Microsoft Defender XDR Deception Capabilities

Deception teknolojisi, güvenlik ekiplerine olası bir saldırı konusunda anında uyarılar sağlayan ve onların gerçek zamanlı yanıt vermelerine olanak tanıyan bir güvenlik önlemidir.

Deception teknolojisi, ağınıza aitmiş gibi görünen cihazlar, kullanıcılar ve ana bilgisayarlar gibi sahte varlıklar oluşturur. Oluşturulan sahte objelerle iletişime giren saldırganlar, güvenlik ekiplerinin bir organizasyonun güvenliğini tehlikeye atacak potansiyel saldırıları önlemesine ve saldırganların eylemlerini izlemesine, böylece ekiplerin ortamlarının güvenliğini daha da artırmasına yardımcı olacaktır.

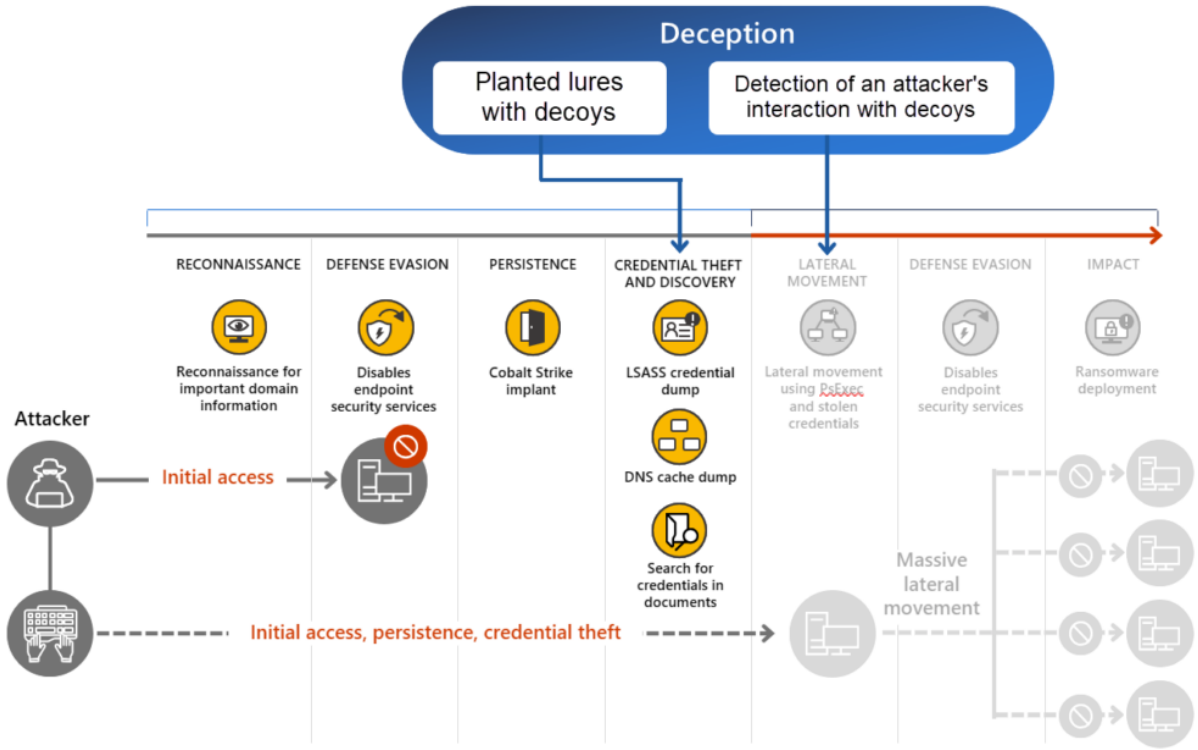
Önkoşullar

Aşağıdaki tabloda, Microsoft Defender XDR'de Deception özelliğini etkinleştirmek için gereken gereksinimler listelenmektedir.

