Custom Detection Rules in Microsoft Defender XDR

Siber güvenliğin dinamiklerinde, ortamınızda oluşabilecek tehditlerin önüne geçmek, savunma stratejilerinizi sürekli güncellemek ve özelleştirmek çok önemlidir. Microsoft Defender XDR paketinin bir parçası olan Microsoft Defender for Endpoint, Custom Detection Rule oluşturma yeteneği de dahil olmak üzere bu amaç için güçlü araçlar sunmaktadır.

Bu blog yazısında, kurumunuzun güvenliğini güçlendirmek için bu özellikten nasıl yararlanabileceğinizi derinlemesine inceliyoruz

Custom Detection Rules

Microsoft Defender XDR – Custom Detection Rule, güvenlik ekiplerinin tehdit algılama yeteneklerini kendi ortamlarına ve ihtiyaçlarına göre uyarlamalarına olanak tanımaktadır. Kurumunuzun tehdit ortamına ve güvenlik ilkelerine dayalı kurallar oluşturarak, genel kuralların gözden kaçırabileceği tehditleri tespit edebilir, uyarabilir ve bunlara yanıt vermenizi sağlamaktadır.

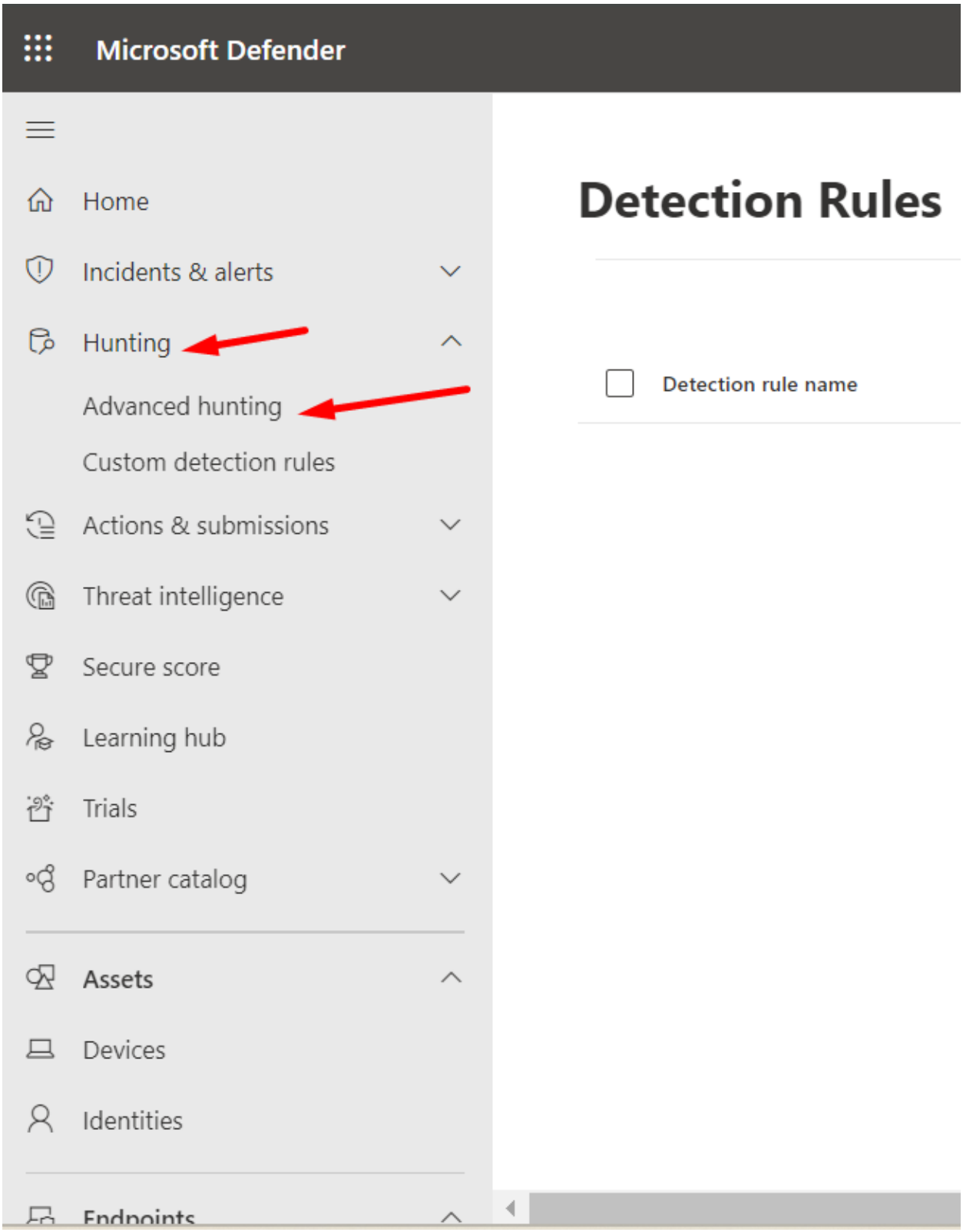
- Tailored Security: Özel kurallar, kuruluşunuzla ilgili olan ancak yaygın olmayabilecek belirli tehditleri ele alabilir.
- Proactive Defence: Ortaya çıkan tehditleri yaygın sorunlara dönüşmeden önce fark etmenizi ve azaltmanızı sağlar.
- Compliance Assurance: Özel kurallar, sektöre özgü uyumluluk gerekliliklerine uyum sağlamaya yardımcı olur.

