLI
- Konfiguracja Cisco ASA Cluster za pomocą ASDM
- Weryfikacja działania ASA Cluster
- Diagnozowanie działania Cisco ASA Cluster
- Opis cech rozwiązania typu ASA Cluster dla Cisco ASA 9.1.4 i wersji nowszych

Moduł 6: Cisco ASA Security Group Firewall i CoA

- Wprowadzenie do rozwiązania typu Cisco Security Group Tagging
- Konfiguracja Cisco ASA Security Group Firewall
- Opis cech SGT dla Cisco ASA 9.2.1 i wersji późniejszych
- Opis CoA dla ASA 9.2.1 i wersji późniejszych

Ad. 9 ARCH Cisco Network Service Architectures v3.0

- Zaprojektowanie routingu wewnętrznego w sieci firmowej i zapewnienie wysokiej dostępności
- Projektownie BGP
- Projektowanie sieci rozległych WAN
- Integracja sieci korporacyjnej z Data Center
- Projektowni w zabezpieczeń usług w sieciach
- Projektowanie jakości usług QoS
- Przejście na protokół IPv6

- Projektowanie sieci dla obsługi ruchu multicastowego

Ad. 10 Interconnecting Cisco Networking Devices:Accelerated v3.0

- Budowanie prostej sieci LAN
 - Zapoznanie z podstawowymi funkcjami sieci
 - Model komunikacji Host-to-Host
 - Wprowadzenie do sieci LAN
 - Oprogramowanie urządzeń Cisco IOS
 - Wprowadzenie do przełączników
 - Przełącznik Ethernet, działanie i konfiguracja
 - Rozwiązywanie najczęstszych problemów związanych z funkcjonowaniem przełączników
- Nawiązywanie połączenia z Internetem
 - Model TCP/IP - warstwa Internetu
 - Adresowanie IP oraz podsieci
 - Model TCP/IP - warstwa Transportowa
 - Podstawy routingu
 - Konfiguracja routera Cisco
 - Proces dostarczania pakietów
 - Konfigurowanie routingu statycznego
 - Filtrowanie ruchu przy pomocy list ACL
 - Zestawianie połączenia z siecią publiczną
- Budowa średniej wielkości sieci
 - Wdrażanie sieci VLAN i połączeń typu trunk
 - Przełączane topologie redundantne
 - Implementacja EtherChannel
 - Routing między sieciami VLAN
 - Wykorzystanie urządzeń sieciowych Cisco, jako serwera DHCP
 - Nadmiarowość w warstwie 3(HSRP)
 - Protokoły routingu dynamicznego(RIPv2)
- Wprowadzenie do IPv6
 - Podstawowa konfiguracja IPv6
 - Konfigurowanie statycznego routingu IPv6
- Rozwiązywanie problemów z łącznością
 - W sieciach IPv4
 - W sieciach IPv6
- Bezpieczeństwo urządzeń sieciowych
 - Zabezpieczanie dostępu administracyjnego

- Konfiguracja Port Security, NTP, zewnętrzna autentykacja
- Implementacja protokołu EIGRP
 - EIGRP w sieciach IPv4
 - EIGRP w sieciach IPv6
 - Diagnostyka i rozwiązywanie problemów z EIGRP
- Implementacja protokołu OSPF
 - OSPF w sieciach IPv4
 - OSPF w sieciach IPv6
 - Diagnostyka i rozwiązywanie problemów z OSPF
- Implementacja sieci WAN
 - Technologie sieci WAN
 - Protokół PPP
 - Tunele GRE
 - Konfiguracja EBGP Single Homed
- Zarządzanie urządzeniami sieciowymi
 - Protokoły Syslog i SNMP
 - Rozwój sieci inteligentnych
 - Wprowadzenie do QoS
 - Pliki konfiguracyjne
 - Licencjonowanie

Ad. 11 Implementing Cisco IP Routing v2.0 (ROUTE)

- Koncepcja protokołów routingu dynamicznego, różne metody zdalnych połączeń i ich wpływ na routing, omówienie protokołu RIPng
- Konfiguracja protokołu EIGRP w środowisku sieci IPv4 i IPv6
- Konfiguracja protokołu OSPF w środowisku sieci IPv4 i IPv6
- Implementacja techniki redystrybucji adresów sieciowych wraz z opcjami ich filtrowania
- Implementacja narzędzi kontroli ścieżki przy wykorzystaniu Policy Base Routing i Cisco IOS IP SLA
- Implementacja metod korporacyjnego dostępu do Internetu
- Dobre praktyki w zabezpieczaniu routera Cisco i metody autentykacji w protokołach routingu dynamicznego

Ad. 12 Implementing Cisco Switched Networks v2.0 (SWITCH)

- **Podstawy projektowania sieci**
 - Analiza struktury sieci kampusowej

- Porównanie przełączników warstwy drugiej oraz przełączników wielowarstwowych
 - Implementacja wzorców konfiguracyjnych w środowisku SDM
 - Implementacja protokołu LLDP
 - Implementacja PoE
- **Architektura sieci kampusowej**
 - Implementacja VLANs oraz łączy typu trunk
 - Implementacja protokołu VTP
 - Konfigurowanie usług DHCP dla IPv4 i IPv6
 - Agregacja portów
- **Implementacja protokołu STP**
 - Implementacja RSTP
 - Wprowadzenie rozwiązań poprawiających stabilność protokołów STP
 - Implementacja MSTP
- **Routing między VLAN-ami**
 - Wykorzystanie routera do routowania pakietów między VLAN-ami
 - Konfigurowanie wielowarstwowego przełącznika
- **Sieci wysokiej niezawodności**
 - Konfigurowanie protokołu NTP
 - Implementacja SNMP v.3
 - Konfigurowanie usługi IP SLA
 - Wkorzystanie usługi Port Mirroring do monitorowania ruchu w sieci
 - Wirtualizacja przełączników sieciowych
- **Redundancja w warstwie trzeciej**
 - Konfigurowanie protokołu HSRP
 - Konfigurowanie protokołu VRRP
 - Balansowanie obciążenia za pomocą VRRP
 - Konfigurowanie protokołu GLBP
- **Bezpieczeństwo sieci kampusowej**
 - Implementacja usługi Port Security
 - Zapobieganie burzom broadcastowym
 - Kontrola dostępu klientów
 - Zapobieganie atakom typu spoofin
 - Ochrona do portów typu trunk
 - Konfigurowanie prywatnych VLAN-ów

ZADANIE NR 7 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu produktów ORACLE:

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	Administracja ORACLE 11G XE - wprowadzenie lub równoważne	3 dni	1
2	Oracle SQL - wprowadzenie do pracy z bazą danych lub równoważne	3 dni	1
3	TOAD ADVANCED lub równoważne	1 dzień	4
4	TOAD BASIC lub równoważne	1 dzień	4

Szczegółowy opis szkoleń:

Ad 1. Administracja Oracle 11g XE – wprowadzenie

- Instalacja bazy danych Oracle 10g XE.
- Program SQL Plus.
- Instrukcja SELECT:
 - selekcja wierszy
 - operatory
 - sortowanie
 - funkcje wbudowane SQL
 - grupowania rekordów
 - złączenia tabel i operatory zbiorowe
 - podzapytania
- Polecenia DML.
- Zarządzanie transakcjami - polecenia TCL.
- Polecenie DDL - tworzenie obiektów bazy danych.
- Niezbędne elementy języka PL/SQL.
- Oracle 10g XE - architektura.
- Instancja Oracle.
- Uruchamianie i zamykanie instancji bazy danych.
- Pliki bazy danych.
- Archiwizacja plików dziennika powtórzeń.
- Struktury do składowania danych.
- Mechanizm FLASHBACK.
- Przestrzenie tabel.
- Przestrzeń wycofania.
- Współbieżność w systemie Oracle.
- Użytkownicy bazy danych.
- Uprawnienia i role w bazie danych.

