Implement end-to-end security controls for cloud and AI workloads Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bulut ve Yapay Zekâ İş Yükleri için Uçtan Uca Güvenlik Kontrollerinin Uygulanması Eğitimi , Microsoft Azure, Microsoft 365 ve yapay zekâ destekli sistemlerde güvenlik kontrollerinin uygulanması ve yönetilmesine yönelik pratik beceriler kazandırır.

Bu eğitim sayesinde katılımcılar:

- **Bulut, hibrit ve çoklu bulut ortamlarında** kimlikleri, verileri, altyapıları ve uygulamaları korumaya yönelik güvenlik kontrollerini uygulamayı öğrenir.
- **Microsoft Entra ID, Azure Key Vault, Microsoft Defender for Cloud ve Microsoft Sentinel** gibi teknolojilerle güvenlik yönetimi becerilerini geliştirir.
- **Yapay zekâ uygulamaları ve AI agent'ların** kimlik, veri erişimi, ağ geçidi ve altyapı güvenliğini sağlamaya yönelik yöntemleri keşfeder.
- **Yetkisiz erişimi azaltma, güvenli yapılandırmaları uygulama ve güvenlik risklerini yönetme** konularında uygulamalı deneyim kazanır.
- **SC-500 sertifikasyon sınavına** yönelik teknik bilgi ve yetkinliklerini geliştirir.

Bu **4 günlük eğitim**, güvenlik profesyonellerinin **Microsoft Azure, Microsoft 365 ve yapay zekâ destekli iş yüklerinde** uçtan uca güvenlik kontrollerini uygulama ve yönetme becerilerini geliştirmek amacıyla hazırlanmıştır.

Eğitim boyunca katılımcılar; **kimlik ve erişim güvenliği, veri koruma, altyapı güvenliği, uygulama güvenliği ve yapay zekâ iş yüklerinin korunması** gibi temel alanlara odaklanır. Microsoft güvenlik teknolojilerinin yetkisiz erişimi önlemek, güvenlik açıklarını azaltmak, güvenli yapılandırmaları uygulamak ve kurumların genel güvenlik duruşunu güçlendirmek için nasıl kullanılabileceği ele alınır.

Eğitmen anlatımı, uygulamalı laboratuvar çalışmaları, bilgi kontrol soruları, gösterimler ve teknik tartışmalar aracılığıyla katılımcılar; Microsoft Entra ID, Azure Key Vault, Azure Policy, Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Purview ve Microsoft Security Copilot gibi çözümlerle çalışma deneyimi kazanır.

Yapay zekânın modern bulut çözümlerinde giderek daha fazla kullanılmasıyla birlikte eğitim,**AI agent'ların, kimliklerin, veri erişim yollarının, ağ geçitlerinin, güvenlik korumalarının (guardrails) ve destekleyici altyapıların** korunmasına da odaklanır.

Katılımcılar, bulut ve yapay zekâ ortamlarındaki farklı güvenlik kontrollerinin birlikte nasıl çalıştığını ve bu kontrollerin gerçek dünyadaki güvenlik mühendisliği görevlerine nasıl uygulanabileceğini öğrenir.

Sınav ve Değerlendirme

Bu eğitim, **SC-500 sertifikasyon sınavına** hazırlığı destekler.

Implement end-to-end security controls for cloud and AI workloads Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Sınavla ilişkili çalışma alanları; **kimlik, erişim ve yönetişim yönetimi; depolama, veritabanı ve ağ güvenliği; işlem kaynaklarının korunması; güvenlik duruşunun yönetilmesi ve izlenmesi** konularını kapsar.

Prerequisites

Eğitimden en yüksek verimi alabilmek için katılımcıların aşağıdaki konularda temel bilgi ve deneyime sahip olması önerilir:

- **Microsoft Azure temelleri:** Abonelikler, kaynak grupları, sanal ağlar, depolama hesapları, sanal makineler ve Azure rol tabanlı erişim kontrolü (RBAC).
- **Kimlik ve erişim yönetimi:** Microsoft Entra ID, kimlik doğrulama, yetkilendirme, çok faktörlü kimlik doğrulama (MFA), Conditional Access ve uygulama veya hizmet kimlikleri.
- **Temel güvenlik kavramları:** En az ayrıcalık ilkesi, derinlemesine savunma, Zero Trust, şifreleme, denetim, tehdit koruması ve güvenli yapılandırma.
- **Bulut ağ teknolojileri:** Sanal ağlar, alt ağlar, private endpoint'ler, güvenlik duvarları, VPN bağlantıları ve ağ güvenlik kuralları.
- **Azure iş yükleri:** Depolama, SQL veritabanları, sanal makineler, container'lar, App Services ve API'ler.
- **Microsoft güvenlik çözümleri:** Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender XDR, Microsoft Purview veya Microsoft Security Copilot.
- **Yapay zekâ temelleri:** Copilot'lar, AI agent'lar, prompt'lar, modeller ve veri temellendirme (data grounding).
- **Uygulama deneyimi:** Azure portalını kullanma ve laboratuvar ortamında temel yapılandırma değişiklikleri gerçekleştirme.