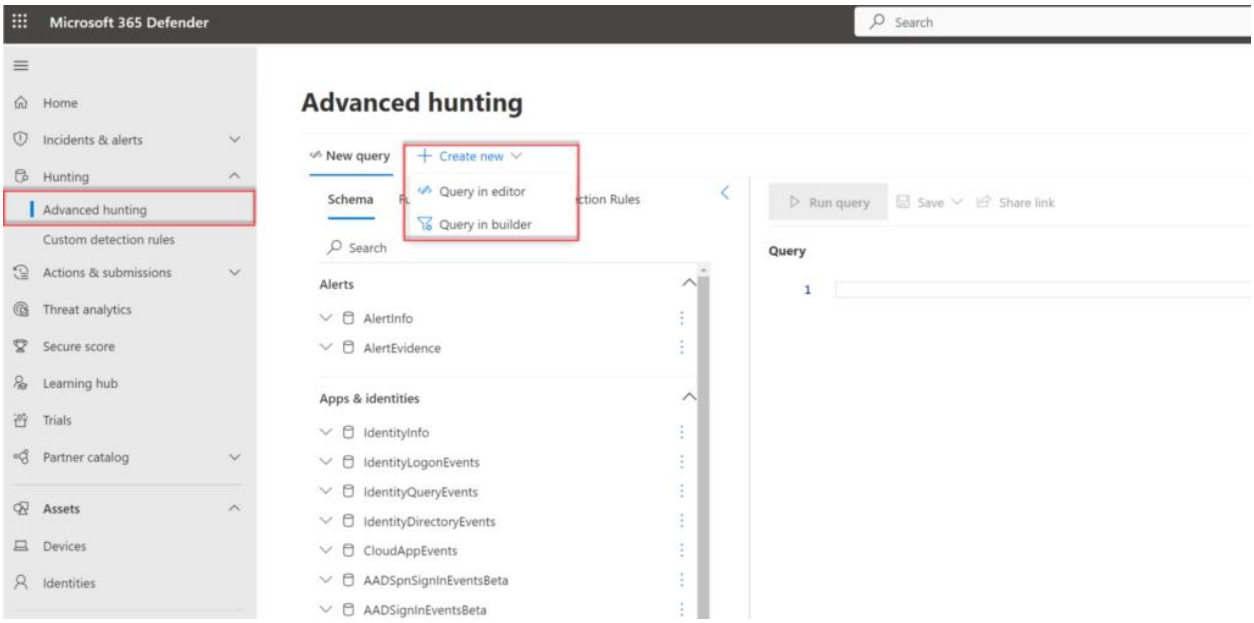
Custom Detection Rules Entegrasyonu

İlk olarak;

Ortamınızı analiz ederek ve mevcut tespit yeteneklerindeki boşlukları belirleyerek başlayın.

security.microsoft.com Adresine giriş yapınız. Advanced Hunting Sekmesine tıklayınız.