Gereklilik	Detaylar
Abonelik gereksinimleri	- Microsoft 365 E5 - Microsoft Security E5 - Microsoft Defender for Endpoint plan 2
Dağıtım gereksinimleri	- Defender for Endpoint is the primary EDR solution - Automated investigation and response capabilities in Defender for Endpoint is configured - Devices are joined or hybrid joined in Microsoft Entra - PowerShell is enabled on the devices - The deception feature covers clients operating on Windows 10 RS5 and later in preview
İzinler	Deception yeteneklerini yapılandırmak için Microsoft Entra yönetim merkezinde veya Microsoft 365 yönetim merkezinde aşağıdaki rollerden birine atanmış olmanız gerekir : - Global Administrator - Security Administrator

Microsoft Defender XDR Deception yeteneği nasıl çalışır?

Microsoft Defender portalındaki yerleşik deception özelliği, ortamınıza uygun tuzaklar ve yemler oluşturmak için kuralları kullanır. Bu özellik, ağınıza uygun tuzaklar ve yemler önermek için makine öğrenimini uygular. Tuzakları ve yemleri manuel olarak oluşturmak için deception özelliğini de kullanabilirsiniz. Bu tuzaklar ve yemler daha sonra otomatik olarak ağınıza dağıtılır ve PowerShell kullanılarak belirttiğiniz cihazlara yerleştirilir.



Decoys , ağınıza aitmiş gibi görünen sahte cihazlar ve hesaplardır. **Lures,** belirli cihazlara veya hesaplara yerleştirilen sahte içeriklerdir ve bir saldırganın ilgisini çekmek için kullanılır. İçerik bir belge, bir yapılandırma dosyası, önbelleğe alınmış kimlik bilgileri veya bir saldırganın okuyabileceği, çalabileceği veya etkileşimde bulunabileceği herhangi bir içerik olabilir. Yemler önemli şirket bilgilerini, ayarlarını veya kimlik bilgilerini taklit eder.

Deception özelliğinde iki tür yem mevcuttur:

- **Temel yemler** – müşteri ortamıyla hiç etkileşimi olmayan veya çok az etkileşimi olan yerleştirilmiş belgeler, bağlantı dosyaları ve benzerleri.
- **Gelişmiş yemler** – önbelleğe alınmış kimlik bilgileri ve müşteri ortamına yanıt veren veya onunla etkileşime giren müdahaleler gibi yerleştirilmiş içerikler. Örneğin saldırganlar, oturum açmak için kullanılabilecek Active Directory sorgularına verilen yanıtlar olan sahte kimlik bilgileriyle etkileşime girebilir.

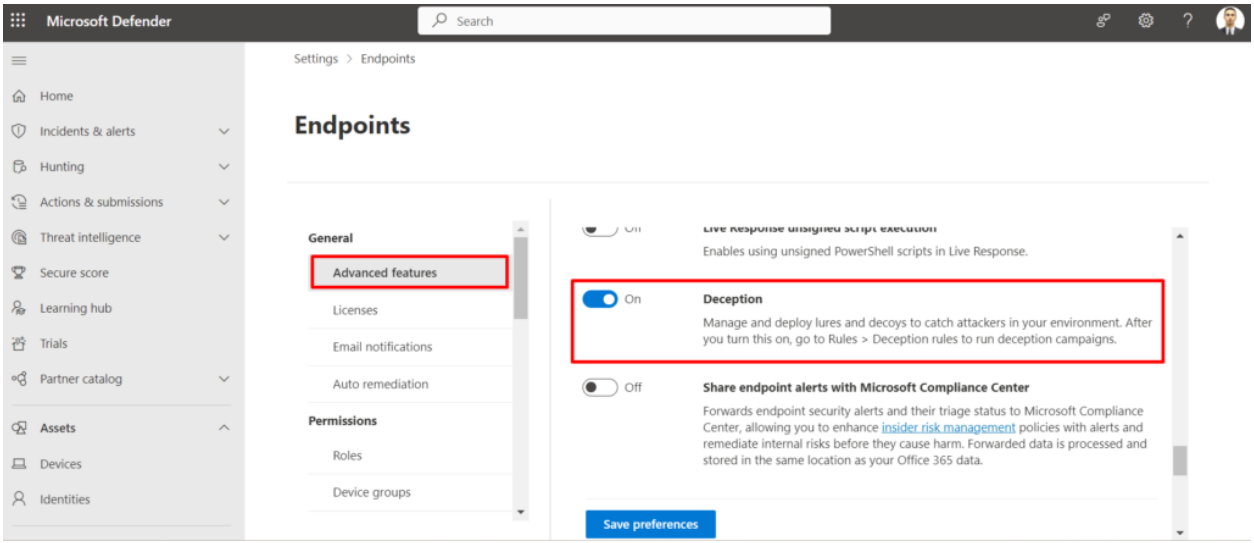
Yemler yalnızca bir deception kuralı kapsamında tanımlanan Windows istemcilerine yerleştirilir. Ancak, herhangi bir Defender for Endpoint yerleşik istemcisinde herhangi bir sahte ana bilgisayar veya hesap kullanma girişimleri bir deception uyarısına neden olur. Cihazlzar Uç Nokta için Microsoft Defender'a Onboard'da nasıl ekleyeceğinizi öğrenin . Yemlerin Windows Server 2016 ve sonraki sürümlere yerleştirilmesi gelecekteki geliştirmeler için planlanmaktadır.