- Profile użytkownika.
- Warsztaty:
 - tryb archive log - utrata pliku danych nie należącego do przestrzeni tabel system,
 - tryb archive log - utrata dowolnego lub wszystkich plików danych i odzyskanie po wykonaniu uprzednio backupu online,
 - odtwarzanie po utracie wszystkich plików kontrolnych,
 - odtwarzanie bazy danych za pomocą rmana - opcja nocatalog,
 - odtwarzanie bazy danych za pomocą rmana - opcja katalog.

Ad. 2 Oracle SQL - wprowadzenie do pracy z bazą danych

- Wprowadzenie do pracy z bazą danych Oracle
 - Architektura bazy danych
 - Model relacyjny bazy danych
 - Użytkownicy, schematy, sesje
 - Narzędzia i pliki konfiguracyjne
- Podstawy zapytań
 - Projekcja, selekcja, sortowanie
 - Operatory, wyrażenia, trójstanowa logika
- Funkcje skalarne
 - Operacje na liczbach i tekstach
 - Funkcje wyliczeniowe
 - Konwersje typów
 - Operacje na datach
 - Obsługa ustawień narodowych i regionalnych
- Agregacje danych
 - Funkcje grupujące
 - Klauzula DISTINCT
 - Klauzule GROUP BY i HAVING
- Złączenia
 - Krzyżowe, wewnętrzne, zewnętrzne
 - Składnia Oracle i ANSI SQL
 - Nietypowe metody łączenia (SELF, NATURAL, ANTY, NONEQUAL)
 - Operatory zbiorowe (UNION, UNION ALL, INTERSECT, MINUS)
- Podzapytania proste
 - Jednowierszowe, wielowierszowe, wektorowe
 - Wielokrotnie zagnieżdżane
 - Podzapytania jako źródła danych (FROM, WITH)
- Podzapytania skorelowane
 - Parametryzowanie podzapytań
 - Operatory EXISTS i NOT EXISTS
 - Podzapytania skalarne
- Budowa repozytorium
 - Tworzenie i zarządzanie tabelami (CREATE, ALTER, DROP, RENAME)
 - Więzy integralności (CONSTRAINTS)
- Manipulowanie danymi (DML)
 - Instrukcje INSERT, UPDATE, DELETE

- Podstawy transakcyjności
- Dodatek – Operacje na dużych zbiorach danych (merge, insert all, insert first)
- Dodatek - Współbieżna praca użytkowników
- Transakcje autonomiczne, punkty zachowania
- Blokady
- FLASHBACK

Ad. 3 Toad Advenced

- Edytory i przeglądraki TOAD
 - Edytor SQL,
 - Edytor PL/SQL,
 - SQL Modeller
- Import i eksport
 - SQL Loader
- Poprawność kodu
 - PL/SQL Debugger
- Optymalizacja kodu
 - SQL Optimizer,
 - Code Pert,
 - Code Tester, B
 - Benchmark Factory
- Administracja bazą danych
 - Moduł DBA
- Funkcje analityczne i raporty
 - Master Detail Browser,
 - Fast Report
- Bazy wiedzy
 - Knowledge XPert for Oracle,
 - Administration,
 - Knowledge XPert for PL/SQL Development
- Moduły wspomagające
 - Toad Data Modeler
- TOAD Tips & Tricks

Ad. 4 TOAD BASIC

- Konfiguracja Toad
- Edytory i przeglądraki TOAD
 - Edytor SQL,
 - Edytor PL/SQL,
 - SQL Modeller
- Zarządzanie obiektami bazy
 - Schema Browser
 - ER Diagram
 - Code Roam Map
- Efektywne konstruowanie zapytań SQL
 - Query Builder
- Import i eksport

- SQL Loader
- Funkcje analityczne i raporty
 - Master Detail Browser,
 - Fast Report
- Moduły wspomagające
 - Toad Data Modeler

ZADANIE NR 8 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu Red Hat

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	RH124 Red Hat System Administration I lub równoważne	5 dni	1
2	RH134 Red Hat system Administration II lub równoważne	5 dni	1

Szczegółowy opis szkoleń:

Ad. 1 RH124 Red Hat System Administration I

- Dostęp do wiersza poleceń.
 - Logowanie do systemu Linux i wykonanie prostych poleceń z użyciem powłoki.
- Zarządzanie plikami z wiersza poleceń.
 - kopiowanie, przenoszenie, tworzenie, usuwanie i organizowanie plików z poziomu powłoki Bash.
- Uzyskiwanie pomocy w Red Hat Enterprise Linux
 - Rozwiązywanie problemów z wykorzystaniem systemów pomocy online i narzędzi wsparcia Red Hat.
- Tworzenie, przeglądanie i edycja plików tekstowych
 - Tworzenie, przeglądanie i edycja plików tekstowych z wyjścia poleceń i w edytorze.
- Zarządzanie lokalnymi użytkownikami i grupami Linux.
 - Zarządzanie lokalnymi użytkownikami i grupami Linux oraz zarządzanie lokalnymi politykami haseł.
- Kontrolowanie dostępu do plików z wykorzystaniem uprawnień systemu plików w Linux.
 - Ustawianie uprawnień do plików i interpretowania efektów różnych kombinacji uprawnień.
- Monitorowanie i zarządzanie procesami Linux.
 - Uzyskiwanie informacji o systemie i kontrola uruchomionych procesów.
- Kontrolowanie usług i daemonów.
 - Zarządzanie i monitoring usług sieciowych i daemonów systemowych z użyciem systemd.
- Konfiguracja i zabezpieczanie usługi OpenSSH.
 - Dostęp i zapewnienie bezpiecznego dostępu do wiersza poleceń w systemach zdalnych z wykorzystaniem OpenSSH.
- Analiza i przechowywanie logów.

- Lokalizowanie i dokładna interpretacja odpowiednich plików logów systemowych w celu rozwiązywania błędów.
- Zarządzanie sieciami w Red Hat Enterprise Linux.
 - Konfiguracja podstawowa sieci Ipv4 w systemach Red Hat Enterprise Linux.
- Archiwizacja i kopiowanie plików pomiędzy systemami.
 - Archiwizacja i kopiowanie pomiędzy różnymi systemami.
- Instalacja i aktualizacja oprogramowania.
 - Pobieranie, instalacja, aktualizacja i zarządzanie pakietami od Red Hat i repozytoriami pakietów yum.
- Dostęp do systemu plików Linux.
 - Dostęp i inspekcja istniejących systemów plików w systemie Red Hat Enterprise Linux.
- Systemy wirtualne.
 - Tworzenie i użytkowanie maszyn wirtualnych z wykorzystaniem KVM i libvirt.

