Microsoft Teams 'i Defender ile Nasıl Koruyabiliriz ?

Toplantı uygulamaları kullanımı ve uzaktan çalışmanın yaygınlaşmasıyla artık yeni bir riske de kendimizi açmış bulunuyoruz. Microsoft Teams, kötü amaçlı yazılımları iletmek veya saldırganların açıklıktan faydalanarak bilgi güvenliği zaafiyetine sebebiyet vermek için kullanabildiği ve korumamız gereken bir saldırı yüzeyi konumuna büründü. Geçtiğimiz aylarda Microsoft Güvenlik araştırmacıları tarafından çok sayıda saldırı türü yayınlandı. Saldırganlar, kötüye kullanım ve kötü amaçlı mesajlar göndermek için sürekli olarak yeni yöntemler geliştiriyorlar.

Microsoft Teams aracılığıyla kötü amaçlı saldırıları tespit etmek ve önlemek için birkaç yeni özellikten bahsetmek istiyorum;

Microsoft Defender for Office 365, Microsoft Teams için Safe Links ve Sharepoint, OneDrive ve Microsoft Teams için Safe Attachment aracılığıyla Teams'deki URL'ler ve dosyalar için **tıklama süresi koruması** sağlıyor.

Bu iki özelliğe ek olarak da , Şüpheli Teams iletilerini bildirme, ZAP(Zero-Hour Auto Purge) özelliklerinin kullanımı, Karantina Teams iletileri , Teams Mesaj Varlık Paneli ve Saldırı simulasyon uygulamaları ile belli çalışmalar yapılabiliyor.

Tüm özellikler Microsoft 365 Defender'ın bir parçasıdır ve Microsoft 365 E5/Office 365 Plan 2 mevcut olduğunda kullanılabilir durumdadır.

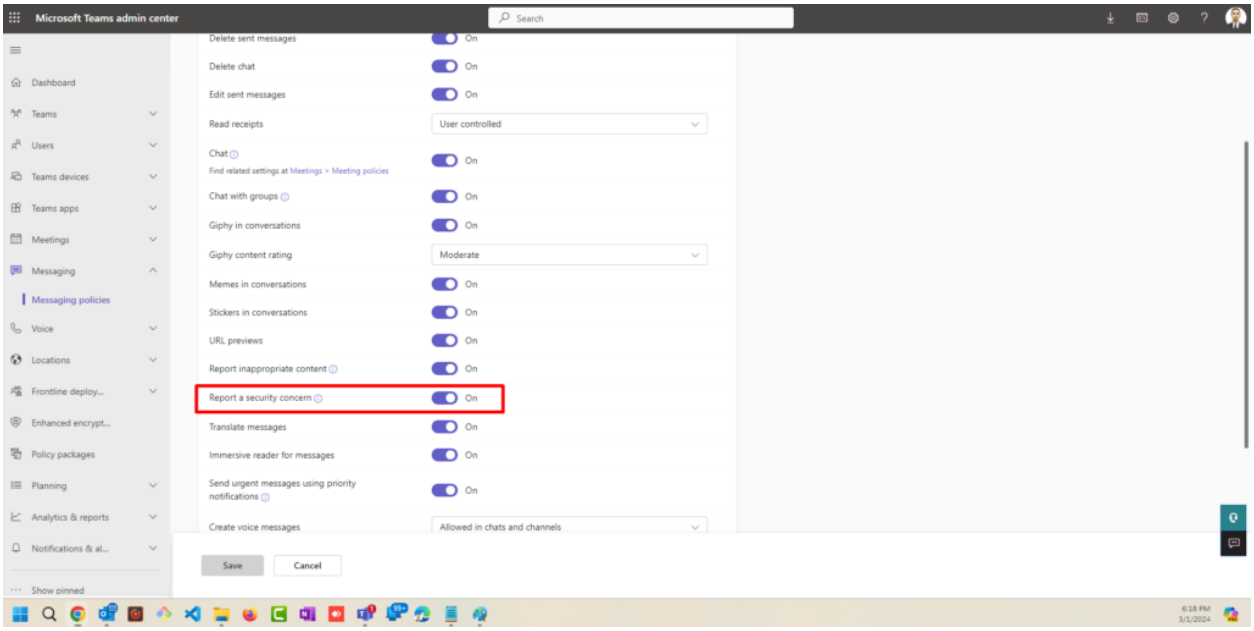
Şüpheli olan Teams İletilerini Nasıl Bildirebilirim ?

Bu özellik sayesinde kullanıcılar şüpheli Teams mesajlarını yetkililere bildirebilirler. Yöneticiler/Güvenlik analistleri bildirilen mesajları görebilir. Kullanıcılar Teams'deki mesajları birebir sohbetlerden, kanallardan ve toplantı konuşmalarından raporlayabilir. Kullanıcılar mesajları kötü amaçlı veya şiddet içeren, kaba sözler içeren mesaj olarak bildirebilirler.

