

# Phishing Simulation Çalışmaları için M365 Defender 'da Bypass İşlemleri

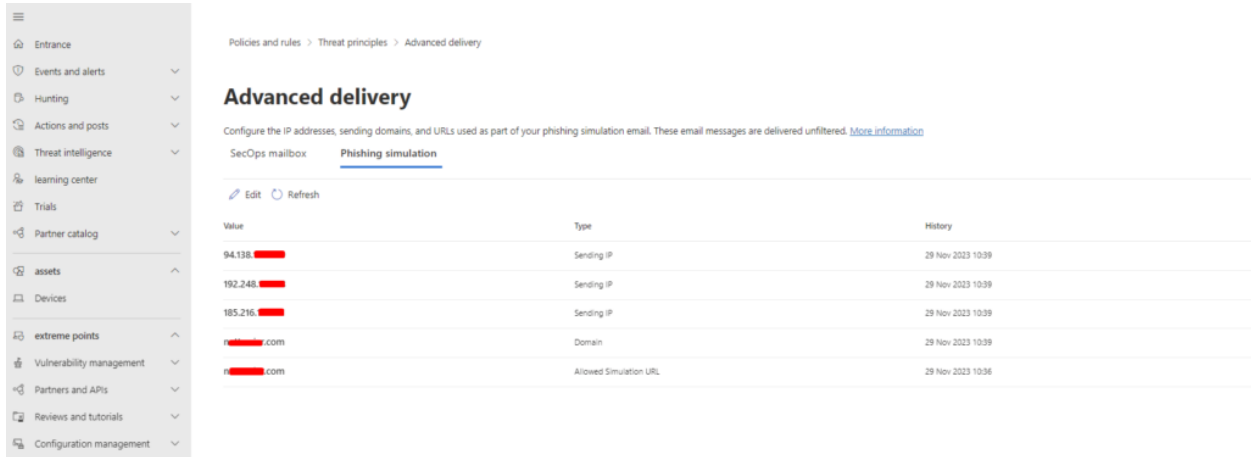
Kurumlara yönelik e-posta veya sms ile gerçekleştirilen ve hedef kitlenin siber güvenlik farkındalığını test eden simülasyon çalışmalarını Phishing Simulation olarak adlandırıyoruz. Saldırganlar saldırılarda kullandığı içerikleri simule edebildiğimiz bu platformlar sayesinde çalışanların farkındalık seviyelerini ölçebilir, ölçeklendirebilir ve eğitimlerle güçlendirebiliriz.

Microsoft bu testleri sağlamak için Defender for office 365 bünyesinde "Phishing Simulation Training" modülünü kullanmaktadır. Oluşturulan payload'lar sayesinde bu testler gerçekleştirilebilir ve sonuçlar raporlanabilir.

Ancak üçüncü parti bir Phishing Simulation ürünü kullanılmak istendiğinde Microsoft Defender for Office 365 ve içerisinde bulunan Threat Protection politikaları aktif olduğu için gelecek olan simulation maillerini algılayarak bunları engelleyecektir. Bu sebeple bir "**Allowlist**" oluşturarak Simulation Testi'nin başarıyla gerçekleşmesi için **Advanced Delivery Policy** oluşturulmalıdır.


Aşağıdaki adımları izleyerek politikayı güncelleyebilirsiniz.

Aşağıdaki bağlantıdan Microsoft 365 Defender'da oturum açarak Advanced Delivery sayfasına ulaşabilirsiniz; <https://security.microsoft.com/advanceddelivery?viewid=PhishingSimulation>



Value	Type	History
94.135. [redacted]	Sending IP	29 Nov 2023 10:39
192.248. [redacted]	Sending IP	29 Nov 2023 10:39
185.216. [redacted]	Sending IP	29 Nov 2023 10:39
[redacted].com	Domain	29 Nov 2023 10:39
[redacted].com	Allowed Simulation URL	29 Nov 2023 10:36

*Note: Link üzerinden erişemezseniz bu adımlarla Advanced Delivery ekranına erişebilirsiniz. <https://security.microsoft.com/> and clicking through Email & Collaboration > Policies & Rules > Threat Policies > Advanced Delivery > Phishing Simulation*

2.  **Edit** seçeneğini tıklayarak ekleme yapabilir veya düzenleyebilirsiniz. Daha önce bir konfigürasyon yapılmadıysa orada **Add** seçeneğini görüyor olacaksınız.

## Edit third-party phishing simulations

Phishing simulations are attacks organized by your security team and used for training and education purposes. Simulations can help identify vulnerable users and reduce the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one **Sender domain** entry [source domain or DKIM] and at least one **Sender IP entry to ensure message delivery**. URLs in the email message body are automatically allowed on click, based on the permission process of this phishing simulation system.

Note: **The Allowed simulation URLs** field is optional and can be used for non-email based simulated phishing campaign scenarios. Specifying URLs in this field ensures that these URLs are not blocked on click for simulated phishing scenarios using Microsoft Teams and Office applications (Word, Excel,...). [Learn more](#)

Domain (0 items) ⓘ



Sending IP (0 items)



Allowed simulation URLs (0 items) ⓘ



Save

Cancel

Edit ekranında açılan sayfada yukarıda gördüğünüz gibi Domain / Sending IP / Allowed Simulation URLs ekranını görüntülüyor olacaksınız. Aşağıda belirtilmiş olan formatlarda Phishing Simulation sağlayıcısı olan üçüncü parti firmanın bilgilerini girmeniz gerekmektedir.

- Sending Domain:

simulation.aliteknoloji.com

outbound.aliteknoloji.com

- Sending IP:

2.146.21.123

10.202.24.211

- Simulation URLs to allow:

authwebmail.com/\*

\*.authwebmail.com/\*

aliteknoloji.com/\*

\*.aliteknoloji.com/\*

Tüm girişler yapıldıktan sonra "save" diyerek sonuçlandırabiliriz.

Bu işlem sonrasında, bu IP adresinden ve Domainden gelen mailler filtrelere takılmayarak kullanıcıya ulaşacaktır. Ayrıca Phishing Simulation içerisinde yer alan ortalama linkleri "Safe Links" politikasına takılmadan son kullanıcının kontrolünde olacaktır. Simulation çalışmaları sonrası buradan ilgili domain ve ip addressleri silinebilir.

*Not: Listesinin etkili olması bir saat kadar sürebilmektedir*