anomali tespiti yapmak için bir makine öğrenimi job'ı oluştur

1. Veriyi Hazırlama

Öncelikle, analiz etmek istediğimiz veriyi Elasticsearch'e yüklememiz gerekiyor. Örnek veri setimiz, kullanıcıların zaman damgalarıyla birlikte gerçekleştirdiği istekleri içerecek:

```json
PUT /web_requests/_doc/1
{
  "timestamp": "2023-10-01T00:00:00",
  "user_id": "user_1",
  "request_count": 5
}

PUT /web_requests/_doc/2
{
  "timestamp": "2023-10-01T00:01:00",
  "user_id": "user_2",
  "request_count": 2
}

// Bu şekilde devam edin...
```

2. Anomali Tespiti Job'ı Oluşturma

Anomali tespiti için bir job oluşturmak üzere aşağıdaki adımları izleyelim.

a. Job Tanımı

Aşağıdaki örnekte, her 15 dakikada bir kullanıcı isteklerinin sayısını incelemek için bir job tanımlıyoruz:

```json
POST _ml/anomaly_detectors/web_requests_anomaly
{
  "analysis_config": {
    "bucket_span": "15m",
    "detectors": [
      {
        "function": "high_count",
        "field_name": "request_count",
        "by_field_name": "user_id"
      }
    ]
  },
  "data_description": {
    "time_field": "timestamp"
```

```
  }
}
```

Açıklama:
- `bucket_span`: Analiz edilen zaman aralığı. Burada 15 dakikalık dilimler kullanıyoruz.
- `detectors`: Anomali tespiti için kullanılacak algoritmanın tanımı. `high_count`, belirli bir zaman diliminde beklenenden fazla isteği tespit eder.
- `by_field_name`: Kullanıcı kimliğine göre gruplama yapar.

3. Job'ı Başlatma

Job oluşturulduktan sonra, onu başlatmalısınız:

```json
POST _ml/anomaly_detectors/web_requests_anomaly/_start
```

4. Sonuçları İnceleme

Job çalıştığında, anomali tespit sonuçlarını sorgulayabilirsiniz. Sonuçları almak için şu API'yi kullanın:

```json
GET _ml/anomaly_detectors/web_requests_anomaly/results/anomalies
```

Bu sorgu, tespit edilen anomali durumlarını döndürecektir. Örneğin, bir kullanıcının beklenmedik bir şekilde artan istek sayısını gösteren kayıtlar alabilirsiniz.

5. Sonuçların Görselleştirilmesi

Sonuçları görselleştirmek için Kibana'yı kullanabilirsiniz. Anomali tespit sonuçlarını görselleştirmek için aşağıdaki adımları izleyin:

1. **Kibana**'da "Machine Learning" sekmesine gidin.
2. **Anomaly Detection** altında oluşturduğunuz job'ı seçin.
3. Tespit edilen anomalilerin grafiklerini ve raporlarını inceleyin.

6. Anomalilerin İzlenmesi

Anomalileri daha detaylı incelemek için, belirli bir zaman diliminde anomalilerin nedenini anlamak için ilgili veriyi sorgulayabilirsiniz. Örneğin, yüksek istek sayısına sahip kullanıcıları listeleyerek hangi etkinliklerin bu anomaliyi tetiklediğini görebilirsiniz.