Ad. 2 RH134 Red Hat System Administration II

- Automatyzacja instalacji z wykorzystaniem Kickstart
 - Automatyzacja instalacji systemów Red Hat Enterprise Linux z użyciem Kickstart.
- Wyrażenia regularne.
 - Izolacja i wyszukiwanie zawartości plików tekstowych z wykorzystaniem wyrażeń regularnych i narzędzia grep.
- Tworzenie i edycja plików tekstowych w vim.
 - Edytor vim.
- Harmonogram zadań w Linux.
 - Planowanie zadań w celu automatycznego wykonania w przyszłości.
- Zarządzanie priorytetami procesów w Linux.
 - Wpływ priorytetów na działanie procesów w Linux.
- Kontrola dostępu do plików poprzez listy kontroli dostępu (ACL).
 - Zarządzanie bezpieczeństwem plików z wykorzystaniem list kontroli dostępu POSIX.
- Zarządzanie SELinux.
 - Zarządzanie zachowaniem SELinux w celu zapewnienia bezpieczeństwa systemu.
- Podłączenie do sieciowych usług zarządzania tożsamością.
 - Konfiguracja systemu w celu użycia usług zarządzania tożsamością.
- Tworzenie dysków, partycji i systemów plików w Linux.
 - Zarządzanie prostymi partycjami i systemami plików.
- Zarządzanie woluminami logicznymi (LVM).
 - Zarządzanie LVM z poziomu wiersza poleceń.
- Dostęp do usług udostępniania plików w sieci z wykorzystaniem NFS.
 - Bezpieczny dostęp do udziałów NFS.
- Dostęp do usług udostępniania plików w sieci z wykorzystaniem SMB.
 - Wykorzystanie autofs i wiersza poleceń do montowania/odmontowania udziałów SMB. 1
- Kontrola i rozwiązywanie problemów związanych z procesem startu systemu Red Hat Enterprise Linux.
- Ograniczenie komunikacji sieciowej z użyciem zapory sieciowej.

- Konfiguracja podstawowej zapory sieciowej.

ZADANIE NR 9 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu bezpieczeństwa teleinformatycznego:

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	C)IHE Certified Incident Handling Engineer lub równoważne	5 dni	1
2	C)PTE – Certified Penetration Testing Engineer lub równoważne	5 dni	6
3	C)PEH – Certied Professional Ethnical Hacker lub równoważne	5 dni	1
4	C)ISSM – Cetified Information Systems Manager lub równoważne	5 dni	1
5	Testy penetracyjne: atakowanie i ochrona systemów informatycznych	3 dni	4
6	Informatyka śledcza (computer forensics) - specjalista	5 dni	8
7	Wprowadzenie do zagadnień bezpieczeństwa IT	3 dni	32
8	C)PTC Certified Penetration Testing Consultant lub równoważne	4 dni	1

Uczestnicy szkoleń wynikających z voucherów otrzymają imienny certyfikat ukończenia każdego szkolenia a w przypadku szkoleń wskazanych w pkt. 1 i 8 dodatkowo vouchery na egzaminy – ważne przez 6 mcy od zakończenia szkolenia.

Szczegółowy opis szkoleń:

Ad.1 C)IHE - Certified Incident Handling Engineer

- Wprowadzenie
 - Informacje na temat szkolenia
 - Co to jest Incident Handling?
 - Terminologia: zdarzenie naruszenia bezpieczeństwa informacji

- Co to jest Incydent bezpieczeństwa?
- Dlaczego należy wdrożyć obsługę incydentów
- Podstawowe cele procesu zarządzania incydentami
- Omówienie postępowania podczas incydentu
- Sześć etapów obsługi incydentów
- Zagrożenia, podatności i exploity
 - Przegląd zagrożeń
 - Malware
 - Botnety
 - IP Spoofing
 - ARP Cache Poisoning
 - DNS spoofing
 - Session Hijacking
 - Buffer Overflows
 - Phishing
 - Social Engineering
 - Narzędzie: SET
 - Atak: Denial of Service
 - Ataki na sieci bezprzewodowe
 - Vulnerability Assessment
 - Testy penetracyjne
 - Exploity
- Etap 1: Przygotowanie
 - Polityki i procedury
 - Wsparcie zarządu
 - Zespół obsługujący incydenty
 - Organizacja pracy zespołu
 - Formy komunikacji
 - Raportowanie o incydencie
 - Szkolenia techniczne
 - Security Awareness
 - Podstawowe technologie
 - Anti-virus
 - SEIM
 - User Identity
 - Ticketing System
 - Digital Forensics
 - eDiscovery
 - Data Backup/Recovery
- RTIR
 - System ticketowy Request Tracker
 - Komponenty systemu RT
 - Ticket
 - Kolejki
 - RTIR – RT Incident Response
 - RTFM – RT FAQ Manager
- Wstępne przygotowania
 - Zestaw narzędzi do obsługi incydentów
 - Czego szukać?
 - Dane ulotne

- Windows Log Events
- Windows Services
- Windows Network Usage
- Windows Scheduled Tasks
- Windows Accounts
- Windows Tools
- Linux Log Events
- Linux Processes

Ad. 2 C)PTE – Certified Penetration Testing Engineer

- Przegląd kursu
- Biznesowa i techniczna logistyka testów penetracyjnych
- Podstawy systemu Linux
- Zbieranie informacji
- Wykrywanie systemów
- Enumeracja
- Wykrywanie podatności
- Malware
- Ataki na systemy Windows
- Ataki na systemy UNIX/Linux
- Zaawansowane techniki wykorzystywania
- Testowanie sieci bezprzewodowych
- Podśluchiwanie sieci i systemy IDS
- Ataki na bazy danych
- Ataki na aplikacje webowe
- Dokumentacja i tworzenie raportu
- Zabezpieczanie systemów Windows - Powershell
- Przeprowadzenie testów przy pomocy Powershell

Laboratorium:

- Wprowadzenie do środowiska laboratoryjnego
- Podstawy systemu Linux
- Korzystanie z narzędzi do raportowania
- Zbieranie informacji
- Wykrywanie systemów
- Enumeracja
- Wykrywanie podatności
- Malware
- Atakowanie systemów Windows
- Atakowanie systemów Linux / Unix
- Zaawansowane techniki wykrywania podatności i ich wykorzystywania
- Podśluchiwanie sieci i systemy IDS
- Atakowanie baz danych
- Atakowanie aplikacji webowych

Ad. 3 C)PEH Certified Professional Ethical Hacker

- Wprowadzenie do zasad etycznego hackingu

- Podstawy systemu Linux
- Protokoły
- Kryptografia
- Łamanie haseł
- Złośliwe oprogramowanie
- Urządzenia bezpieczeństwa
- Zdobywanie informacji – pasywny rekonesans
- Socjotechnika
- Aktywny rekonesans
- Wykrywanie i ocena podatności
- Ataki sieciowe
- Hackowanie serwerów
- Hackowanie web aplikacji
- Hackowanie sieci bezprzewodowych
- Utrzymywanie dostępu i zacieranie śladów

Laboratorium:

- Wprowadzenie do środowiska laboratoryjnego
- Podstawy systemu Linux
- Protokoły sieciowe
- Kryptografia
- Łamanie haseł
- Złośliwe oprogramowanie
- Zdobywanie informacji
- Wykrywanie i ocena podatności
- Przechwytywanie i analiza ruchu sieciowego
- Włamania do systemów Windows
- Atakowanie baz danych
- Atakowanie web aplikacji
- Tylne furtki (Backdoors)

Ad. 4 C)ISSM – Cetified Information Systems Security Manager

- Wprowadzenie
- Zarządzanie bezpieczeństwem informacji
- Zgodność i zarządzanie ryzykiem informacji
- Opracowywanie i zarządzanie programem bezpieczeństwa informacji
- Zarządzanie incydentami bezpieczeństwa informacji

Ad. 5 Testy penetracyjne: atakowanie i ochrona systemów informatycznych

- Podstawowe informacje
 - Wprowadzenie do tematyki testów penetracyjnych
 - Włamanie Audyt/Auydt/Test penetracyjny
 - Aspekty prawne
 - Metodologie i fazy testu penetracyjnego
 - Planowanie (Planning)
 - Rekonesans (Reconnaissance)
 - Skanowanie (Scanning)

