

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.



Home



Incidents & alerts



Hunting



Advanced hunting

Custom detection rules



Actions & submissions



Threat intelligence



Secure score



Learning hub



Trials



Partner catalog



Assets



Devices



Identities



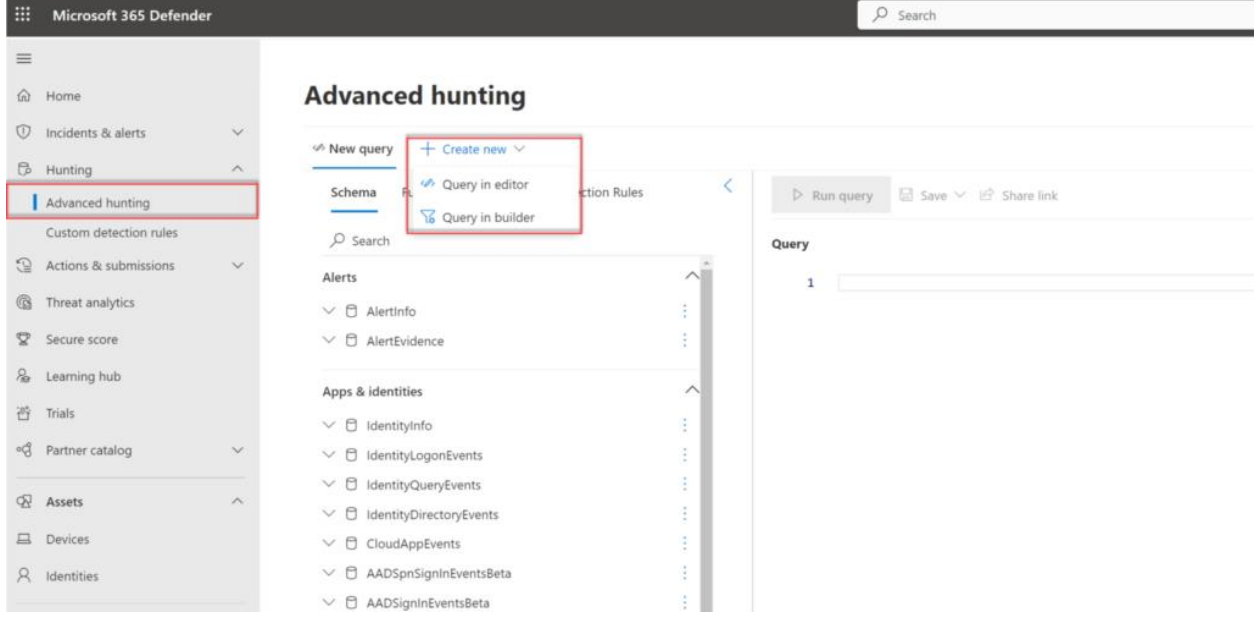
Endpoints



Detection Rules



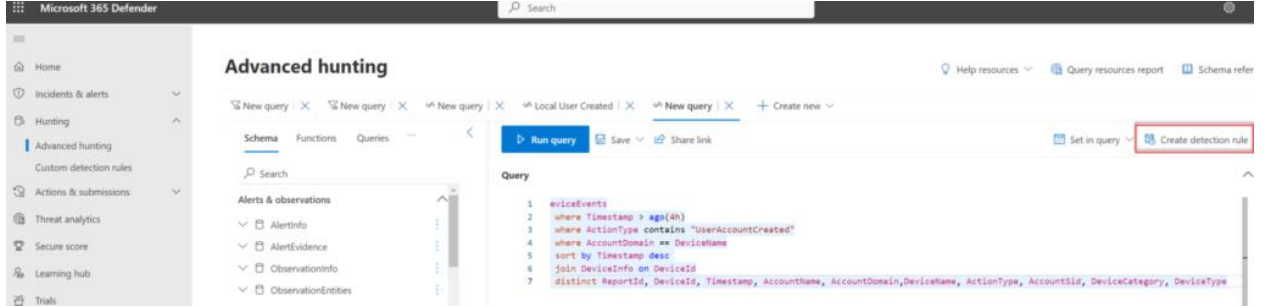
Detection rule name



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;

Microsoft 365 Defender

Search

Advanced hunting

Custom detection rules

Alerts & observations

Alert details

Impacted entities

Actions

Scope

Summary

Alert details

Provide the name of the alert and the information displayed with it.