Bir saldırgan, Defender for Endpoint'in yerleşik herhangi bir istemcisinde bir tuzak veya tuzak kullandığında, deception yeteneği, istemcide deception konuşlandırılıp dağıtılmadığına bakılmaksızın olası saldırgan etkinliğini gösteren bir uyarıyı tetikler.

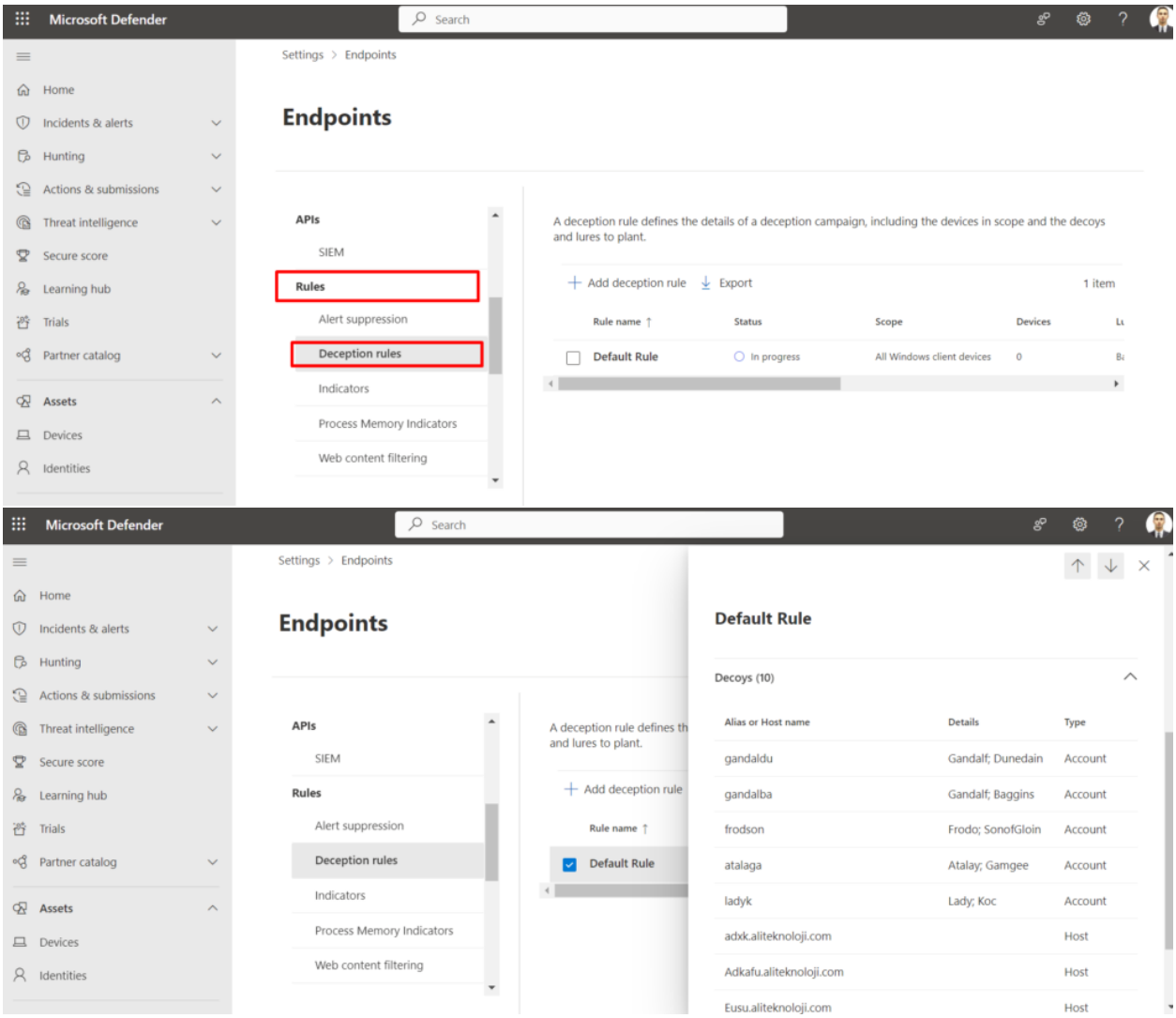
Microsoft Defender XDR Deception Capability'nin Aktifleştirilmesi;