- Wtargnięcie (Gaining Access)
 - Utrzymanie dostępu (Maintaining Access)
 - Zatarcie śladów (Covering Tracks)
 - Raportowanie (Reporting)
- Footprinting i rekonesans
 - Pasywne i aktywne zbieranie informacji
 - Inżynieria społeczna
- Skanowanie
 - Skanowanie sieci
 - Skanery automatyczne
- Enumeracja podatności
 - Rodzaje podatności
 - Wyszukiwanie podatności
- Wtargnięcie
 - Rodzaje ataków
 - Łamanie haseł
 - Ataki na sieci LAN
- Utrzymanie dostępu
 - Backdoory i rootkity
- Zatarcie śladów
- Raportowanie
 - Dobre praktyki
- Omijanie systemów IDS oraz Firewall
- Honyputy
- Buffer Overflow i Fuzzing
- Metody ochrony systemów
 - Dobre praktyki
- Warsztaty
 - Rekonesans podmiotów, skanowanie sieci, serwerów, usług
 - Google Hacking
 - Enumeracja zasobów
 - Penetracja sieci
 - Ataki phishingowe

Ad. 6 Informatyka śledcza (computer forencis) – specjalista

- Definicje przestępczości komputerowej - cyberprzestępczości funkcjonujące w literaturze przedmiotu.
- Klasyfikacja i podział cyberprzestępczości dokonywanej przez organizacje i instytucje międzynarodowe.
- Ochrona systemów komputerowych w wybranych przepisach prawa krajowego:
 - Ustawa Kodeks Karny
 - Ustawa o ochronie danych osobowych
 - Ustawa o ochronie własności intelektualnej
 - Ustawa o świadczeniu usług drogą elektroniczną.
- Klasyfikacje osób naruszających bezpieczeństwo systemów informatycznych, motywy ich działania oraz stosowane metody działania.
- Procedury postępowania w przypadku wystąpienia i ujawnienia incydentu , reakcja na incydent w oparciu o politykę bezpieczeństwa , organizacja zespołu reagowania.

Terminologia związana z incydem, analiza po włamaniowa oraz śledztwem komputerowym.

- Wytyczne i standardy określające prowadzenie analizy po włamaniowej, śledztwa komputerowego oraz zabezpieczanie dowodów cyfrowych.
- Zabezpieczanie danych cyfrowych w systemach informatycznych w tym:
 - działania w ramach tzw. TRIAGE -
 - Zabezpieczanie danych ulotnych w działającym systemie
 - Zabezpieczanie danych cyfrowych w systemie statycznym (wyłączonym)
 - Zabezpieczenia danych zdalnie (Cloud)
 - Zabezpieczanie danych sieciowych
 - Zabezpieczanie danych w systemach „Big Data”.
- Formaty stosowanych obrazów informatyki śledczej wraz ze sposobami ich weryfikacji.
- Dokumentowanie i przechowywanie dowodów cyfrowych na potrzeby dalszego postępowania po incydencie.
- Wyposażenie techniczne, sprzętowe i programowe, niezbędne w śledztwie informatycznym.
- Analiza logów systemowych. Ustalenie historii wykonywanych operacji. Śledzenie zmian w systemie.
- Wykrywanie rootkitów, backdorów, keyloggerów, koni trojańskich i innych anomalii systemowych.
- Analiza komunikatorów systemowych, przegląd historii odwiedzanych stron WWW i analiza poczty elektronicznej.
- Analiza potencjalnych kanałów dostępu do badanego komputera.
- Ukrywanie danych na dysku twardym. Sposoby ukrywania danych oraz metody ich ujawniania.
- Steganografia - ukrywanie tajnych informacji w "zwykłych" plikach. Dostęp do informacji zaszyfrowanych.
- Metody omijania haseł systemowych. Programy łamiące hasła zabezpieczające dostęp do plików.
- Odzyskiwanie danych usuniętych z dysku twardego, płyt CD/DVD, kart pamięci oraz pendrive'ów.
- Aplikacje i programy używane do odzyskiwania danych.
- Bezpieczne i trwałe usuwanie danych. Procedury kasowania danych oznaczonych klauzulą poufne i ściśle tajne.

Ad. 7 Wprowadzenie do zagadnień bezpieczeństwa IT

- Wprowadzenie do tematyki bezpieczeństwa
 - Czym jest bezpieczeństwo IT?
 - Terminologia
- Organizacje i normy
 - Kryteria oceny poziomu bezpieczeństwa
- Zarządzanie bezpieczeństwem
 - Inicjowanie procesów bezpieczeństwa IT
 - Tworzenie procedur bezpieczeństwa
 - Zagrożenia i zabezpieczenia rozważane przy tworzeniu polityki bezpieczeństwa
- Kryptografia oraz środowisko PKI
 - Terminologia i organizacje standaryzujące

- Algorytmy
- Funkcje skrótu
- Protokoły i mechanizmy zabezpieczające transmisję danych
 - SSH
 - PGP
 - SSL/TLS
 - Tunelowanie danych
- Metody autentykacji użytkowników
 - LDAP
 - Kerberos
- Sieć I TCP/IP
 - Wprowadzenie do TCP/IP
 - Metody uwierzytelniania w sieciach LAN
 - Bezpieczeństwo sieci bezprzewodowych
- Skanowanie sieci
 - Mapowanie sieci
 - Skanowanie portów
 - Wykrywanie systemu operacyjnego
- Opis typowych i aktualnych trendów ataków
 - Typy ataków
 - Zapobieganie
 - Źródła informacji o nowych typach ataków
- Systemy wykrywania włamań IDS/IPS
 - Host IDS
 - Network IDS
 - Firewalle
 - Typy firewalli
 - Działanie i implementacje
- Sieci VPN
 - SSL VPN
 - IPsec VPN
- Dobre praktyki
 - Sposoby weryfikacji spójności systemów
 - Sposoby składowania i ochrona logów
 - Co i jak monitorujemy?

Ad. 8 C)PTC Certified Penetration Testing Consultant

- Budowanie zespołu przeprowadzającego testy bezpieczeństwa,
- Automatyzacja skanowania NMAP,
- Eksploatacja systemu (cel procesu eksploatacji, dostosowywanie eksploatacji, przykładowe drogi ataku, unikanie),
- Fuzzing z wykorzystaniem Spike,
- Przepełnienie bufora,
- Stack Based Windows Buffer Overflow (poszukiwanie podatności, wykorzystanie kodu),
- Bezpieczeństwo aplikacji webowych,
- Linux Stack Smashing,
- Windows Exploit Protection,

- Mechanizmy SEH i ASLR,
- Tworzenie raportów z testów penetracyjnych.

Szkolenie powinno zawierać ćwiczenia laboratoryjne.