Detection name *

Detection name

Frequency *

Alert title *

Provide a distinct title for responders

Severity *

Select severity

Category *

Select category

Threat analytics report

Select Threat

Description *

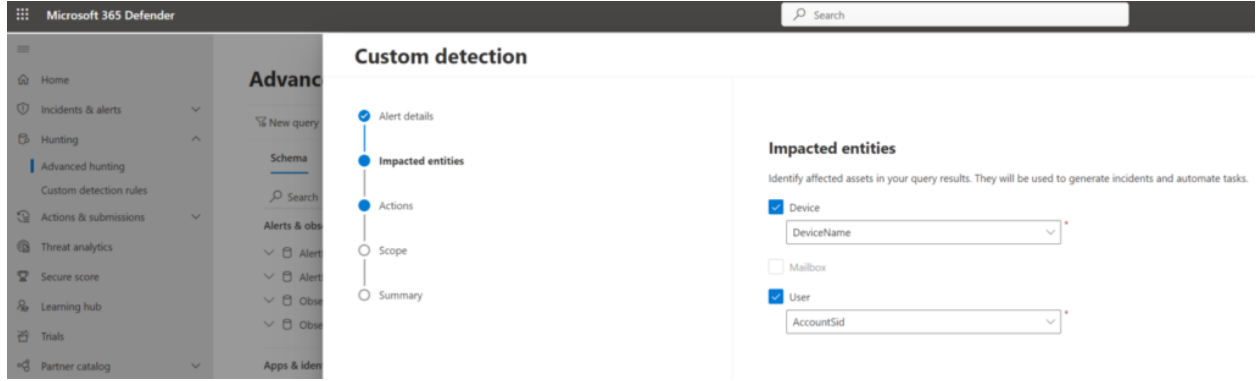
Describe the breach activities that the alert can catch