Deception yeteneği varsayılan olarak kapalıdır. Açmak için aşağıdaki adımları uygulayabilirsiniz:

1. **Settings** > **Endpoints**.
2. **General**, select **Advanced features**.
3. Look for **Deception** capabilities and switch to **On**.



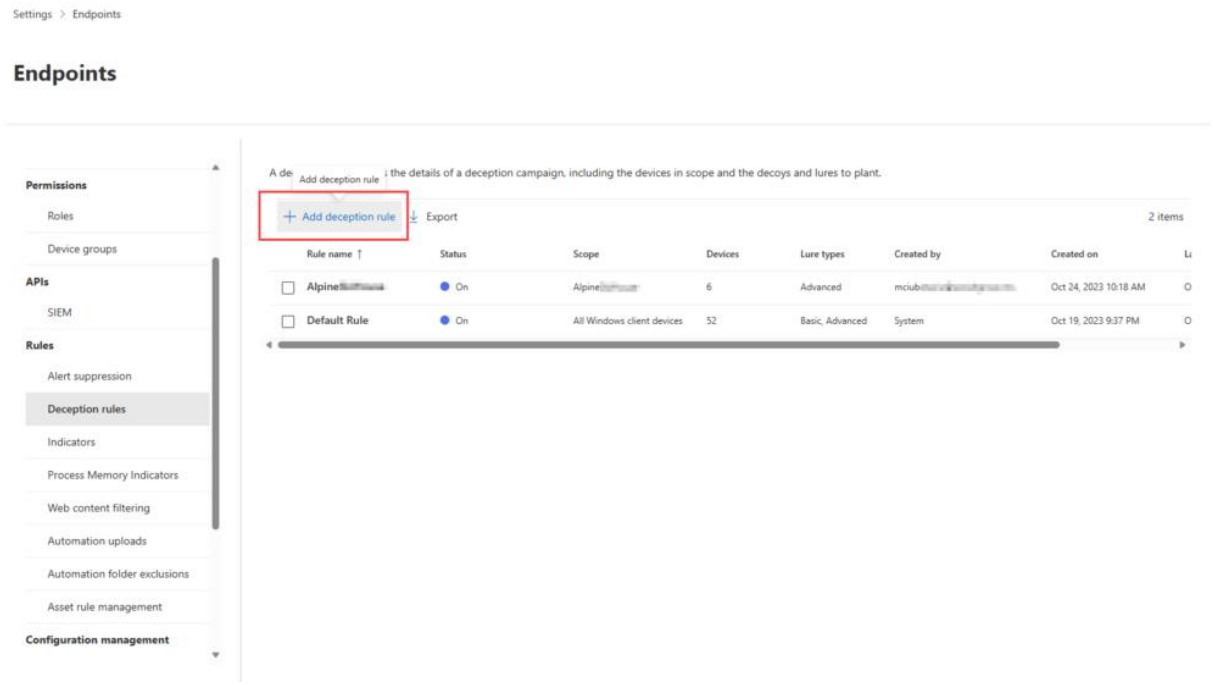
Deception yeteneği etkinleştirildiğinde varsayılan bir kural otomatik olarak oluşturulur ve etkinleştirilir. Buna göre düzenleyebileceğiniz varsayılan kural, yemlere entegre edilmiş tuzak hesapları ve ana bilgisayarları otomatik olarak oluşturur ve bunları kuruluştaki tüm hedef cihazlara yerleştirir. Deception özelliğinin kapsamı kuruluştaki tüm cihazları kapsayacak şekilde ayarlanırken, tuzaklar yalnızca Windows istemci cihazlarına yerleştirilmektedir.



