## **Hubble Nedir?**

**Hubble**, sistemlerin, dosyaların ve servislerin güvenlik açısından **belirli politikalar çerçevesinde sürekli gözlemini** sağlayan, **SaltStack tabanlı** açık kaynaklı bir güvenlik denetim aracıdır.  
Genellikle sistemlerin **uygunluk (compliance)** durumlarını ve **güvenlik duruşunu** ölçmek amacıyla kullanılır.

Özellikle sistem yöneticileri, SOC ekipleri ve denetim (audit) ekipleri için uygundur.

## **Neden Kullanılır?**

* Sistemlerin CIS, NIST gibi standartlara **uygunluğunu kontrol etmek** için
* Dosya izinlerini, sistem ayarlarını, çalışan servisleri vs. **otomatik olarak analiz etmek** için
* Sürekli gözlem ve güvenlik analizi sağlamak için
* Logları analiz ederek anomali tespiti yapmak için

## **Hubble Ne Yapar?**

Hubble modüler bir yapıya sahiptir ve şu alanlarda denetim yapabilir:

* Audit (denetim): CIS/NIST uyum denetimi
* File (dosya) analizi: Hatalı izinler, şüpheli dosyalar
* Grains/metadata: Donanım/sistem bilgileri toplama
* Logs: Syslog analizi, anormal durum tespiti
* Inspect: Komut çıkışı analizi (örneğin netstat, ps, who)
* Service: Şüpheli çalışan servislerin tespiti
* Statistics: Sistemdeki kullanıcı, servis, işlem sayıları vb.

**Kurulum:**

**git clone https://github.com/hubblestack/hubble.git**

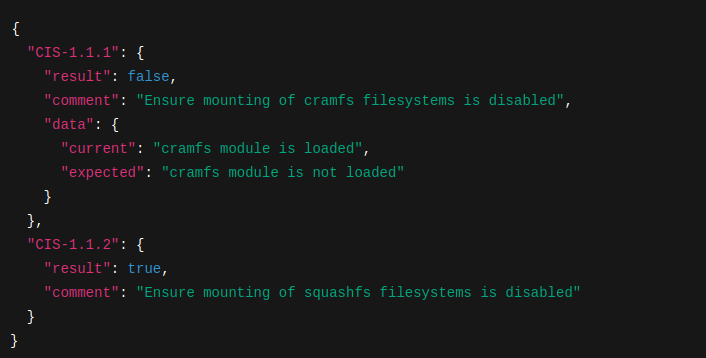
* cd hubble
* pip3 install -r requirements.txt

**Örnek konfigürasyonla çalıştırılır:**

* cp hubble/hubble.cfg /etc/hubble/hubble.cfg
* sudo hubble --config /etc/hubble/hubble.cfg

**Örnek Kullanım:**

hubble --module audit --profile hubblestack\_nova.ubuntu\_2004\_cis



**Bu çıktıda:**

* Denetlenen kuralların kimlik numarası (örneğin CIS-1.1.1)
* Sonucun başarılı olup olmadığı
* Açıklama ve varsa karşılaştırmalı veri yer alır.

## **Kullanım Senaryoları**

* CIS Benchmark denetimi (Ubuntu, CentOS gibi sistemler için)
* Şirket içi güvenlik politikalarının otomatik denetimi
* ISO 27001, NIST gibi sertifikasyonlara hazırlık
* Log, servis veya sistem yapılandırmasındaki anormalliklerin tespiti

## **Hubble Temel Parametreleri**

* --module <modül\_adı>  
  Çalıştırılacak modülü belirtir. Örnek: audit, file, log, inspect, service, statistics  
  (Örnek: hubble --module audit)
* --profile <profil\_adı>  
  Denetim için kullanılacak uyumluluk veya güvenlik profilini belirtir.  
  Örnek: hubblestack\_nova.ubuntu\_2004\_cis
* --config <dosya\_yolu>  
  Hubble için kullanılacak konfigürasyon dosyasını belirtir.  
  (Örnek: --config /etc/hubble/hubble.cfg)
* --output <dosya>  
  Çıktıların kaydedileceği dosya yolunu belirtir.
* --debug  
  Detaylı hata ve işlem çıktısı verir. Sorun giderme için kullanılır.
* --version  
  Hubble sürüm bilgisini gösterir.
* --help  
  Yardım metnini ve komut seçeneklerini gösterir.