ZADANIE NR 10 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu backup:

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	Veem Certified Engineer (VMCE) lub równoważne	3 dni	1

Szczegółowy opis szkolenia:

Ad.1 Veeam Certified Engineer (VMCE)

- Omówienie portfolio produktów Veeam
 - Produkty Veeam
 - Veeam Availability Suite™
 - Kluczowe pojęcia
- Wdrożenia
 - Podstawowe komponenty i ich interakcje
 - Opcjonalne komponenty
 - Scenariusze wdrożenia
 - Wymagania wstępne
 - Proces aktualizacji oprogramowania Veeam Backup & Replication™
- Początkowa konfiguracja
 - Dodawanie serwerów
 - Dodawanie VMware Backup Proxy
 - Dodawanie Hyper-V Off-host Backup Proxy
 - Dodawanie repozytoriów kopii zapasowych
 - Wykonywanie i odtwarzania kopii zapasowej konfiguracji
 - Zarządzanie ruchem sieciowym
 - Globalne ustawienia dla powiadomień
 - Zapoznanie z interfejsem użytkownika
- Ochrona
 - Tworzenie zadań kopii zapasowej
 - Tworzenie punktów przywracania wykorzystując VeeamZIP™ oraz Quick Backup
 - Kopiowanie kopii zapasowych
 - Replikacja
 - Tworzenie zadań kopiowania maszyn wirtualnych lub plików
- Weryfikacja
 - Weryfikacja odtwarzania z wykorzystaniem SureBackup®
 - SureReplica
- Odtwarzanie całych maszyn wirtualnych

- Odtwarzanie danych
- Praca z narzędziami Veeam Backup & Replication
- Różne formy odtwarzania oparte o repliki
- Odtwarzanie obiektów
 - Odtwarzanie na poziomie elementów (item-level)
 - Odtwarzanie plików systemu gościa
- Zaawansowana ochrona danych
 - Wsparcie dla urządzeń taśmowych
 - Wsparcie dla systemów pamięci masowej typu SAN
 - Wsparcie dla systemów pamięci masowych z funkcją deduplikacji
 - Veeam Cloud Connect
 - Veeam Backup Enterprise Manager
 - Wsparcie dla VMware vCloud Director
- Cechy i funkcje oprogramowania Veeam ONETM
 - Auto-wykrywanie infrastruktury wirtualnej oraz infrastruktury kopii zapasowych
 - Kategoryzacja biznesowa
 - Predefiniowane ostrzeżenie
 - Monitorowanie bez nadzoru
 - Raportowanie i tablice informacyjne (dashboards)
 - Zbieranie danych bez wykorzystania agentów
 - Specyficzne cechy dla Hyper-V
 - Veeam One Deployment
 - Veeam One Assessment Tool
- Warianty produktów
 - Porównanie dostępnych wariantów produktów
 - Pełne i darmowe tryby funkcjonowania
- Diagnozowanie i rozwiązywanie problemów (troubleshooting)
 - Jak zidentyfikować problem
 - Jak oceniać i analizować problematyczne zagadnienia (issue)
 - Poszukiwanie dodatkowych informacji
 - Wsparcie ze strony Veeam

ZADANIE NR 11 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu usług programistycznych:

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	WebServices with SOAP and WSDL Basics lub równoważne	2 dni	3
2	Combined JAVA, .NET and Web Application Security lub równoważne	3 dni	3
3	Docker dla software developerów I administratorów IT lub równoważne	1 dzień	2
4	Tworzenie aplikacji internetowych w języku Java z wykorzystaniem Framework Vaadin 8 - od podstaw	5 dni	2

5	Tworzenie usług sieciowych (Web Services) w języku Java	5 dni	2
---	---	-------	---

Szczegółowy opis szkoleń:

Ad. 1 WebServices with SOAP and WSDL Basics (Wprowadzenie do technologii usług sieciowych (WebServices))

- Przegląd usług sieciowych (Web Services).
 - Dlaczego potrzebujemy rozproszonej aplikacji (Web Services)?
 - Architektura zorientowana na usługi (SOA)
 - HTTP i XML - o co w tym wszystkim chodzi?
 - Protokół do przesyłania wiadomości / protokół komunikacyjny wykorzystujący XML (SOAP)
 - Język służący do definiowania i opisu korzystania z usług sieciowych (WSDL)
 - Gromadzenie i udostępnianie informacji o dostępnych usługach (UDDI)
 - Profile WS-* - czym są ?
 - System komunikacji //--pomiędzy aplikacjami--// (REST)
- Technologia XML
 - Dlaczego XML w usługach sieciowych (WebServices)
 - Schemat XDS
 - Reprezentacja dokumentów XML
 - Przekształcanie dokumentów XML na dowolny inny format zgodny z XML (XSLT)
 - Analiza na podstawie przykładów HTTP / XML Web Services,
- SOAP
 - Model wiadomości
 - Przestrzeń nazw
 - SOAP ponad http
 - Znacznik envelope – komunikat, transakcja
 - Nagłówek wiadomości
 - Ciało/struktura wiadomości
 - Mechanizm błędu SOAP
 - Typy/Nagłówki/Załączniki
- WSDL
 - Usługi sieciowe jako oprogramowanie oparte na komponentach
 - Zastosowanie IDL- historia dystrybucji przetwarzania danych
 - WSDL
 - WSDL model informacji
 - Model abstrakcyjny -- Semantyka usług
 - Komunikaty
 - Style komunikatów
 - “Concrete Model” – Porty, usługi, lokalizacje
 - Rozszerzenie WSDL -- Wiązania
 - Opis usługi
- DANE BINARNE (XML, JSON)

- Nagłówki WS-I
- Wykorzystanie base64Binary
- Typ MIME

Ad.2 Combined JAVA, .NET and Web Application Security

- Zapoznanie się z podstawowymi pojęciami z zakresu bezpieczeństwa, bezpieczeństwa IT i bezpiecznego kodowania
- Luki w sieci poza dziesiątką OWASP - jak ich unikać
- Będą mieć praktyczne zrozumienie kryptografii
- Korzystanie z różnych funkcji zabezpieczeń środowiska programistycznego Java
- Korzystanie z różnych funkcji zabezpieczeń środowiska programistycznego .NET
- Luki w .NET i ASP.NET
- Typowe błędy w kodowaniu i jak ich unikać
- Luki w strukturze Java
- Bezpieczne metody kodowania

Ad. 3 Docker dla software developerów i administratorów IT

Co to jest Docker?

- Przypadki użycia
- Główne komponenty Dockera
- Podstawy architektury Dockera

Architektura Dockera

- Obrazy
- Rejestr
- Kontenery

Podstawy technologii

- Przestrzeń nazw
- Grupy
- Unia FS
- Format kontenera

Instalacja Dockera

- Instalacja na Ubuntu przez apt-get
- Instalacja najnowszej wersji Dockera

Konteneryzacja aplikacji

- Przykład „hello world”
- Interaktywny kontener
- Demonizacja programów

Wykorzystanie kontenerów

- Uruchamianie aplikacji webowej w kontenerze
- Analiza kontenera
- Mapowanie portów
- Wyświetlanie logów
- Obserwacja procesów
- Zatrzymywanie i uruchamianie
- Usuwanie kontenerów

Zarządzanie obrazami

- Listowanie obrazów
- Pobieranie obrazów
- Wyszukiwanie obrazów

Networking kontenerów

- Szczegółowe mapowanie portów
- Łączenie i nazywanie kontenerów
- Zmienne środowiskowe

Dane w kontenerach

- Wolumeny danych
- Katalogi hosta jako wolumin danych
- Pliki hosta jako wolumin danych
- Kontenery woluminów danych
- Kopie zapasowe i przywracanie woluminów danych

Ekosystem

- Co to jest Docker Hub?
- Rejestracja w Docker Hub
- Logowanie przez linie poleceń
- Uploadowanie do Docker Huba
- Prywatne repozytoria
- Automatyczne buildowanie

Ad. 4 Tworzenie aplikacji internetowych w języku Java z wykorzystaniem Framework Vaadin 8 - od podstaw

1. Wprowadzenie do Framework Vaadin 8
 - Zagadnienia podstawowe, architektura, najważniejsze biblioteki
2. Utworzenie projektu maven z użyciem Eclipse i IntelliJ
3. Tworzenie aplikacji po stronie serwera
4. Cykl życia sesji
 - Tworzenie, zamykanie i wygasanie sesji
 - Obsługa zdarzeń inicjalizacji i zamykania
5. Cykl życia aplikacji i komponentów
 - Deployment i undeployment