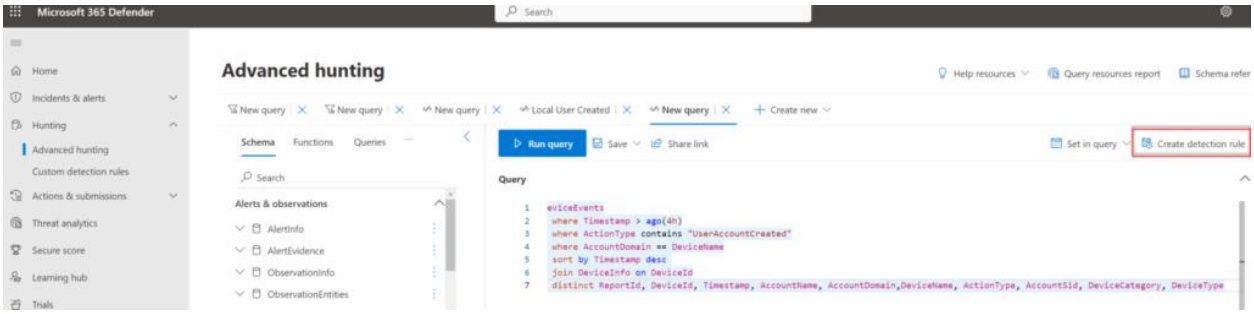

Microsoft Defender
Home
Incidents & alerts
Hunting
Advanced hunting
Custom detection rules
Actions & submissions
Threat intelligence
Secure score
Learning hub
Trials
Partner catalog
Assets
Devices
Identities
Endpoints
Detection Rules
Detection rule name



Microsoft: Kusto Sorgu Diline (KQL) genel bakış;

Guide moddaki Query Builder , Kusto Sorgu Dilini (KQL) bilmeden yeni sorguların oluşturulması için daha fazla görsel sağlar. Her deneyim kademesi sorgu oluşturucuyu kullanabilir ve verileri filtreleyebilir. KQL dilinde olduğu için bu konuda daha fazla bilgi edinmesi önerilir.

Custom Detection Rule Oluşturmak için Query Builder'da KQL sorgusunu oluşturun ve genel ayrıntılar dahil gerekli tüm bilgileri belirtmek için Create Detection Rule seçeneğini seçiyoruz.



Her kural son 30 gündeki eşleşmeleri kontrol eder. Kural birden fazla sıklık aralığıyla oluşturulabilir. Aşağıdaki şemaları kullanabiliriz;

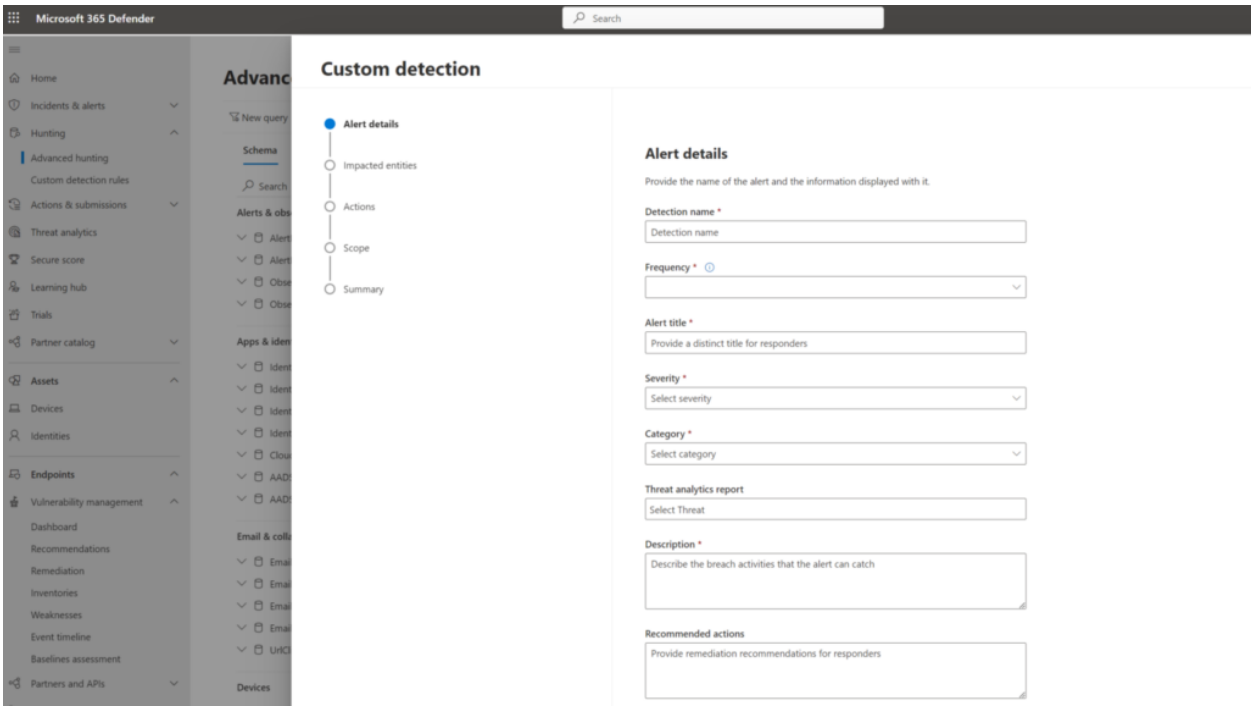
- **Every 24 hours**
- **Every 12 hours**
- **Every 3 hours**
- **Every hour**

