Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

Securing Windows Server 2016

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

Overview

Bu eğitim, BT profesyonellerine yönetmekte oldukları BT altyapısının güvenliğini nasıl arttırabileceklerini öğretmektedir. Bu eğitim, ağ ihlallerinin zaten gerçekleşmiş olduğu varsayımının önemini vurgulayarak başlar ve ardından yöneticilerin sadece ihtiyaç duyulan görevleri ihtiyaç duyulan zamanlarda gerçekleştirebilmelerini sağlamak amacıyla yönetici bilgilerinin ve haklarının nasıl korunacağını öğretir.

Bu eğitim ayrıca kötü yazılım tehlikelerini nasıl azaltabileceğinizi, Windows Server 2016'deki denetim ve Gelişmiş Tehlike Analizi özelliğini kullanarak güvenlik sorunlarını nasıl belirleyebileceğinizi, sanallaştırma platformunuzu nasıl güvenlik altına alabileceğinizi ve güvenliği arttırmak amacıyla da Nano sunucu ve konteyneri gibi yeni kurulum seçeneklerini nasıl kullanabileceğinizi ayrıntılarıyla açıklamaktadır. Eğitim ayrıca şifreleme ve dinamik erişim kontrolünü kullanarak dosyalara erişimin korunmasına nasıl yardımcı olabileceğinizi ve ağınızın güvenliğini nasıl arttırabileceğinizi de açıklar.

Prerequisites

Herhangi bir ön koşul yoktur.

Who Should Attend

Bu eğitim, Windows Server 2016 ağlarını güvenli bir şekilde yönetme ihtiyacı duyan BT profesyonelleri içindir. Bu profesyoneller genelde İnternet'e ve bulut hizmetlerine erişimi yönetilmekte olan Windows Server tabanlı ortamlar olarak yapılandırılmış ağlarla çalışmaktadırlar.

What You Will Learn

- Bu eğitimin tamamlanmasının ardından öğrenciler:
- Windows Server'ı güvence altına alabilecek.
- Uygulama geliştirme ve sunucu iş yükü altyapısını güvence altına alabilecek.
- Temel güvenlik unsurlarını yönetebilecek.
- Yeterince ve zamanında (JIT) yönetimi yapılandırabilecek ve yönetebilecek.
- Veri güvenliğini yönetebilecek.
- Windows Güvenlik Duvarı'nı ve yazılım tanımlı dağıtık güvenlik duvarını yapılandırabilecek.
- Ağ trafiğini güvence altına alabilecek.
- Sanallaştırma altyapınızı güvence altına alabilecek.
- Kötü yazılımları ve tehlikeleri yönetebilecek.
- Gelişmiş denetimi yapılandırabilecek.
- Yazılım güncellemelerini yönetebilecek.
- Advanced Threat Analytics (ATA) ve Microsoft Operations Management Suite'i (OMS) kullanarak tehlikeleri yönetebilecek.

Outline

- Module 1: Breach detection and using the Sysinternals tools
- Module 2: Protecting credentials and privileged access
- Module 3: Limiting administrator rights with Just Enough Administration
- Module 4: Privileged Access Management and administrative forests
- Module 5: Mitigating malware and threats
- Module 6: Analysing activity by using advanced auditing and log analytics
- Module 7: Analysing activity with Microsoft Advanced Threat Analytics feature and Operations Management Suite
- Module 8: Securing your virtualization an infrastructure
- Module 9: Securing application development and server-workload infrastructure
- Module 10: Protecting data with encryption
- Module 11: Limiting access to file and folders
- Module 12: Using firewalls to control network traffic flow

- Module 13: Securing network traffic
- Module 14: Updating Windows Server