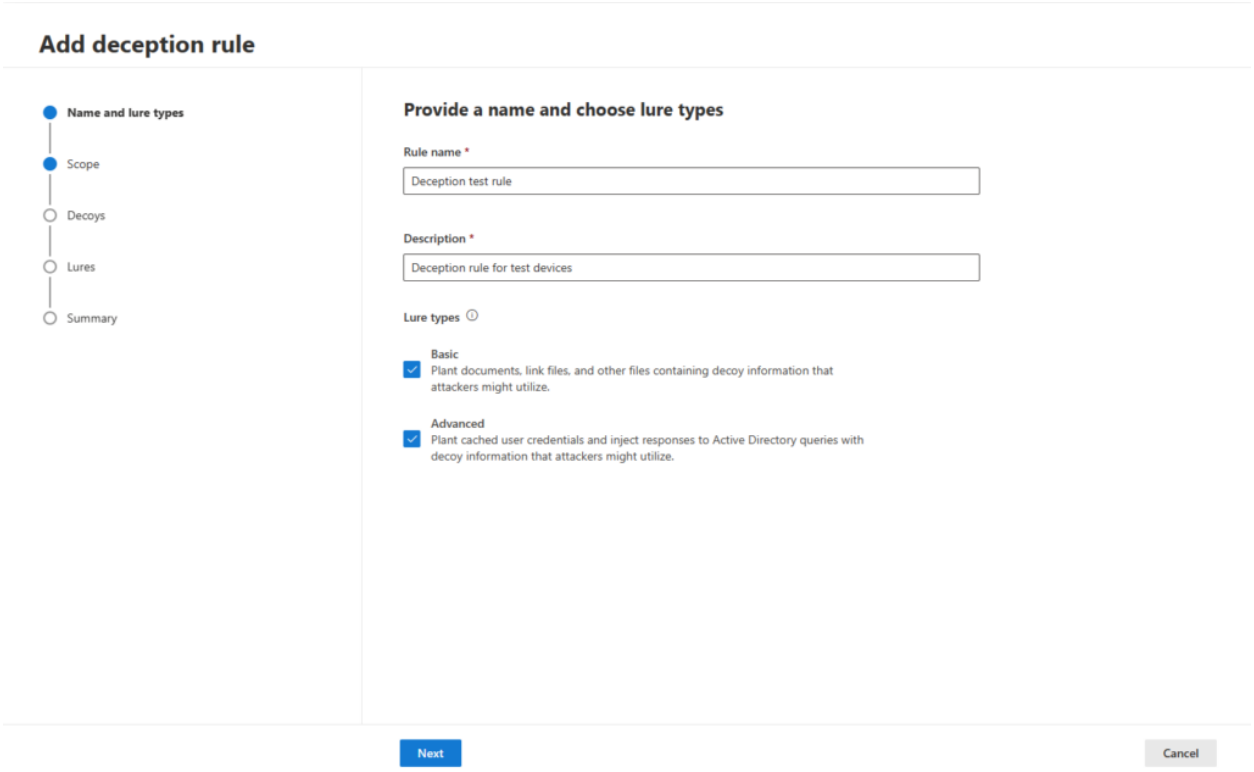
Deception kuralları oluşturma ve değiştirme

Deception Kuralı oluşturmak için ;