NRT kuralları ile neredeyse gerçek zamanlı yeni özel tespitler ve kimlik tehditlerini daha hızlı oluşturmak mümkündür.

Şu anda NRT, kullanımda yalnızca bir tablo olduğunda ve sorgunun bir parçası olarak birleştirme, birleştirme veya harici veri operatörü bulunmadığında sorgular için desteklenmektedir. Şu anda NRT aşağıdaki tablolar için desteklenmektedir:

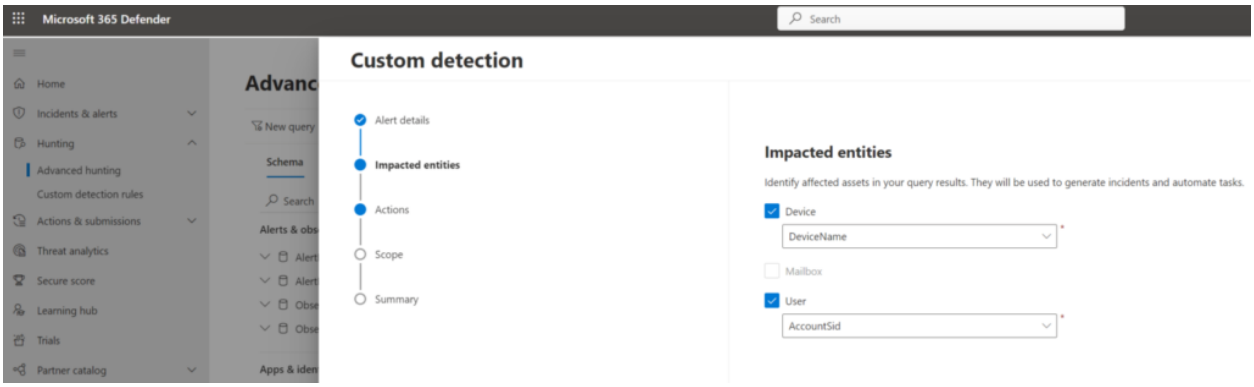
- AlertEvidence
- DeviceEvents
- DeviceFileCertificateInfo
- DeviceFileEvents
- DeviceImageLoadEvents
- DeviceLogonEvents
- DeviceNetworkEvents
- DeviceNetworkInfo
- DeviceInfo
- DeviceProcessEvents
- DeviceRegistryEvents
- EmailAttachmentInfo
- EmailEvents
- EmailPostDeliveryEvents
- EmailUrlInfo
- UrlClickEvents

Tüm isterleri dolduruyoruz;



