Security in Google Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Overview

Security in Google Cloud eğitimi, Google Cloud ortamlarında kullanılan güvenlik kontrolleri ve teknikleri hakkında kapsamlı bir temel oluşturmayı amaçlar.

Kayıtlı dersler, demonstrasyonlar ve uygulamalı laboratuvar çalışmaları boyunca katılımcılar güvenli bir Google Cloud çözümünün temel bileşenlerini inceleyerek bunların kullanımını deneyimler. Eğitim kapsamında Cloud Identity, Resource Manager, Identity and Access Management (IAM), Virtual Private Cloud (VPC) firewall'ları, Cloud Load Balancing, Direct Peering, Carrier Peering, Cloud Interconnect ve VPC Service Controls gibi temel güvenlik ve altyapı teknolojileri ele alınır.

Program; kimlik ve erişim yönetiminden ağ güvenliğine, Compute Engine ve bulut verilerinin korunmasından uygulama ve Google Kubernetes Engine güvenliğine kadar uzanan geniş bir kapsam sunar. Ayrıca DDoS saldırılarına karşı koruma, hassas verilerin yönetimi, monitoring, logging, auditing ve güvenlik taraması konuları uygulamalı çalışmalarla desteklenir.

Eğitimde Kullanılan Ürün ve Teknolojiler

Google teknolojileri:

Cloud Identity, Resource Manager, IAM, HSM, Secret Manager, Google Kubernetes Engine, Managed Service for Microsoft Active Directory, Cloud Interconnect, Cloud Storage, Web Security Scanner, Identity-Aware Proxy, VPC Service Controls, Google Cloud operations suite (formerly Stackdriver), Google Cloud Armor, Compute Engine ve Cloud Data Loss Prevention API.

Üçüncü taraf teknolojileri:

Forseti Inventory ve Forseti Scanner.

Prerequisites

Katılımcıların aşağıdaki bilgi ve deneyimlere sahip olması beklenmektedir:

- Google Cloud Fundamentals: Core Infrastructure eğitimini tamamlamış veya eşdeğer deneyime sahip olmak
- Networking in Google Cloud eğitimini tamamlamış veya eşdeğer deneyime sahip olmak
- Tercihen temel Kubernetes terminolojisine aşina olmak
- Deneyim veya SANS SEC301: Introduction to Cyber Security gibi çevrimiçi eğitimler aracılığıyla temel bilgi güvenliği kavramlarını bilmek
- Komut satırı araçları ve Linux işletim sistemi ortamlarında temel seviyede yetkin olmak
- On-premises veya public cloud ortamlarında uygulama deployment ve yönetimini kapsayan Systems Operations deneyimine sahip olmak
- Python veya JavaScript kodlarını okuyup anlayabilecek seviyede bilgi sahibi olmak

Security in Google Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

Bu eğitim özellikle:

- Cloud information security analyst, architect ve engineer'ları
- Information security ve cybersecurity uzmanları
- Cloud infrastructure architect'leri

için uygundur.

What You Will Learn

Eğitimin sonunda katılımcılar:

- Google'ın güvenlik yaklaşımını anlayabilir.
- Cloud Identity kullanarak yönetici kimliklerini yönetebilir.
- Resource Manager ve IAM ile least privilege yönetim yaklaşımını uygulayabilir.
- Identity-Aware Proxy kullanabilir.
- VPC firewall'ları ve Google Cloud Armor aracılığıyla IP trafiğine yönelik kontroller oluşturabilir.
- Özellikle veri ve sanal makinelerin herkese açık erişiminden kaynaklanan güvenlik açıklarını giderebilir.
- Cloud Data Loss Prevention API ile hassas verileri tarayabilir ve redaksiyon uygulayabilir.
- Audit logs üzerinden resource metadata yapılandırmalarındaki değişiklikleri analiz edebilir.
- Forseti kullanarak Google Cloud deployment'larını tarayabilir ve özellikle veri ile VM'lerin public erişimine ilişkin önemli güvenlik açıklarının giderilmesine yönelik çalışmalar gerçekleştirebilir.