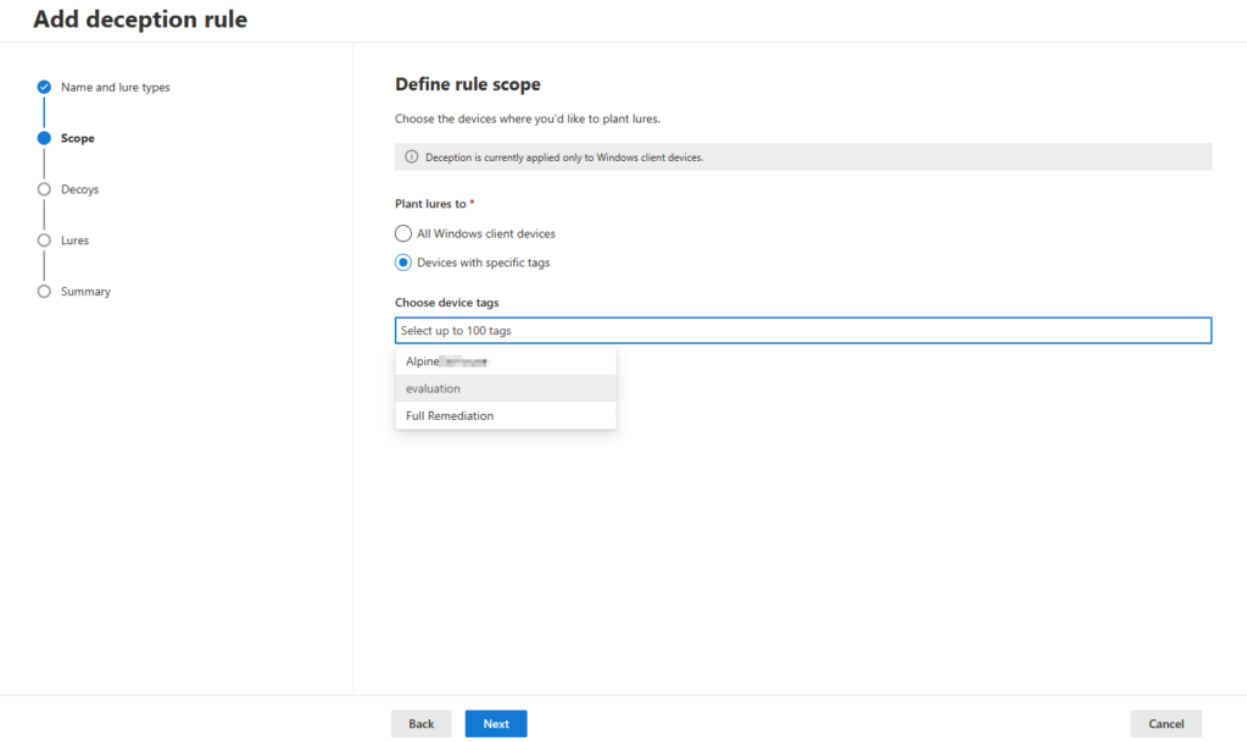
Add Deception Rule seçeneğini seçiyoruz;



Kural oluşturma bölmesinde bir kural adı ve açıklama ekleyin ve hangi yem türlerinin oluşturulacağını seçmeliyiz. Advanced ve Basic birlikte seçilebilmektedir.



Kapsam bölümünde yemleri yerleştirmeyi düşündüğünüz cihazları belirleyeceğiz. Yemleri tüm Windows istemci cihazlarına veya belirli etiketlere sahip istemcilere yerleştirmeyi seçebilirsiniz. Deception özelliği şu anda yalnızca Windows istemcilerini kapsamaktadır.



Deception yeteneğinin daha sonra otomatik olarak sahte hesaplar ve ana bilgisayarlar oluşturması birkaç dakika sürmektedir. Deception yeteneğinin, Active Directory'deki Kullanıcı Asıl Adını (UPN) taklit eden sahte hesaplar oluşturuyor ve bu hesapları görüntüleyebiliyorsunuz.