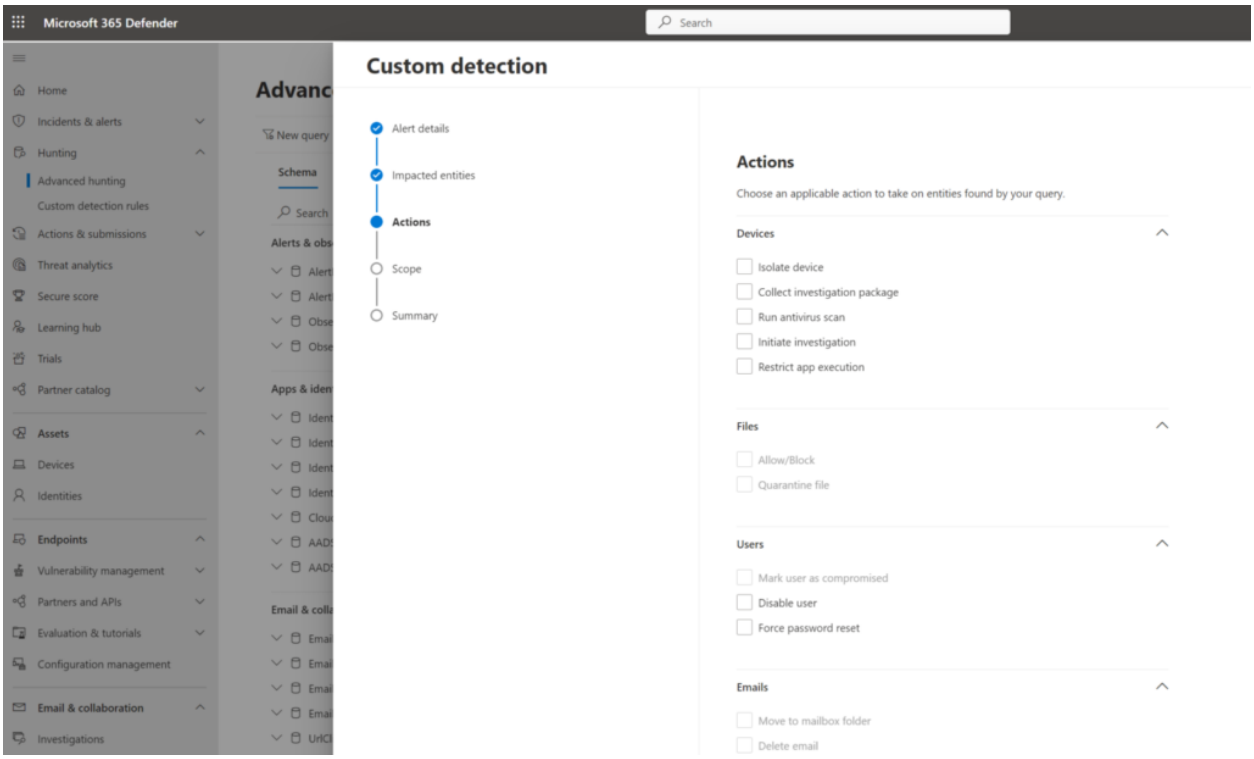
Impacted entities

Impacted entities, doğru etkilenen varlıkları sorgulamak ve yapılandırmak için önemlidir. Etkilenen varlık cihaz, kullanıcı veya etkilenen objelerdir. Cihaz eşlemesi örneğin DeviceId veya DeviceName ile eşleşmesi mümkündür. Kullanıcı, AccountSid ile eşleşmesi mümkündür.



