Cado Response CE / Community Tools Kurulum Rehberi

# 1. Giriş

Cado Response CE, geçmişte bulut ortamlarında olay müdahalesi ve dijital adli analiz için ücretsiz bir çözüm sunmaktaydı.   
Ancak şu anda bu platform kullanımdan kaldırılmıştır. Yerine Cado Security, açık kaynaklı araçlar sunmaktadır.  
Bu belgede, Cado’nun GitHub üzerinden sunduğu açık kaynaklı araçların (cloudgrep, varc vb.) kurulumu ve kullanımı anlatılacaktır.

# 2. Gereksinimler

- Python 3.8+  
- Git  
- pip (Python package installer)  
- Linux (Ubuntu/Kali önerilir) veya macOS

# 3. Cloudgrep Kurulumu (Örnek)

Cloudgrep, bulut ortamlarında log aramak için kullanılan bir araçtır.

Aşağıdaki adımları takip ederek kurulumu gerçekleştirebilirsiniz:

1. GitHub deposunu klonlayın:  
 git clone <https://github.com/cado-security/cloudgrep.git>

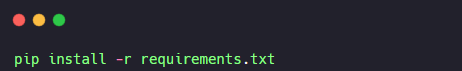
ekran görüntüsü, metin, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.  
  
2. Dizin içine girin:  
 cd cloudgrep

ekran görüntüsü, grafik, grafik tasarım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

3. Gerekli paketleri kurun:  
 pip install -r requirements.txt

  
  
4. Yardım menüsünü görüntüleyin:  
 python3 cloudgrep.py –help

ekran görüntüsü, yazı tipi, grafik, metin içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# 4. varc Kurulumu (VPC Akış Günlüklerini İnceleme)

varc, AWS VPC flow log’larını analiz etmek için kullanılan bir Cado aracıdır.

Kurulum:  
1. GitHub deposunu klonlayın:  
 git clone <https://github.com/cado-security/varc.git>

ekran görüntüsü, yazı tipi, grafik, metin içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.  
  
2. Dizin içine girin:  
 cd varc

ekran görüntüsü, saat, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.  
  
3. Gerekli bağımlılıkları yükleyin:  
 pip install -r requirements.txt

ekran görüntüsü, metin, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.  
  
4. Yardım komutlarını görmek için:  
 python3 varc.py --help  
metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# 5. Örnek Terminal Çıktısı

┌──(kali㉿root)-[~]  
└─$ python3 cloudgrep.py --profile default --query 'sourceIPAddress="1.2.3.4"'  
  
[INFO] Scanning logs for query: sourceIPAddress="1.2.3.4"  
[RESULT] Found 12 matching entries in AWS CloudTrail logs.  
metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# 6. Sonuç

Cado CE artık aktif bir platform değildir. Ancak Cado tarafından sunulan açık kaynak araçlar (cloudgrep, varc)   
olay müdahalesi ve bulut ortamı analizi için oldukça faydalıdır. Yukarıdaki kurulum adımları ile hızlıca bu araçları çalıştırabilirsiniz.