Implement end-to-end security controls for cloud and AI workloads Eğitimi

Süre: **4 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

Bu eğitim, **bulut, hibrit ve yapay zekâ destekli ortamlarda kurumsal sistemlerin ve verilerin güvenliğinden sorumlu güvenlik mühendisleri** için tasarlanmıştır.

Özellikle aşağıdaki alanlarda çalışan profesyoneller için uygundur:

- **Bulut güvenliği ve siber güvenlik mühendisleri**
- **Kimlik ve erişim yönetimi uzmanları**
- **Ağ, altyapı ve uygulama güvenliği uzmanları**
- **Güvenlik operasyonları ve tehdit yönetimi ekipleri**
- **DevOps ve bulut platformu uzmanları**
- **Yapay zekâ çözümlerinin güvenliğinden sorumlu profesyoneller**
- **Veri güvenliği ve yönetişim uzmanları**

Eğitim ayrıca mimarlar, sistem yöneticileri, geliştiriciler, güvenlik analistleri, veritabanı uzmanları ve ağ profesyonelleriyle birlikte çalışan; **kimlik, erişim, yönetişim, veri, ağ, işlem kaynakları, uygulama platformları, yapay zekâ iş yükleri ve bulut güvenlik duruşu yönetimi** alanlarında sorumluluk üstlenmeye hazırlanan katılımcılar için de uygundur.

Implement end-to-end security controls for cloud and AI workloads Eğitimi

Süre: **4 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Bu eğitimi tamamladığınızda:

- **Microsoft Entra ID** kullanarak kullanıcıların, uygulamaların ve AI agent'ların kimlik ve erişim güvenliğini sağlamayı; kimlik doğrulama kontrollerini ve ayrıcalıklı erişim yapılandırmalarını uygulamayı,
- **Azure Key Vault** ve ilgili güvenlik kontrolleriyle gizli bilgileri, kriptografik anahtarları, sertifikaları, depolama kaynaklarını, veritabanlarını ve diğer hassas varlıkları korumayı,
- **Azure Policy, RBAC ve güvenlik önerileri** aracılığıyla yönetişim, uyumluluk ve en az ayrıcalık ilkelerini uygulamayı,
- Ağ segmentasyonu, trafik denetimi, özel bağlantılar ve güvenlik duvarları kullanarak**Azure ağ ve kaynak erişim güvenliğini** güçlendirmeyi,
- **Yapay zekâ iş yüklerinin, agent'ların, kimliklerin, veri erişim yollarının, AI gateway'lerin ve guardrail mekanizmalarının** güvenliğini değerlendirmeyi ve korumayı,
- **Sanal makineler, hibrit sunucular, container'lar, uygulama platformları ve API'ler** için güvenlik kontrolleri uygulamayı,
- **Microsoft Defender for Cloud** ve ilgili güvenlik çözümleriyle Azure, hibrit ve çoklu bulut ortamlarında güvenlik duruşunu yönetmeyi ve izlemeyi,
- **Microsoft Sentinel** kullanarak güvenlik olaylarının toplanması, günlük yönetimi ve temel güvenlik operasyonlarını yapılandırmayı,
- **Microsoft Security Copilot** ile güvenlik operasyonlarını destekleyen çalışma alanlarını, eklentileri, agent'ları ve erişim kontrollerini yönetmeyi,
- Bulut ve yapay zekâ sistemlerinde**uçtan uca güvenlik kontrollerini** gerçek güvenlik mühendisliği senaryolarına uygulamayı öğreneceksiniz.

Outline

1. Microsoft Entra ID ile Erişim Güvenliğinin Sağlanması

Bulut ve yapay zekâ iş yüklerinin korunmasında**kimlik güvenliğinin** temel rolü ele alınır. Kimlik doğrulama yöntemleri, Conditional Access, ayrıcalıklı erişim, uygulama kayıtları ve uygulama kimliklerinin güvenliği incelenir.