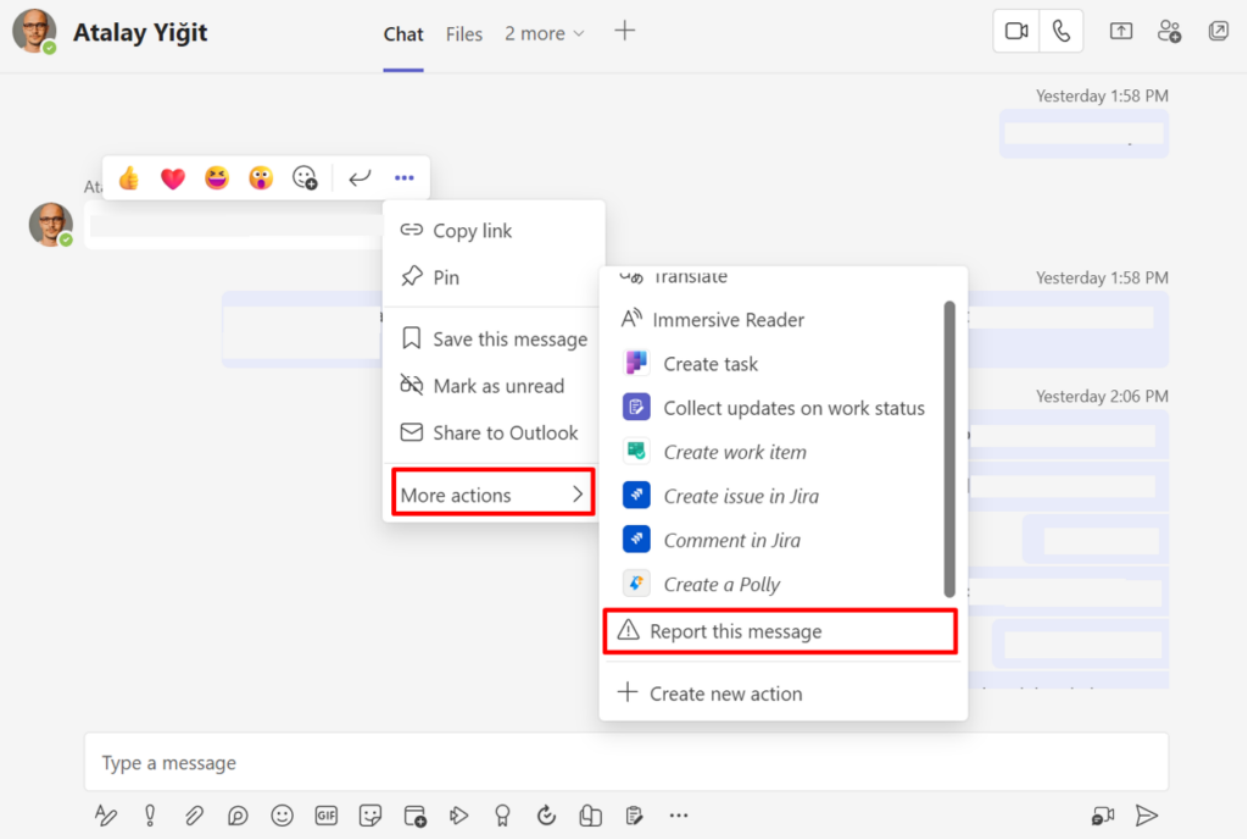
Öncelikle, Teams ayarlarımızda report özelliğinin açık olması gerekmektedir.

