Szkolenie

Zabezpieczanie systemu Windows Server 2016

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie przeznaczone jest dla specjalistów IT chcących zdobyć wiedzę odnośnie podniesienia bezpieczeństwa infrastruktury, którą zarządzają.

Szkolenie realizowane na podstawie kursu MS 20744.

Szkolenie prezentuje metody i aspekty bezpieczeństwa w oparciu o platformę środowiska Windows Server 2016. Szkolenie nawiązuje do najnowszych mechanizmów platformy Advanced Threat Analysis czy nowych opcji wdrożeń w oparciu o instancję Nano Server. Tematyka szkolenia prezentuje praktyczne przykłady wykorzystania usług dostępu do zasobów za pomocą mechanizmów szyfrowania danych jak i Dynamic Access Control (DAC).

Wymagania:

- Ukończone szkolenia 740, 741, 742 lub wiedza z tego zakresu
- Praktyczna znajomość podstaw sieciowych, w tym TCP/IP, User Datagram Protocol (UDP), Domain Name System (DNS)
- Praktyczna wiedza na temat zarządzania infrastrukturą Active Directory Domain Services (AD DS)
- Praktyczna wiedza z podstaw wirtualizacji na platformie Microsoft Hyper-V
- Znajomość zasad bezpieczeństwa Windows Server

Po ukończeniu szkolenia uczestnicy potrafią:

- Zabezpieczyć system Windows Server
- Zarządzać bezpieczeństwem danych
- Skonfigurować zaporę systemu Windows

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

- Skonfigurować zaawansowaną inspekcję
- Zarządzać aktualizacjami oprogramowania
- Zarządzać zagrożeniami za pomocą zaawansowanej analizy zagrożeń (ATA) oraz Microsoft Operations Management Suite (OMS)

Szkolenie prowadzone jest w języku polskim.

Program szkolenia

Moduł 1 Wykrywanie zagrożeń przy użyciu narzędzi Sysinternals

- Przegląd zagadnień związanych z wykrywaniem zagrożeń
- Narzędzia pakietu Sysinternals wykorzystywane do wykrywania zagrożeń

Moduł 2 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)

Moduł 3 Ograniczanie uprawnień administratora przy użyciu Just Enough Administration (JEA)

- Idea rozwiązania JEA
- Konfiguracja i wdrożenie (JEA)

Moduł 4 Uprzywilejowany dostęp przez Access Management

- Prezentacja schematu ESAE
- Przegląd funkcji MIM
- Implementacja funkcji JIT oraz praktyczne aspekty MIM

Moduł 5 Wykrywanie niepożądanego oprogramowania i zagrożeń

- Konfiguracja Windows Defender
- Wdrożenie AppLocker
- Konfigurowanie i korzystanie z Device Guard

- Wdrożenie i korzystanie z Enhanced Mitigation Experience Toolkit (EMET)

Moduł 6 Analiza aktywności przy użyciu zaawansowanych metod audytowania i logów serwisowych

- Przegląd metod audytowania
- Rozumienie zaawansowanych metod audytowania
- Konfiguracja przeprowadzania metod audytu przy użyciu Windows PowerShell

Moduł 7 Analiza aktywności z wykorzystaniem Microsoft Advanced Threat Analytics (ATA) i Operations Management Suite (OMS)

- Przegląd funkcjonalności ATA
- Idea rozwiązania OMS

Moduł 8 Zabezpieczanie infrastruktury wirtualizacji

- Prezentacja funkcji Guarded Fabric VMs
- Zrozumienie chronionych i zaszyfrowanych maszyn wirtualnych w oparciu o platformę Windows Server 2016

Moduł 9 Zabezpieczanie wdrażania oprogramowania i infrastruktury serwerowej

- Prezentacja narzędzia Security Compliance Manager
- Wprowadzenie do Nano Server
- Prezentacja funkcji "kontenerów" wirtualizacji

Moduł 10 Szyfrowanie danych

- Planowanie i wdrożenie Encrypting File System (EFS)
- Planowanie i wdrożenie BitLocker

Moduł 11 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)

Moduł 12 Konfiguracja usługi Firewall i kontrola usług ruchu sieciowego

- Windows Firewall
- Rozwiązania programowe Firewall

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Moduł 13 Zabezpieczanie ruchu sieciowego

- Metody zagrożeń ruchu sieciowego i role schematów bezpieczeństwa
- Konfiguracja zaawansowanych funkcji w usłudze DNS
- Analiza ruchu sieciowego przy użyciu Microsoft Message Analyzer
- Zabezpieczanie i analiza połączeń związanych z protokołem SMB

Moduł 14 Aktualizowanie Windows Server

- Prezentacja usługi WSUS
- Wdrażanie polityki aktualizacji przez usługę WSUS

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.