İşlenecek Konular:

- Kimlik doğrulama yöntemlerinin uygulanması ve yönetilmesi
- **Privileged Identity Management (PIM)** yapılandırması

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Conditional Access ile **çok faktörlü kimlik doğrulamanın (MFA)** zorunlu hale getirilmesi
- Uygulama ve hizmet kimliklerinin güvenliğinin sağlanması
- Güvenli API'ler kullanan declarative agent'lar için API eklentilerinin kimlik doğrulaması

2. Azure Key Vault ile Gizli Bilgilerin ve Anahtarların Korunması

Bulut iş yüklerinde kullanılan hassas kimlik bilgilerinin ve kriptografik varlıkların korunması ele alınır. Güvenli erişim, gizli bilgi yönetimi, sertifikalar, yönetilen kimlikler ve iş yükü koruma yöntemleri incelenir.

İşlenecek Konular:

- **Azure Key Vault** yapılandırması ve güvenliğinin sağlanması
- Kriptografik anahtarların ve gizli bilgilerin (secrets) yönetilmesi
- Sertifika yönetimi ve Key Vault etkinliklerinin izlenmesi
- **Managed Identities** kullanılarak korunan kaynaklara erişim sağlanması
- Microsoft Defender for Cloud ile Azure Key Vault'un korunması

3. Yönetişim ve Güvenlik Kontrollerinin Uygulanması

Güvenli ve uyumlu bulut ortamlarının sürdürülebilmesi için **yönetişim ve en az ayrıcalık ilkelerinin** nasıl uygulanacağı incelenir.

İşlenecek Konular:

- **Azure Policy** ve kaynak kilitleri (Resource Locks) ile yönetişim kurallarının uygulanması
- **Role-Based Access Control (RBAC)** atamalarının yönetilmesi
- Erişim incelemeleri (Access Reviews) ile uygun erişim yetkilerinin desteklenmesi
- Güvenlik kontrollerinin yapılandırılması ve güvenlik önerilerinin uygulanması
- Mevzuat ve düzenleyici gereksinimlere uyumluluğun değerlendirilmesi
- Azure güvenlik özellikleriyle yedekleme verilerinin korunması
- **Infrastructure as Code (IaC)** aracılığıyla güvenlik kontrollerinin uygulanması

4. Depolama, Veritabanı ve Ağ Güvenliğinin Sağlanması

Bulut ortamlarındaki veri hizmetlerinin korunması ve kaynaklara yönelik ağ erişiminin kontrol edilmesi üzerinde durulur.

İşlenecek Konular:

- Azure Storage için erişim ve ağ güvenliğinin yönetilmesi

BİLGİNÇ
IT Academy

info@bilginc.com
bilginc.com

- Güvenlik duvarları, **Private Endpoints** ve **Shared Access Signatures (SAS)** yapılandırması
- Microsoft Defender for Storage kullanımı
- **Azure SQL Database** güvenliğinin sağlanması
- SQL denetimi (SQL Auditing) ve Microsoft Defender for SQL yapılandırması
- Veri maskeleme ve ledger özelliklerinin incelenmesi
- İş yüklerinin ağ segmentasyonu ve izolasyonu
- **Azure Firewall** ile ağ trafiği denetiminin merkezileştirilmesi
- Uzak ve hibrit bağlantıların güvenliğinin sağlanması
- Platform hizmetlerinin genel ağ erişimine açıklığının azaltılması

5. Sunucu, Sanal Makine ve Hibrit Altyapı Güvenliği

Azure sanal makinelerinin ve hibrit sunucuların korunmasına yönelik güvenlik kontrolleri incelenir.

İşlenecek Konular:

- Disk şifrelemenin uygulanması
- **Trusted Launch** güvenlik özelliklerinin yapılandırılması
- Güvenli erişim için **Azure Bastion** kullanılması
- Azure Arc özellikli hibrit sunucuların güvenliğinin yönetilmesi
- **Microsoft Defender for Servers** uygulanması
- **Just-in-Time (JIT)** sanal makine erişiminin zorunlu hale getirilmesi
- Sanal makineler için güvenlik yapılandırma kontrollerinin uygulanması
- Aracısız (agentless) güvenlik özelliklerinin incelenmesi

6. Yapay Zekâ İş Yükleri için Güvenlik Kontrollerinin Uygulanması

Yapay zekâ uygulamaları ve otonom agent'larla ilişkili yeni güvenlik riskleri değerlendirilir.**Kimlik güvenliği, veri koruma, platform güvenlik sınırları, ağ geçitleri ve iş yükü korumasının** AI risklerini azaltmak için nasıl birlikte kullanılabileceği incelenir.