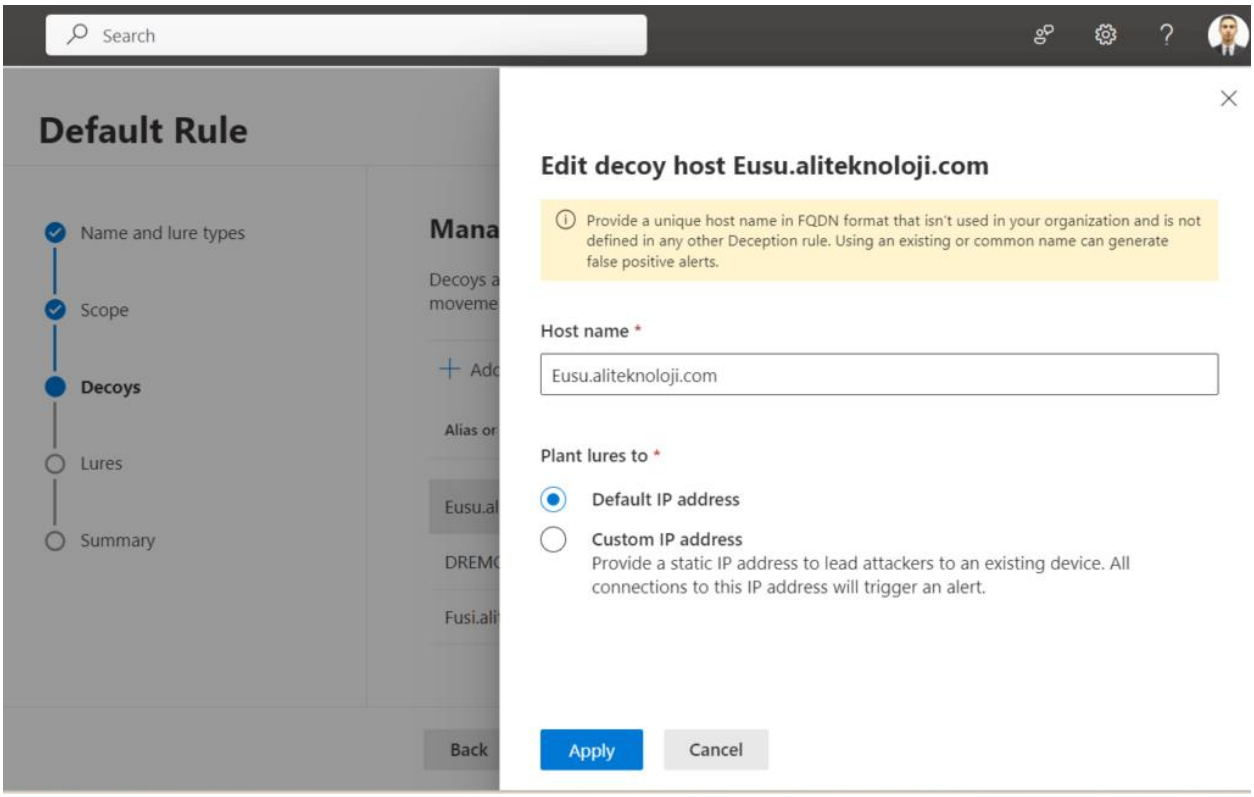
Otomatik olarak oluşturulan tuzakları inceleyebilir, düzenleyebilir veya silebilirsiniz. Ayrıca bu bölüme kendi tuzak hesaplarınızı ve ana bilgisayarlarınızı da ekleyebilirsiniz. Yanlış pozitif algılamaları önlemek için eklenen ana bilgisayarların/IP adreslerinin kuruluş tarafından kullanılmadığından emin olmak önemlidir.