- Serializacja
 - Servlet i service
 - Kontrolki
 - Widoki
 - Panele
 - UIProvider
6. Nawigacja pomiędzy widokami i zagadnienia pokrewne
 - Zależności pomiędzy komponentami: (UIProvider, Page, Session, Service)
 - Przekazywanie danych pomiędzy widokami
 - Tworzenie widoków
 - Obsługa zdarzeń w widokach
 - Nawigator
 7. Podstawowe komponenty (Label, Link, TextField, TextArea, PasswordField, RichTextArea, DateField, Button, CheckBox, ComboBox, ListSelect, Table, Grid, MenuBar, Upload, ProgressBar, Slider, Calendar)
 8. Zarządzanie rozmieszczeniem komponentów (UI, Window, VerticalLayout, HorizontalLayout, GridLayout, FormLayout, Panel, HorizontalSplitPanel, VerticalSplitPanel, TabSheet, CssLayout)
 9. Wstrzykiwanie css
 - Kompatybilność względem typu przeglądarki
 10. Obsługa zdarzeń i słuchaczy
 - Korzystanie z anonimowych klas
 - Implementacja słuchaczy w klasach
 - Rozpoznawanie źródeł zdarzeń
 11. Dostęp do zasobów statycznych
 - Zasoby dostarczane ze źródeł statycznych
 - Zasoby dostarczane poprzez class loader
 - Zasoby dotyczące "look and feel"
 12. Obsługa błędów
 - Dostosowywanie komunikatów systemowych
 - Obsługa wyjątków nieprzechwyconych
 13. Powiadomienia
 - Rodzaje powiadomień
 - Dostosowywanie powiadomień
 - Stylizacja CSS
 14. Elementy interfejsu użytkownika
 - Cechy wspólne (Element : "caption", "enabled", "icon", "locale", "read-only", "style name", "visible")
 - Komponenty typu "Field" ("Data binding" i konwersje, Obsługa zmiany wartości pola, Buforowanie pola, Walidacja pola, Tworzenie formularzy poprzez "binding": - Prosty "binding" , -Wykorzystanie "FieldFactory", -Wiązanie pól z Beanami, -Walidacja Beanów)
 15. Przechowywanie danych w kontenerze
 - Podstawowe wykorzystanie kontenerów
 - IndexedContainer
 - BeanContainer
 - BeanItemContainer
 - HashMap

- Praca z danymi kontenera (Pobieranie danych, Dodawanie danych, Usuwanie danych, Modyfikacja danych)
16. Wykorzystanie Vaadin Add-Ons w projekcie maven
 17. Połączenia do baz danych z wykorzystaniem pakietu JAVA.SQL
 - DriverManager
 - Connection
 - Statement
 - PreparedStatement
 - ResultSet
 18. Vaadin designer, jako narzędzie wspomagania pracy
 - Instalacja pluginu
 - Komponenty i ich obsługa
 - Dodawanie komponentów
 - Ustawianie właściwości
 - Rozmieszczanie komponentów

Ad. 5 Tworzenie usług sieciowych (Web Services) w języku Java

1. Wprowadzenie do Web Service
 - Protokół http
 - SOAP
 - WSDL
2. Biblioteka JAX-WS
 - Podstawy, historia WS w Javie
 - tworzenie Webservice'u z użyciem JAX-WS
 - adnotacje
 - budowa klienta
 - narzędzie wsimport
3. Konfiguracja i użytkowanie JAX-WS
 - Typy dokumentów SOAP,
 - EndpointProvider,
 - wywołania asynchroniczne po stronie klienta i konfiguracja na serwerze
 - integracja z EJB
4. Biblioteka JAXB
 - Konfiguracja JAXB, marshalling i unmarshalling, przegląd adnotacji
5. RESTful services
 - Filozofia REST
 - biblioteka JAX-RS
 - tworzenie serwisu
 - adresacja usług
 - połączenie z EJB
6. Bezpieczeństwo usług
 - Konfiguracja bezpieczeństwa
 - sprawdzanie uprawnień na serwerze
 - tworzenie własnych polis

ZADANIE NR 12 – opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup voucherów szkoleniowych z zakresu usług narzędziowych

Lp.	Tytuł szkolenia	Czas trwania	Liczba uczestników
1	Testy wydajnościowe aplikacji internetowych z wykorzystaniem Apache JMeter	3 dni	2
2	Kontrola wersji z Git	2 dni	2
3	Monitoring systemów - Zabbix	4 dni	2
4	Testy wydajnościowe JMeter w praktyce	2 dni	3
5	Szkolenie SoapUI	2 dni	3
6	Business Process Management (BPM)	5 dni	1
7	Zarządzanie infrastrukturą IT przy pomocy narzędzi OpenSource	3 dni	2
8	Odzyskiwanie danych, techniki laboratoryjne	2 dni	6
9	Wdrażanie klienckich systemów operacyjnych z wykorzystaniem Windows deployment Service	3 dni	5

Szczegółowy opis szkoleń:

Ad. 1 Testy wydajnościowe aplikacji internetowych z wykorzystaniem Apache JMeter

- Aplikacje Web
 - Komunikacja HTTP
 - Podstawowa architektura aplikacji internetowych
- Wprowadzenie do JMeter
 - Zasada działania JMeter
 - Elementy aplikacji: Workbench, plan testów, interfejs
 - Zagadnienia: plan testów, grupa wątków, elementy planu testów
 - Dokumentacja narzędzia, jak efektywnie korzystać z Component reference, function reference
 - Ograniczenia narzędzia JMeter
- Praca z narzędziem JMeter
 - Nagrywanie ruchu użytkownika

- HTTP Proxy
- Budowanie scenariusza na podstawie nagrania
- Konfiguracja planu testów
 - HTTP Request Defaults
- Parametryzacja testu
 - Pliki CSV
 - Generowanie losowych danych
 - Pobieranie danych za pomocą JDBC
- Weryfikacja poprawności wykonania
 - Asercje
- Korelacja
 - Pobieranie tokenów z żądań HTTP (Regular expression extractor)
 - Użycie JMeter do symulacji wykonania skryptów (Beanshell pre/post procesor)
- Sterowanie wykonaniem skryptu
 - Kontrolery
- Zarządzanie obciążeniem
 - Konfiguracja sesji użytkownika
 - Opóźnienia i kontrolery obciążenia
 - Uruchamianie testów przy pomocy schedulera
 - Sterowanie obciążeniem przy pomocy JMeter Plugins
- Raportowanie i analiza parametrów wydajnościowych
 - Grafy i tabele
 - Drzewo wyników
 - Pliki JTL
 - Konwersja wyników
- Analiza raportów
 - Analiza plików JTL
 - Co mówią nam parametry wydajnościowe
 - Analiza wyników za pomocą arkusza kalkulacyjnego
 - Szacowanie ruchu i wymagań dla infrastruktury
- Monitorowanie testowanych systemów
 - Identyfikacja wąskich gardeł
 - Integracja narzędzi monitorujących z JMeter
- Testowanie rozproszone
 - Generowanie obciążenia za pomocą generatorów
 - Konfiguracja środowiska do testów rozproszonych
- Automatyzacja testów
 - Uruchamianie testów z poziomu linii komend
 - Integracja z Ant

Integracja JMeter z systemem ciągłej integracji na przykładzie.