Outline

Modül 1 – Google Cloud Security Temelleri

Konular

- Google Cloud'un güvenlik yaklaşımı
- Shared Security Responsibility Model
- Google ve Google Cloud tarafından azaltılan tehditler
- Access Transparency

Kazanımlar

Katılımcılar Google Cloud'un güvenlik yaklaşımını ve paylaşımlı güvenlik sorumluluğu modelini inceler. Google ve Google Cloud tarafından ele alınan tehdit türlerini öğrenir, Access Transparency kavramını tanımlar ve kullanım amacını anlar.

Modül 2 – Cloud Identity

Konular

- Cloud Identity

- Google Cloud Directory Sync
- Google Authentication ve SAML-based SSO
- Authentication best practices

Kazanımlar

Katılımcılar Cloud Identity'nin ne olduğunu ve hangi işlevleri yerine getirdiğini öğrenir. Directory Sync kullanılarak on-premises LDAP veya AD sunucusundaki kullanıcı ve izinlerin cloud ortamıyla güvenli biçimde nasıl senkronize edildiğini inceler.

Google Cloud authentication yöntemlerini, SSO yapılandırmasını ve Cloud Identity üzerinde groups, permissions, domains ve administrators yönetimine ilişkin iyi uygulamaları öğrenir.

Modül 3 – Identity and Access Management (IAM)

Konular

- Resource Manager
- IAM Roles
- IAM Policies
- IAM Recommender
- IAM Troubleshooter
- IAM Audit Logs
- IAM best practices

Kazanımlar

Projects, folders ve organizations dahil olmak üzere Resource Manager yapısı incelenir. Katılımcılar custom roles dahil IAM rollerini uygulamayı ve organization policies dahil IAM policies yapısını anlamayı öğrenir.

Separation of duties, least privilege, policy'lerde Google Groups kullanımı ve basic roles kullanımından kaçınma gibi iyi uygulamalar ele alınır. IAM, custom roles ve organization policies yapılandırmaları incelenir.

Uygulama

- Lab: Configuring IAM

Modül 4 – Isolation ve Security için Virtual Private Cloud Yapılandırması

Konular

- VPC Firewalls
- Load Balancing ve SSL Policies
- Interconnect ve Peering Policies
- VPC Network best practices
- VPC Flow Logs

Kazanımlar

Ingress ve egress kuralları dahil VPC firewall yapılandırmasına ilişkin iyi uygulamalar incelenir. Load balancing, SSL policies, private Google API access ve SSL proxy kullanımı ele alınır.

Peering, Shared VPC ve subnetwork kullanımı dahil VPC network güvenliği, VPN güvenliği ve Interconnect/Peering seçeneklerinin güvenlik açısından değerlendirilmesi üzerinde durulur. Katılımcılar ayrıca partner güvenlik ürünlerini tanır, VPC firewall yapılandırmasını öğrenir ve VPC Service Controls kullanarak data exfiltration'ın önlenmesini inceler.

Uygulamalar

- Lab: Configuring VPC Firewalls
- Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Modül 5 – Compute Engine Güvenliği: Teknikler ve İyi Uygulamalar

Konular

- Service Accounts, IAM Roles ve API Scopes
- VM Login yönetimi
- Organization Policy Controls
- Compute Engine best practices
- CSEK ile disk encryption

Kazanımlar

Katılımcılar default ve customer-defined Compute Engine service account'larını öğrenir. VM'lerde IAM roles ve scopes kullanımını inceler ve Shielded VM'lerin sistem ve uygulama bütünlüğünün korunmasına nasıl yardımcı olduğunu anlar.

Uygulamalar

- Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes
- Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Modül 6 – Cloud Data Güvenliği: Teknikler ve İyi Uygulamalar

Konular

- Cloud Storage IAM permissions ve ACLs
- Cloud Data auditing
- Signed URLs ve Policy Documents
- CMEK ve CSEK ile encryption
- Cloud HSM
- BigQuery IAM Roles ve Authorized Views
- Storage best practices

Kazanımlar

Cloud kaynaklarının permissions ve roles ile korunması, cloud verilerinin denetlenmesi ve Cloud Storage nesnelerine Signed URLs üzerinden erişim verilmesi incelenir.

Katılımcılar Signed Policy Document kullanarak Cloud Storage bucket'larına yerleştirilebilecek içerikleri yönetmeyi; CMEK, CSEK ve Cloud HSM kullanarak verileri şifrelemeyi; BigQuery verilerini IAM roles ve Authorized Views aracılığıyla korumayı öğrenir.