Default Rule

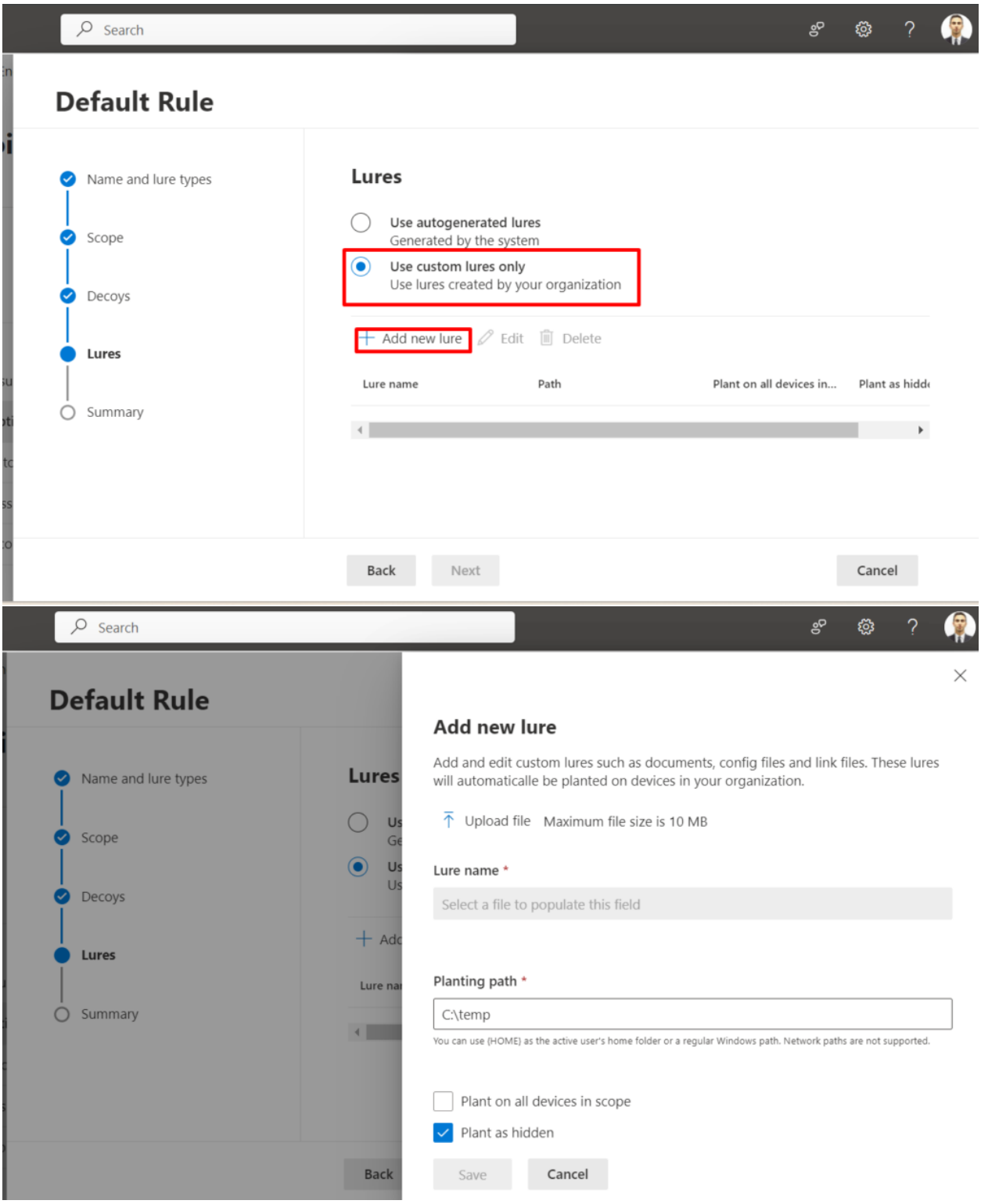
Decoys (10)

Alias or Host name	Details	Type
gandaldu	Gandalf; Dunedain	Account
gandalba	Gandalf; Baggins	Account
frodson	Frodo; SonofGloin	Account
atalaga	Atalay; Gamgee	Account
ladyk	Lady; Koc	Account
adxk.aliteknoloji.com		Host
Adkafu.aliteknoloji.com		Host
Eusu.aliteknoloji.com		Host

Tuzak hesap adını, ana bilgisayar adını ve yemlerin yerleştirildiği IP adresini tuzaklar bölümünde düzenleyebilirsiniz. IP adreslerini eklerken kuruluşta mevcutsa korumalı alan IP'si kullanmanızı öneririz. Yaygın olarak kullanılan adresleri kullanmaktan kaçınmalısınız; örneğin *127.0.0.1* , *10.0.0.1* ve benzeri.



Lures bölümünde otomatik olarak oluşturulmuş yemler mi yoksa özel yemler mi kullandığınızı belirleyeceksiniz. Yalnızca kendi yeminizi yüklemek için **Use Custom Lures** altında **Add New Rules** seçeneğini seçebilirsiniz . Özel yemler herhangi bir dosya türünde olabilir (.DLL ve .EXE dosyaları hariç) ve her biri 10 MB ile sınırlıdır. Özel yemler oluştururken ve yüklerken, yemlerin saldırganlar için çekici olmasını sağlamak amacıyla önceki adımlarda oluşturulan sahte ana bilgisayarları veya sahte kullanıcı hesaplarını içermesini veya bunlardan bahsetmesi gerçekçi bir senaryoya sahip olmanızı sağlayacaktır.



Tüm bu işlemler sonrası, Summary kısmında kontrollerimizi yaptıktan sonra kuralımızı oluşturabiliriz. Yeni kural, başarılı bir şekilde oluşturulduktan sonra Deception Rules bölmesinde görünür. Kural oluşturma işleminin tamamlanması yaklaşık 12-24 saat sürebilmektedir.

Bir sonraki makalede görüşmek üzere