İşlenecek Konular:

- **Microsoft Entra Agent Identity** güvenliğinin sağlanması
- Microsoft Defender XDR ile yapay zekâ kimlik risklerinin analiz edilmesi
- **Copilot Studio agent'larının** korunması

BİLGİNÇ
IT Academy

info@bilginc.com
bilginc.com

- Microsoft Foundry üzerinde **AI Gateway** güvenliğinin yapılandırılması
- Yapay zekâ güvenlik korumalarının (**AI Guardrails**) yapılandırılması ve yönetilmesi
- Microsoft Defender for Cloud ile AI iş yüklerinin korunması
- Yapay zekâ hizmetleri için iş yükü korumasının etkinleştirilmesi
- **Microsoft Agent 365** ile agent yönetimi
- Microsoft Purview **Data Security Posture Management** ile yapay zekâ veri risklerinin belirlenmesi

7. Container ve Uygulama Platformlarının Güvenliğinin Sağlanması

Modern uygulama platformları, container'lar, API'ler ve web hizmetleri için güvenlik kontrollerinin uygulanması ele alınır.

İşlenecek Konular:

- Microsoft Defender for Containers ile container risklerinin tespit edilmesi
- **Azure Kubernetes Service (AKS)** güvenliğinin sağlanması
- Azure Container Registry, Container Instances ve Container Apps hizmetlerinin korunması
- **Azure Functions** ve Logic Apps güvenliğinin sağlanması
- Azure App Services için güvenlik kontrollerinin uygulanması
- **Web Application Firewall (WAF)** özelliklerinin kullanılması
- Azure API Management ile API arka uç hizmetlerinin güvenliğinin sağlanması

8. Bulut Güvenlik Duruşunun Yönetilmesi

Bulut, hibrit ve çoklu bulut ortamlarında güvenlik risklerini belirleme, güvenlik duruşunu iyileştirme ve koruma süreçlerini yönetme becerileri geliştirilir.

İşlenecek Konular:

- Hibrit ve çoklu bulut ortamlarının **Microsoft Defender for Cloud** ile bağlantısının kurulması
- **Cloud Security Posture Management (CSPM)** ile risklerin belirlenmesi
- Korumasız varlıkların ve güvenlik açıklarının tespit edilmesi
- Harici saldırı yüzeyi yönetiminin (External Attack Surface Management) incelenmesi
- Düzenleyici uyumluluğun değerlendirilmesi
- İş yükü koruma planlarının etkinleştirilmesi ve yapılandırılması
- Azure sanal makineleri için güvenlik açığı ayarlarının yönetilmesi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- **Secure Score**, güvenlik önerileri, gizli bilgi taraması (Secret Scanning) ve yönetişim kontrollerinin kullanılması

9. Microsoft Sentinel ile Güvenlik Olaylarının Toplanması ve Yönetilmesi

Microsoft Sentinel kullanılarak temel güvenlik operasyonları, olay verilerinin toplanması, otomasyon ve günlük yönetimi süreçleri incelenir.

İşlenecek Konular:

- Microsoft Sentinel çalışma alanlarının oluşturulması ve yönetilmesi
- Güvenlik içeriklerinin yönetilmesi
- Microsoft ve harici veri kaynaklarının bağlanması
- **Syslog, Common Event Format (CEF)** ve Windows sistem verilerinin toplanması
- Otomasyon kuralları ve **Playbook** uygulamalarının oluşturulması
- Veri depolama süreçlerinin yönetilmesi
- Toplanan günlüklerin sorgulanması ve denetlenmesi

10. Microsoft Security Copilot'un Uygulanması

Microsoft Security Copilot çözümünün çalışma alanları, eklentiler, agent'lar ve erişim kontrolleri aracılığıyla güvenlik operasyonlarını nasıl desteklediği incelenir.

İşlenecek Konular:

- Microsoft Security Copilot özelliklerinin ve yeteneklerinin anlaşılması
- **Security Copilot çalışma alanlarının** yapılandırılması
- Eklentilerin ve agent'ların yönetilmesi
- **Security Compute Unit (SCU)** tüketim modelinin anlaşılması
- İlgili rollerin ve erişim yetkilerinin yönetilmesi