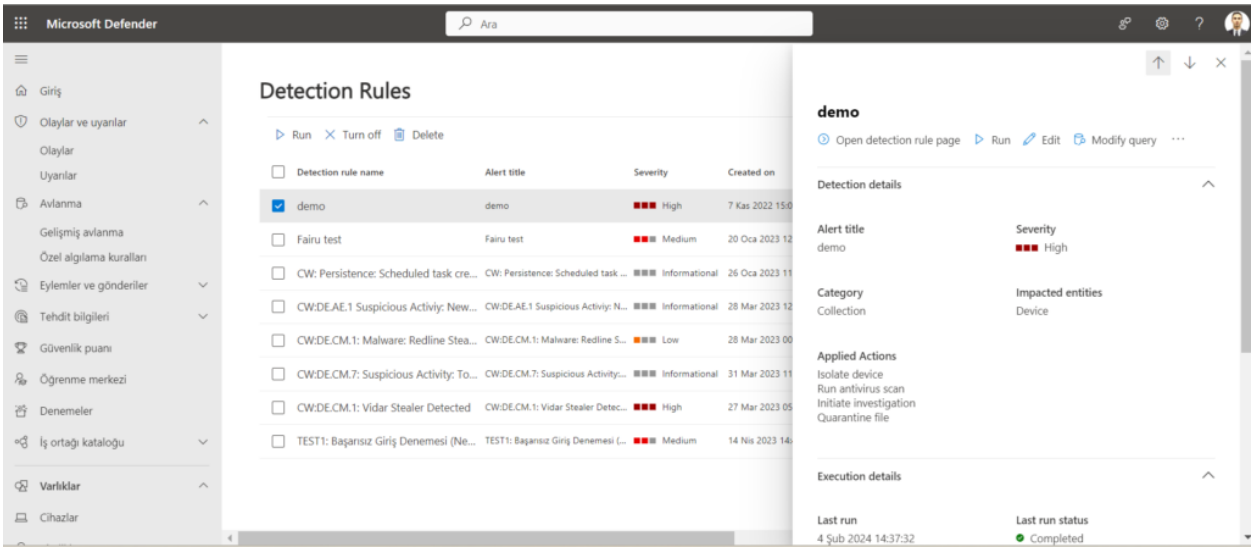
Actions

Her custom detection, cihazlar, kullanıcılar, dosyalar veya e-postalar üzerinde otomatik olarak yanıt eylemleri gerçekleştirebilir. Cihazlar için izole etmek, araştırma paketleri toplamak, antivirüs taramaları çalıştırmak, araştırmalar başlatmak veya uygulama yürütmeyi kısıtlamak mümkündür.



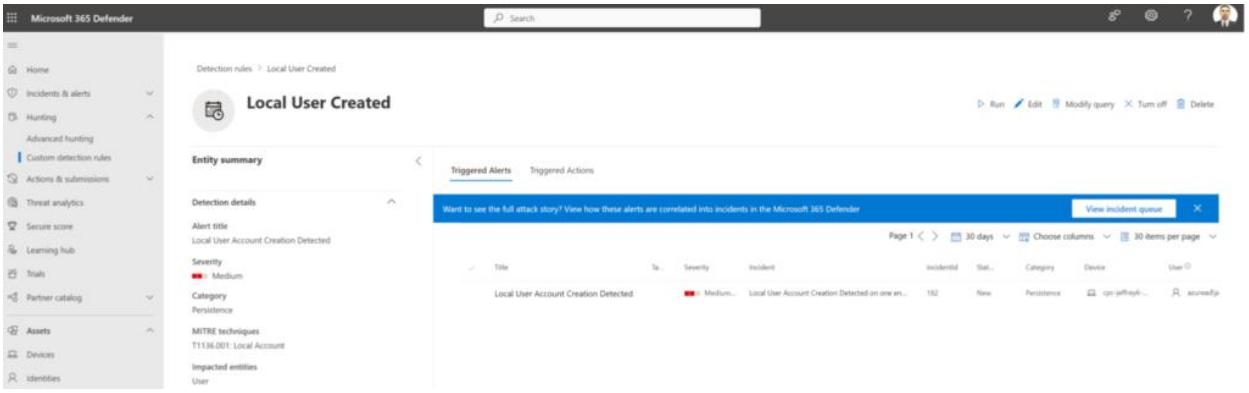
Oluşturulan Detection Rule'lar nasıl görüntülenir?

Oluşturulan tüm detection Rule'ları görüntülemek için **Advanced Hunting**-> **Custom Detection Rules** bölümüne gidiyoruz ve belirli bir kuralı açıyoruz. Bu görünümde, son çalıştırma, son çalıştırma durumu, sıklık, sonraki çalıştırma ve güncellenen zaman dahil olmak üzere tüm bilgiler mevcuttur.



Open detection Rule Page tıklıyoruz;

Detection Rule Page , tüm tetiklenen eylemleri ve kuralın tetiklenen eylemler bölümünü gösterir.



Custom Detection Rule ile yapılacak olan çalışmaları bir sonraki yazıda kaleme alıyor olacağım.

Bir sonraki yazı da görüşmek üzere.