Ad.2 Kontrola wersji z GIT

- Wprowadzenie
 - jak działają systemy kontroli wersji
 - charakterystyka pracy z rozproszonym systemem kontroli wersji

- instalacja i podstawowa konfiguracja Gita
- narzędzia dostarczane z Gitem
- Lokalna praca z Gitem
 - inicjalizacja i konfiguracja repozytorium
 - katalog .git
 - zatwierdzanie zmian (commit), narzędzie git gui
 - przechowywanie zmian (stash)
 - ignorowanie i modyfikacja zmian
 - przeglądanie zmian (diff), narzędzia do przeglądania zmian
 - przegląd historii (log), narzędzie gitk
 - tworzenie etykiet, rodzaje etykiet (tag)
 - cofanie zmian (reset, reflog)
 - praca z gałęziami (branch)
 - scalanie zmian i zmiana bazy (merge, rebase, cherry pick)
 - rozwiązywanie konfliktów
- Zdalne repozytoria
 - metody dostępu do repozytoriów, używane protokoły (ssh, http)
 - pobieranie repozytorium (clone)
 - wypychanie i pobieranie zmian (push, fetch, pull)
 - powiadamianie o zmianach (pull request)
 - praca ze zdalnymi gałęziami
 - praca z podprojektami (submodule, subtree)
- Praca grupowa z Git
 - metody współdzielenia zmian
 - praca w środowisku użytkowników o różnych rolach (programista, tester, wdrożeniowiec)
 - zasady zarządzania wydaniem i historią projektu
 - rozszerzenie gitflow
- Inne możliwości Gita
 - zaawansowane opcje konfiguracji
 - architektura Gita, obiekty i system ich nazywania
 - automatyzacja zadań Gita, skrypty dla zdarzeń (hooks)
 - konserwacja i optymalizacja repozytorium (fsck, gc)
 - wyszukiwanie błędów za pomocą Gita (bisect)
 - wyszukiwanie winnych (blame)
 - przepisywanie historii (filter-branch)
 - przechowywanie dużych plików
- Git i dodatkowe narzędzia
 - graficzne nakładki na Git na przykładzie Git Extensions
 - przegląd kodu, działanie Gita z Gerritem
 - praca z GitHub i GitLab
 - Powered by TCPDF (www.tcpdf.org)

Ad. 3 – Monitoring systemów – Zabbix

- Konfiguracja środowiska (konfiguracja Zabbix Server, Zabbix Agent, Zabbix Proxy) .
- Przygotowanie systemu (wstępna konfiguracja, omówienie funkcjonalności).
- Monitorowanie agentowe i bezagentowe (wydajność, systemem operacyjny, hardware).

- Webscenariusze
- Skrypty własne w monitorowaniu
- Szablony urządzeń.
- Wizualizacja danych (wykresy, mapy sieciowe).
- Monitorowanie systemów Windows.
- Monitorowanie rozproszone (oddziały i filie).
- Podstawy klastra HA - Zabbix
- Podstawy API na przykładzie języka PHP
- Sesja Q&A - rozwiązanie zgłoszonych przypadków od uczestników.

Ad. 4 Testy wydajnościowe Jmeter w praktyce

- Wprowadzenie do testów obciążeniowych i aplikacji JMeter
 - Podstawowe metryki wykorzystywane przy ocenie wydajności
 - Budowa planu testu w aplikacji JMeter
 - Benchmark architektury
 - komunikacja wyników
- Modelowanie i generowanie obciążenia
 - Identyfikacja scenariuszy testowych
 - Modelowanie zachowań użytkowników
 - Implementacja skryptów
 - Dane w testach wydajnościowych
 - Symulacja różnych scenariuszy w aplikacji JMeter
- Przeprowadzanie testów
 - Środowisko testowe
 - Jakość wyników
 - Optymalizacja działania aplikacji JMeter
 - Integracja ze środowiskiem CI
- Monitorowanie pracy testowanego systemu
 - Monitorowanie pracy aplikacji w systemie Linux oraz Windows
 - Monitorowanie i optymalizacja platformy Java
 - Monitorowanie pracy baz danych (na przykładzie PostgreSQL)
 - Poszukiwanie i rozwiązywanie typowych problemów
- Analiza wyników
 - Statystyka w testach obciążeniowych
 - Przetwarzanie wyników testów z aplikacji JMeter
 - Raportowanie wyników
- Wydajność z perspektywy użytkownika końcowego
 - Podstawowe metryki
 - Czynniki wpływające na postrzeganie wydajności przez użytkowników końcowych
 - Optymalizacja budowy serwisu
- Proces testowania wydajności
 - Ustalanie celów
 - Określanie wymagań wydajnościowych
 - Typy testów obciążeniowych
 - Plan i strategia testu
 - Podejście oparte o ryzyko
 - Role i zadania

- Nagrywanie testów z wykorzystaniem aplikacji JMeter
 - Konfiguracja proxy
 - Filtrowanie zapytań
 - Konfiguracja zapytań
 - Autentykacja
- Parametryzacja testów
 - Zmienne w aplikacji JMeter
 - Pobieranie danych z innych zapytań i plików zewnętrznych
 - Funkcje w aplikacji JMeter
- Kontrola przebiegu testu
 - Pętle
 - Losowe wykonywanie kroków
 - Opóźnienia
- BeanShell
 - Wprowadzenie do języka BeanShell
 - Funkcja __BeanShell
 - BeanShell Sampler i BeanShell Pre-processor
 - BeanShell w testach nietypowych rozwiązań
- Testowanie w środowisku rozproszonym
- Modularyzacja testów
- JMeter plugins

Ad. 5 Szkolenie SoapUI

- Wprowadzenie
 - Praca z aplikacją soapUI
 - Testy manualne w soapUI
- Podstawy automatyzacji testów
 - Elementy dobrego testu
 - Automatyzacja testów w projekcie
- Testowanie usług SOAP
 - Protokół SOAP i odkrywanie funkcji na podstawie WSDL
 - XPath i asercje w testach usług SOAP
 - Zmienne w soapUI
- Testowanie aplikacji Web
 - Możliwości testowania aplikacji Web
 - Web Recording
- Testowanie usług REST
 - Omówienie konwencji REST
 - Projekt usługi REST w soapUI
 - Asercje w testach REST
- Symulacja aplikacji
 - Symulacja usług REST
 - Symulacja usług SOAP
 - Dynamiczne generowanie danych
- Język Groovy
 - Podstawy języka Groovy

- SoapUI Object Model
- Generowanie danych z wykorzystaniem Groovy
- JMS z Groovy
- Wykorzystanie źródeł danych
 - Wykorzystanie baz danych
 - Wykorzystanie plików CSV
 - Wykorzystanie plików Excel
- Testy wydajnościowe
 - Testowanie wydajności w SoapUI
 - Wykorzystanie Groovy w testach wydajnościowych
- Testy bezpieczeństwa
 - Omówienie podstawowych typów ataków
 - Weryfikacja podatności na ataki w soapUI
- Dodatkowe aspekty automatyzacji testów
 - Uruchamianie testów poprzez serwer CI
 - Zarządzanie środowiskami
 - Utrzymanie testów (WSDL update)

Ad. 6 Business Process Management (BPM)

Wprowadzenie

- Krótka historia procesów
- Perspektywa procesów
- Zarządzanie procesami
- Analiza i projektowanie procesów
- Szkielet aplikacyjny BPM (ang. *BPM Framework*)
- Systemy Zarządzania Procesami Biznesowymi – BPMS (ang. *BPM Systems*)
- Architektura procesów biznesowymi

Strategie implementacyjne BPM

- Wartość dodana BPM
- Społeczność BPM
- Dlaczego warto automatyzować zarządzanie procesami biznesowymi?
- Topologia architektury opartej na usługach (ang. *Service-Oriented Architecture - SOA*)
- Przegląd dostawców narzędzi BPM

Łączenie Technologii Informacyjnych i biznesu

- BPM kontra BPMS
- Kiedy wybrać BPMS?
- Współpraca IT z biznesem w celu dopasowania właściwej technologii do Twojego problemu
- Adaptacja modelu rozwojowego
- Przegląd systemu BPM
- Uwarunkowania i słownik pojęć