Recommended actions

Provide remediation recommendations for responders

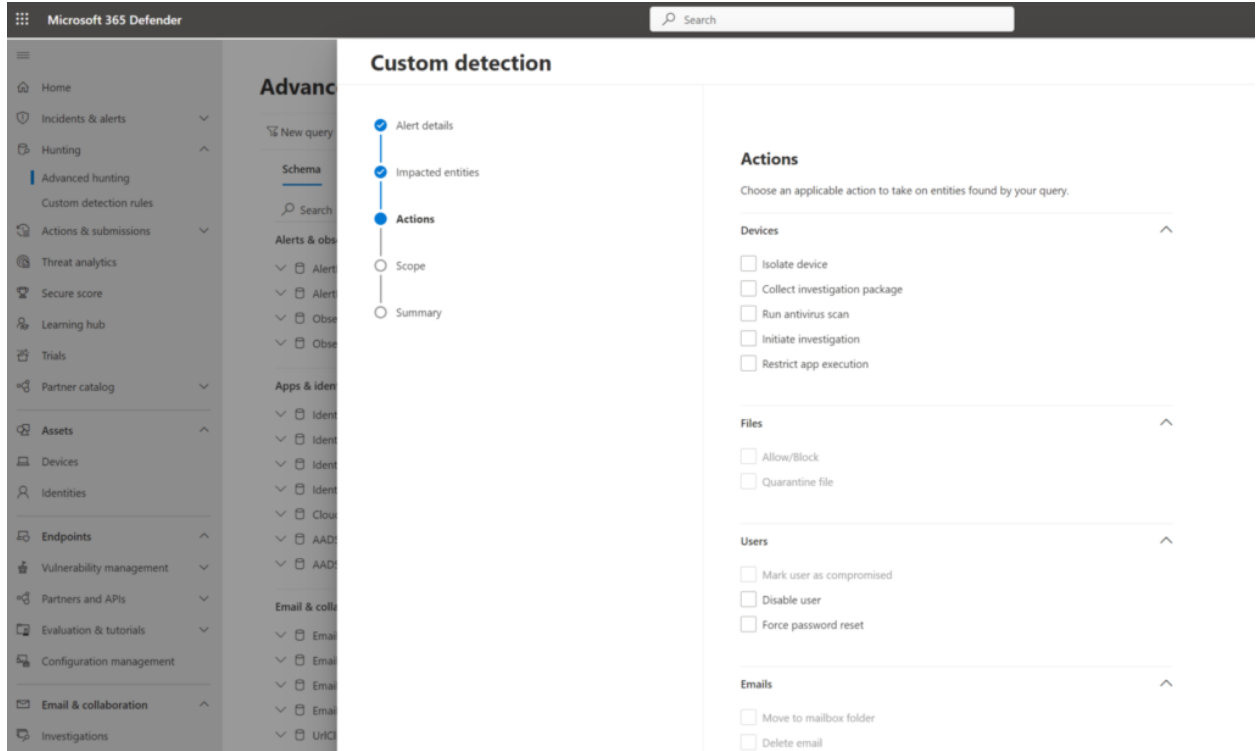
Impacted entities

Impacted entities, doğru etkilenen varlıkları sorgulamak ve yapılandırmak için önemlidir. Etkilenen varlık cihaz, kullanıcı veya etkilenen objelerdir. Cihaz eşleşmesi 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.

The screenshot shows the Microsoft Defender console. On the left is a navigation pane with options like 'Giriş', 'Olaylar ve uyarılar', 'Avlanma', 'Eylemler ve gönderiler', 'Tehdit bilgileri', 'Güvenlik puanı', 'Öğrenme merkezi', 'Denemeler', 'İş ortamı kataloğu', 'Varlıklar', and 'Cihazlar'. The main area is titled 'Detection Rules' and contains a table of rules. The 'demo' rule is selected, and its details are shown on the right. The details include the alert title 'demo', severity 'High', category 'Collection', impacted entities 'Device', and applied actions like 'Isolate device', 'Run antivirus scan', 'Initiate investigation', and 'Quarantine file'. The execution details show the last run on 4 Şub 2024 at 14:37:32, with a status of 'Completed'.

Detection rule name	Alert title	Severity	Created on
<input checked="" type="checkbox"/> demo	demo	High	7 Kas 2022 15:0
<input type="checkbox"/> Fairu test	Fairu test	Medium	20 Oca 2023 12
<input type="checkbox"/> CW: Persistence: Scheduled task cre...	CW: Persistence: Scheduled task ...	Informational	26 Oca 2023 11
<input type="checkbox"/> CW:DE.AE.1 Suspicious Activi: New...	CW:DE.AE.1 Suspicious Activi: N...	Informational	28 Mar 2023 12
<input type="checkbox"/> CW:DE.CM.1: Malware: Redline Stea...	CW:DE.CM.1: Malware: Redline S...	Low	28 Mar 2023 00
<input type="checkbox"/> CW:DE.CM.7: Suspicious Activity: To...	CW:DE.CM.7: Suspicious Activity...	Informational	31 Mar 2023 11
<input type="checkbox"/> CW:DE.CM.1: Vidar Stealer Detected	CW:DE.CM.1: Vidar Stealer Detec...	High	27 Mar 2023 05
<input type="checkbox"/> TEST1: Başarısız Giriş Denemesi (Ne...	TEST1: Başarısız Giriş Denemesi (...)	Medium	14 Nis 2023 14

Open detection Rule Page tıklıyoruz;

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

The screenshot shows the Microsoft 365 Defender console. The left navigation pane includes 'Home', 'Incidents & alerts', 'Hunting', 'Advanced hunting', 'Custom detection rules', 'Actions & submissions', 'Threat analytics', 'Secure score', 'Learning hub', 'Tools', 'Partner catalog', 'Assets', 'Devices', and 'Identities'. The main area is titled 'Local User Created' and shows the details of a triggered alert. The alert title is 'Local User Account Creation Detected', severity is 'Medium', and category is 'Persistence'. The impacted entities are 'User'. The right side shows a table of triggered alerts with columns for Title, To, Severity, Incident, IncidentID, Status, Category, Device, and User. The first row shows 'Local User Account Creation Detected' with a severity of 'Medium' and a status of 'New'.

Title	To	Severity	Incident	IncidentID	Status	Category	Device	User
Local User Account Creation Detected	Local User Account Creation Detected on one en...	Medium	New	152	New	Persistence	ipn-jffhph...	aswneqfj

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

Bir sonraki yazı da görüşmek üzere.