**CloudQuery**

**1. Nedir?**  
CloudQuery, bulut ortamlarındaki (örneğin AWS, Azure, GCP) kaynakları sorgulamak için kullanılan **açık kaynaklı bir denetim ve izleme aracıdır**.  
Verileri bir veritabanına çeker ve bunları **SQL sorguları ile analiz etmeni sağlar.**

Kısaca:  
- "Bulut sistemde ne var?"  
- "SQL ile incele."  
- "Güvenlik açıklarını ya da yanlış yapılandırmaları tespit et."



**2. Ne İşe Yarar?**

* AWS, Azure, Google Cloud gibi bulut sistemlerinden **veri toplar.**
* Bu veriler (örneğin sanal makineler, IAM rolleri, güvenlik duvarları) veritabanına aktarılır.
* Kullanıcı bu verileri SQL sorguları ile analiz eder.
* Cloud Security Posture Management (CSPM) için idealdir.

➡️ Örneğin: “Herkese açık olan S3 bucket var mı?” gibi soruları cevaplayabilir.

**3. Neden Önemlidir?**

* Bulut ortamları büyüdükçe, kaynakların kontrolü zorlaşır.
* Yanlış yapılandırılmış bir kaynak ciddi güvenlik açığı yaratabilir.
* CloudQuery ile tüm kaynaklar tek bir yerde toplanır ve analiz edilir.
* Bu sayede:  
  ✅ Hatalı yapılandırmalar fark edilir.  
  ✅ Güvenlik raporları hazırlanır.  
  ✅ Otomasyon ve sürekli denetim yapılabilir.

Özellikle DevOps, Blue Team ve güvenlik denetçileri için çok faydalıdır.

**4. Nasıl Kurulur? (Linux Örneği)**

Kurulumu oldukça kolaydır. Binary (çalıştırılabilir dosya) indirip kullanılır.

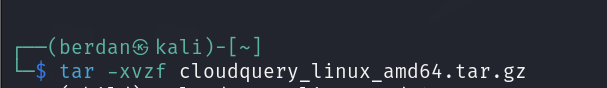
**# 1. CloudQuery binary dosyasını indir (örneğin Linux için)**

**wget** [**https://github.com/cloudquery/cloudquery/releases/latest/download/cloudquery\_linux\_amd64.tar.gz**](https://github.com/cloudquery/cloudquery/releases/latest/download/cloudquery_linux_amd64.tar.gz)

****

**# 2. Arşivi aç**

**tar -xvzf cloudquery\_linux\_amd64.tar.gz**

****

**# 3. Çalıştırılabilir hale getir**

**chmod +x cloudquery**

****

**# 4. Plugin’leri yüklemek için örnek yapılandırmayı kopyala**

**./cloudquery init aws**

**# 5. AWS erişim bilgilerini gir ve çalıştır**

**./cloudquery fetch**

🗃️ Veriler genellikle **PostgreSQL, SQLite, CSV** gibi formatlara aktarılabilir.

**5. Örnek Bir Anlatım:**  
Bir şirketteki AWS ortamını denetliyorsun. Amacın, herkesin erişebildiği S3 klasörlerini (bucket) bulmak. CloudQuery ile bu adımları izlersin:

1. AWS yapılandırmasını yaparsın **(AWS\_ACCESS\_KEY, AWS\_SECRET\_KEY)**
2. Verileri toplarsın:

**./cloudquery fetch**

1. SQL veritabanına aktarılan kaynaklar üzerinden sorgu yazarsın:

**SELECT name, public\_access FROM aws\_s3\_buckets WHERE public\_access = true;**

Sonuç: Herkese açık olan S3 klasörlerini birkaç saniyede listeleyebilirsin!

⚠️ **Uyarı:**  
CloudQuery sadece veri toplar ve analiz eder. Herhangi bir saldırı amacıyla kullanılmaz. Gerçek sistemlerde kullanılmadan önce yetki alınması ve ortamın test ortamı olması gerekir.