Zrozumienie podstawowych pojęć i architektury

- Modelowanie Procesów
- Analiza Procesów
- Projektowanie Procesów
- Komponenty i struktura Systemu Zarządzania Procesami Biznesowymi
- Planowanie zasobów w zarządzaniu procesami
- Kluczowe umiejętności, role i odpowiedzialności

Strategie zarządzania i strategie biznesowe

- Przeszłość: dane i funkcje kontra obiekty i usługi
- Przyszłość: podstawowa logika biznesowa kontra kontrola procesów
- Implikacje przy projektowaniu okiem architektów
- Połączenie biznesu i Technologii Informacyjnych
- Rola Zarządcy Biznesowego
- Rola Analityka Reguł Biznesowych

Modelowanie procesów z wykorzystaniem BPMN

- Wartość dodana BPMN
- Kompozycyjność i podstawowe usługi
- Promowanie podejścia przyrostowego i iteracyjnego
- Dlaczego Przypadki Użycia (ang. *Use Cases*) napędzają projekt?
- Deklaracja własności komunikatów
- Wykorzystanie zbiorów zależności (ang. *correlation sets*)
- Rozwijanie kompleksowego, równoległego wykonywania czynności
- Projektowanie współbieżności
- Propozycję dostawców na implementację BPMB
- Przykład: Microsoft XLANG

Zarządzanie obsługą usterek i wyjątków

- Definiowanie zdarzeń
- Konfiguracja czasem w obsłudze błędów (ang. *Timeouts*)
- Obsługa usterek
- Wyłapywanie wyjątków
- Zarządzanie odszkodowaniami

Reguły Biznesowe

- Motywacje dla tworzenia reguł biznesowych
- Podstawowe pojęcia
- Model Dojrzałości zasad (ang. *Rule Maturity Model - KPI RMM™*)
- Zasady KPI STEP™
- Nowe role biznesu i IT
- Ukierunkowanie na biznes w regułach biznesowych
- Kiedy podejście do reguł biznesowych jest odpowiednie?
- Nowe aspekty w ustalaniu zakresów reguł biznesowych
- Kluczowe elementy planu projektu reguł biznesowych
- Rola „Pilota” reguł biznesowych (ang. *Business Role Pilot*)
- Przegląd wyodrębniania reguł biznesowych na podstawie kodu

BPM jako narzędzie umożliwiające wykorzystanie architektury opartej na usługach – kluczowe składniki

- Interfejsy graficzne aplikacji
- Podstawowe usługi
- Wartość architektury integracji aplikacji (ang. *Enterprise Service Bus* - **ESB**)
- Wykorzystanie repozytorium
- Wykorzystanie „zwinności” podejścia w biznesie
- Plansza BPM (ang. *BPM Board*)
- Dystrybucja białej księgi technologii

Kontrola i pomiar doskonalenia procesów

- Zarządzanie repozytorium
- Konfiguracja bramy jakościowej (ang. *Quality Gateway*)
- 4 filary sukcesu

Metryki

- Kontekst działalności organizacyjnej
- Co czyni metrykę dobrą?
- Pomiar i hierarchia zarządzania
- Zarządzanie procesami – więcej, niż pomiary
- Metryki wewnątrz procesów zarządzania rolami w pomiarze
- Pytania dotyczące pomiarów, na które powinniśmy znać odpowiedź
- Pułapka wysiłku poświęconego zarządzaniu procesami

Architektura systemu Zarządzania Procesami Biznesowymi

- Aspekty biznesowe i integracyjne (B2B, EAI)
- Topologia i skalowalność
- Narzędzia projektowe
- Narzędzia wdrożeniowe
- Monitorowanie i zarządzanie
- Silnik procesu
- Repozytorium definicji procesów

Kluczowa funkcjonalność BPMS

- Wsparcie dla repozytorium
- Wsparcie dla bazy danych
- Monitorowanie Aktywności Biznesowej (ang. *Business activity monitoring* – **BAM**)
- Rozwiązania w zakresie przepływu pracy pomiędzy ludźmi

Ad. 7 Zarządzanie infrastrukturą IT przy pomocy narzędzi OpenSource

- Monitorowanie Infrastruktury Serwerowej:
 - Potrzeba monitorowania systemów operacyjnych i kluczowych usług
 - Monitorowanie sprzętu
 - Protokół SNMP

- Nagios
 - Wymagania systemowe
 - Instalacja i konfiguracja wstępna środowiska Nagios
 - Konfiguracja hostów, usług pod kątem monitorowania
 - Uruchamianie i konfiguracja protokołów używanych przez Nagio
 - Mechanizmy powiadamiania o zdarzeniach i ich konfiguracja np. mail lub sms5. Własne rozwiązania zastosowania Nagios, tworzenie własnych wtyczek, alertów etc.
- Munin
 - Wymogi systemowe
 - Instalacja i konfiguracja wstępna środowiska Munin
 - Monitorowanie sieci przez protokół SNMP
 - Poszukiwanie problemów wydajnościowych w sieci
 - Monitorowanie niestandardowe np. sieci SAN
- Zabbix
 - Wymogi systemowe
 - Instalacja i konfiguracja wstępna środowiska Zabbix
 - Protokoły używane przez Zabbix'a
 - Monitorowanie sieci
 - Monitorowanie sprzętu
 - Poszukiwanie problemów wydajnościowych w sieci
 - Monitorowanie usług i systemów
 - Rozwiązania Własne

Ad.8 Odzyskiwanie danych, techniki laboratoryjne

- Budowa i zasada działania cyfrowych nośników HDD, SSD, pamięć
- Logiczne i fizyczne uszkodzenia HDD
- Systemy plików: partycje i woluminy
- Systemy plików: FAT32 i NTFS
- Obsługa PC3000 + Data Extractor
- Diagnostowanie dysków HDD
- Odzyskiwanie danych – uszkodzone sektory
- Odzyskiwanie danych – uszkodzony obszar serwisowy

Ad. 9 Wdrażanie klienckich systemów operacyjnych z wykorzystaniem Windows Deployment Services

- Projektowanie, konfiguracja i zarządzanie środowiskiem klienckim:
 - omówienie planowania środowiska klienckiego
 - zdefiniowanie wymagań konfiguracyjnych i przygotowanie standardowych ustawień systemowych
- Przegląd i konfiguracja roli Windows Deployment Services:
 - konfiguracja PXE i ustawień bootowania:
 - konfiguracja ustawień instalacyjnych
 - zarządzanie pakietami sterowników w WDS
 - instalacja z wykorzystaniem multiemisji;
- Projektowanie obrazów Windows:

- przegląd architektury instalacji Windows, rodzaje obrazów
- przegląd procesu tworzenia obrazu Windows
- wybór strategii tworzenia obrazu;
- 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 preinstalacyjnym
 - 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
- Wdrażanie Windows z wykorzystaniem Zero Touch Installation:
 - projektowanie środowiska Zero Touch Installation
 - wykonanie Zero Touch Installation z wykorzystaniem Microsoft Deployment Toolkit 2013;
- Zarządzanie aktualizacjami systemu Windows:
 - Implementowanie poprawek Windows Update do obrazów Instalacyjnych
 - Implementowanie poprawek Windows Update używając Windows Update Standalone Installer;
- Scentralizowane zarządzanie stacjami roboczymi w celu ujednoczenia 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;
- Elementy wirtualizacji stanu użytkownika
 - profile mobilne
 - Folder Redirection
 - User Experience Virtualization (UE-V)
 - pliki trybu offline
- 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