Google Cloud Platform'da Güvenlik

Google Cloud Platform'da Güvenlik eğitimi, katılımcılara Google Cloud Platform'daki güvenlik kontrollerine ve tekniklerine genel bir bakış sunar. Katılımcılar, Dağıtılmış Hizmet Reddi saldırıları, kimlik avı saldırıları ve içerik sınıflandırması ve kullanımını içeren tehditler dahil GCP tabanlı bir altyapının birçok noktasında saldırıları azaltma tekniklerini öğrenir.

Hedefler:

- Google'ın güvenliğe yaklaşımını anlamayı
- Cloud Identity kullanarak yönetici kimlikleri yönetmeyi
- Google Cloud Resource Manager, Cloud IAM kullanarak en az ayrıcalıklı yönetim erişimini uygulamayı
- VPC güvenlik duvarlarını ve Cloud Armor'u kullanarak IP trafiği kontrollerini uygulamayı
- Kimliğe Duyarlı Proxy Uygulamayı
- GCP denetim günlükleriyle kaynakların yapılandırmasında veya meta verilerinde yapılan değişiklikleri analiz etmeyi
- Data Loss Prevention API ile hassas verileri tarayın ve çıkartmayı
- Forseti ile bir GCP dağıtımını taramayı
- Özellikle verilere ve sanal makinelere genel erişimde önemli güvenlik açığı türlerini gidermeyi

Topics:

- Giriş
  GCP Güvenliğinin Temelleri
  - GCP paylaşılan güvenlik sorumluluğu modelini anlayın
  - Google Cloud'un güvenlik yaklaşımını anlayın

- Google ve GCP tarafından hafifletilen tehdit türlerini anlayın
- Erişim Şeffaflığını ve Erişim Onayını (beta) Tanımlayın ve Anlayın

- Cloud Identity
  - Google Cloud Directory Sync kullanarak Microsoft Active Directory ile senkronizasyon
  - Microsoft Active Directory için Yönetilen Hizmeti Kullanma (beta)
  - Google kimlik doğrulaması ve SAML tabanlı SSO arasında seçim yapma
  - DNS yapılandırması, süper yönetici hesapları dahil en iyi uygulamalar

- Kimlik, Erişim ve Anahtar Yönetimi
  - GCP Resource Manager: projeler, klasörler ve kuruluşlar
  - Özel roller dahil GCP IAM rolleri
  - Kuruluş politikaları dahil GCP IAM politikaları
  - GCP IAM Etiketleri
  - GCP IAM Öneri Aracı
  - GCP IAM Sorun Giderici
  - GCP IAM Denetleme Günlükleri
  - Görevlerin ayrılması ve en az ayrıcalık, politikalarda Google gruplarının kullanılması ve ilkel rollerin kullanımından kaçınılması dahil en iyi uygulamalar

- İzolasyon ve Güvenlik için Google Sanal Özel Bulutu Yapılandırma
  - VPC güvenlik duvarlarını yapılandırma (hem giriş hem de çıkış kuralları)
  - Yük dengeleme ve SSL politikaları
  - Gizli Google API erişimi
  - SSL proxy kullanımı

- Eşleme ve paylaşılan VPC kullanımı, alt ağların doğru kullanımı dahil VPC ağları için en iyi uygulamalar
- VPN'ler için en iyi güvenlik uygulamaları
- Ara bağlantı ve eşleme seçenekleri için güvenlik konuları
- Ortaklardan temin edilebilen güvenlik ürünleri
- Çevre köprüleri dahil bir hizmet çevresi tanımlama
- Google API'lerine ve hizmetlerine özel bağlantı kurma

- Compute Engine'in Güvenliğini Sağlama
  - Compute Engine hizmet hesapları, varsayılan ve müşteri tanımlı
  - Sanal makineler için IAM rolleri
  - Sanal makineler için API kapsamları
  - Linux sanal makineleri için SSH anahtarlarını yönetme
  - Windows VM'ler için RDP oturum açma bilgilerini yönetme
  - Kuruluş politikası kontrolleri: güvenilen görüntüler, genel IP adresi, seri bağlantı noktasını devre dışı bırakma
  - Müşteri tarafından yönetilen şifreleme anahtarları ve müşteri tarafından sağlanan şifreleme anahtarlarıyla sanal makine görüntülerini şifreleme
  - Sanal makinelere genel erişimi bulma ve düzeltme
  - Sağlamlaştırılmış özel görüntüler, özel hizmet hesapları (varsayılan hizmet hesabı değil), özelleştirilmiş API kapsamları ve kullanıcı tarafından yönetilen anahtarlar yerine uygulama varsayılan kimlik bilgilerinin kullanımı dahil en iyi uygulamalar
  - Müşteri tarafından sağlanan şifreleme anahtarlarıyla sanal makine disklerini şifreleme
  - Sanal makinelerin bütünlüğünü korumak için Korumalı VM'leri kullanma
  - Bulut Verilerinin Güvenliğini Sağlama

- Cloud Storage ve IAM izinleri
- Bulut Depolama ve ACL'ler
- Genel olarak erişilebilen verileri bulma ve düzeltme dahil olmak üzere bulut verilerini denetleme
- İmzalanmış Bulut Depolama URL'leri
- İmzalanmış politika belgeleri
- Müşteri tarafından yönetilen şifreleme anahtarları ve müşteri tarafından sağlanan şifreleme anahtarları ile Cloud Storage nesnelerini şifreleme
- Anahtar yönlendirmeden sonra nesnelerin arşivlenmiş sürümlerini silme dahil en iyi uygulamalar
- BigQuery yetkili görünümleri
- BigQuery IAM rolleri
- EKL'ler yerine IAM izinlerini tercih etme dahil en iyi uygulamalar

- Uygulamaları Güvenli Hale Getirme
  - Uygulama güvenlik açıklarının türleri
  - App Engine ve Cloud Functions'ta DoS korumaları
  - Bulut Güvenliği Tarayıcısı
  - Kimliğe Duyarlı Proxy
- Kubernetes'in güvenliğini sağlama
  - yetki
  - İş Yüklerinin Güvenliğini Sağlama
  - Kümelerin Güvenliğini Sağlama
  - Günlük Kaydı ve İzleme
- Dağıtılmış Hizmet Reddi Saldırılarına Karşı Koruma

- DDoS saldırıları nasıl çalışır?
- Hafifletmeler: GCLB, Cloud CDN, otomatik ölçeklendirme, VPC giriş ve çıkış güvenlik duvarları, Cloud Armor (kural dili dahil)
- Tamamlayıcı iş ortağı ürünleri türleri

- İçerikle İlgili Güvenlik Açıklarına Karşı Koruma
  - Tehdit: Fidye yazılımı
  - Hafifletmeler: Yedeklemeler, IAM, Veri Kaybını Önleme API'si
  - Tehditler: Verilerin kötüye kullanımı, gizlilik ihlalleri, hassas / kısıtlanmış / kabul edilemez içerik
  - Tehdit: Kimlik ve Oauth kimlik avı
  - Hafifletmeler: Cloud ML API'leri kullanarak içeriği sınıflandırma; Data Loss Prevention API kullanarak verileri tarama ve yeniden düzenleme

- İzleme, Günlük Kaydı, Denetim ve Tarama
  - Güvenlik Komuta Merkezi
  - Stackdriver izleme ve günlük kaydı
  - VPC akış günlükleri
  - Bulut denetimi günlük kaydı
  - Forseti'yi Dağıtma ve Kullanma