Uygulamalar

- Lab: Using Customer-Supplied Encryption Keys with Cloud Storage
- Lab: Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS
- Lab: Creating a BigQuery Authorized View

Modül 7 – Application Security: Teknikler ve İyi Uygulamalar

Konular

- Application security vulnerability türleri
- Web Security Scanner
- Identity ve OAuth Phishing tehditleri
- Identity-Aware Proxy
- Secret Manager

Kazanımlar

Katılımcılar farklı uygulama güvenliği açıklarını ve App Engine ile Cloud Functions'ın DoS korumalarını inceler. Web Security Scanner'ın risk azaltmadaki rolünü, Identity ve OAuth phishing tehditlerini ve Identity-Aware Proxy'nin bu risklere karşı kullanımını öğrenir.

Secret Manager kullanılarak application credentials ve metadata'nın güvenli biçimde saklanması da bu modülde ele alınır.

Uygulamalar

- Lab: Using Web Security Scanner to Find Vulnerabilities in an App Engine Application
- Lab: Configuring Identity-Aware Proxy to Protect a Project
- Lab: Configuring and Using Credentials with Secret Manager

Modül 8 – Google Kubernetes Engine Güvenliği

Konular

- Kubernetes/GKE'ye giriş
- Authentication ve Authorization
- Cluster hardening
- Workload security
- Monitoring ve Logging

Kazanımlar

Katılımcılar Kubernetes ortamının temel bileşenlerini ve Google Kubernetes Engine'de authentication ve authorization süreçlerinin nasıl çalıştığını öğrenir.

Kubernetes cluster ve workload'larının saldırılara karşı güçlendirilmesine yönelik yaklaşımlar ile GKE'deki logging ve monitoring seçenekleri incelenir.

Modül 9 – Distributed Denial of Service (DDoS) Saldırılarına Karşı Koruma

Konular

- DDoS saldırılarının çalışma biçimi
- Google Cloud mitigations
- Tamamlayıcı partner ürünleri

Kazanımlar

Katılımcılar DDoS saldırılarının nasıl gerçekleştirildiğini ve Cloud Load Balancing, Cloud CDN, autoscaling, VPC ingress/egress firewalls ve Google Cloud Armor gibi yaygın koruma yöntemlerini inceler.

Google Cloud Armor kullanılarak bir IP adresinin blocklist'e alınması ve HTTP load balancer erişiminin sınırlandırılması ele alınır.

Uygulama

- Lab: Configuring Traffic Blocklisting with Google Cloud Armor

Modül 10 – Content-Related Vulnerabilities: Teknikler ve İyi Uygulamalar

Konular

- Ransomware tehdidi
- Ransomware mitigations
- Data misuse, privacy violations ve sensitive content tehditleri
- Content-related mitigations

Kazanımlar

Ransomware tehdidi ile backups, IAM ve Cloud Data Loss Prevention API gibi azaltma yöntemleri ele alınır.

Katılımcılar data misuse, privacy violations ve sensitive/restricted/unacceptable content risklerini inceler. Cloud ML API'leriyle içerik sınıflandırma ve DLP API ile verilerin taranması ve redaksiyonu gibi koruma yöntemlerini öğrenir.

Uygulama

- Lab: Redacting Sensitive Data with the DLP API

Modül 11 – Monitoring, Logging, Auditing ve Scanning

Konular

- Cloud Audit Logs
- Forseti deployment ve kullanımı

Kazanımlar

Katılımcılar Security Command Center, Cloud Monitoring ve Cloud Logging kullanımını inceler. Monitoring ve Logging Agent'larının kurulumu ile Cloud Audit Logs yapılandırması ve görüntülenmesi üzerinde çalışır.

Ayrıca Forseti'nin deployment ve kullanımını, Forseti Inventory ile ortam envanterinin çıkarılmasını ve

Security in Google Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Forseti Scanner ile deployment'ın güvenlik açıkları açısından taranmasını öğrenir.

Uygulamalar

- Lab: Installing Cloud Logging and Monitoring Agents
- Lab: Configuring and Using Cloud Logging and Monitoring
- Lab: Configuring and Viewing Cloud Audit Logs