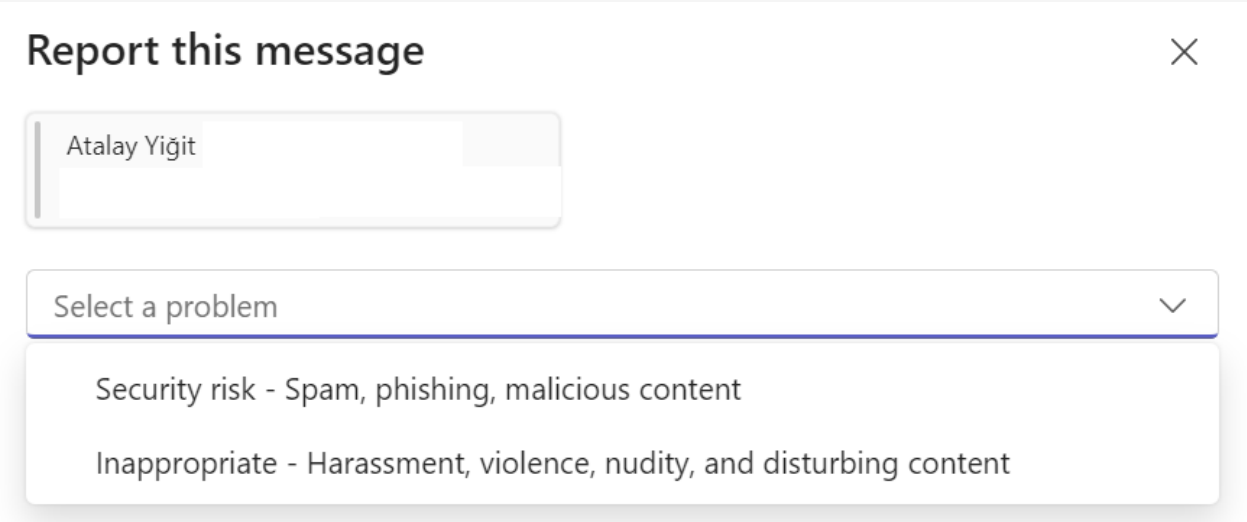
Default olarak açık olacak şekilde yapılandırılmıştır. Kontrol etmek için aşağıdaki adımları izleyebilirsiniz;

admin.teams.microsoft.com/ > Messaging > Messaging Policies



Ayarlar sağlandıktan sonra, sizlere teams üzerinden gönderilmiş her hangi bir iletiye sağ tıklayarak aşağıdaki şekilde report edebilirsiniz.





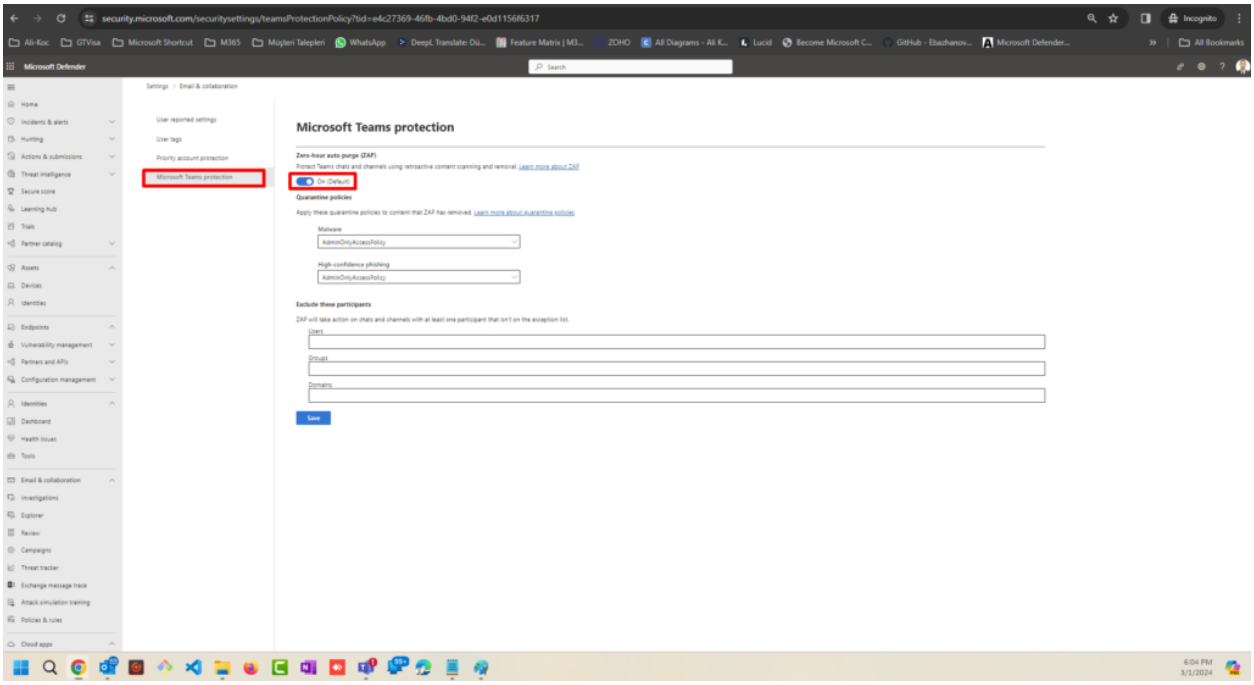
Teams için ZAP (Zero-Hour Auto Purge)

Teams, kötü amaçlı dosyaların/içeriklerin hızla yayılması için elverişli bir kanaldır. Daha hızlı çözümlenebilmesi için ZAP kullanılabilir. Bu özellik, iletileri teslim edildikten sonra analiz eder ve kötü amaçlı dosya veya içerik içeren iletileri otomatik olarak karantinaya alır. Geçmişe dönükte bir tarama yapmaktadır bu sayede geçmişte gerçekleşen eylemleri de saptayabilir

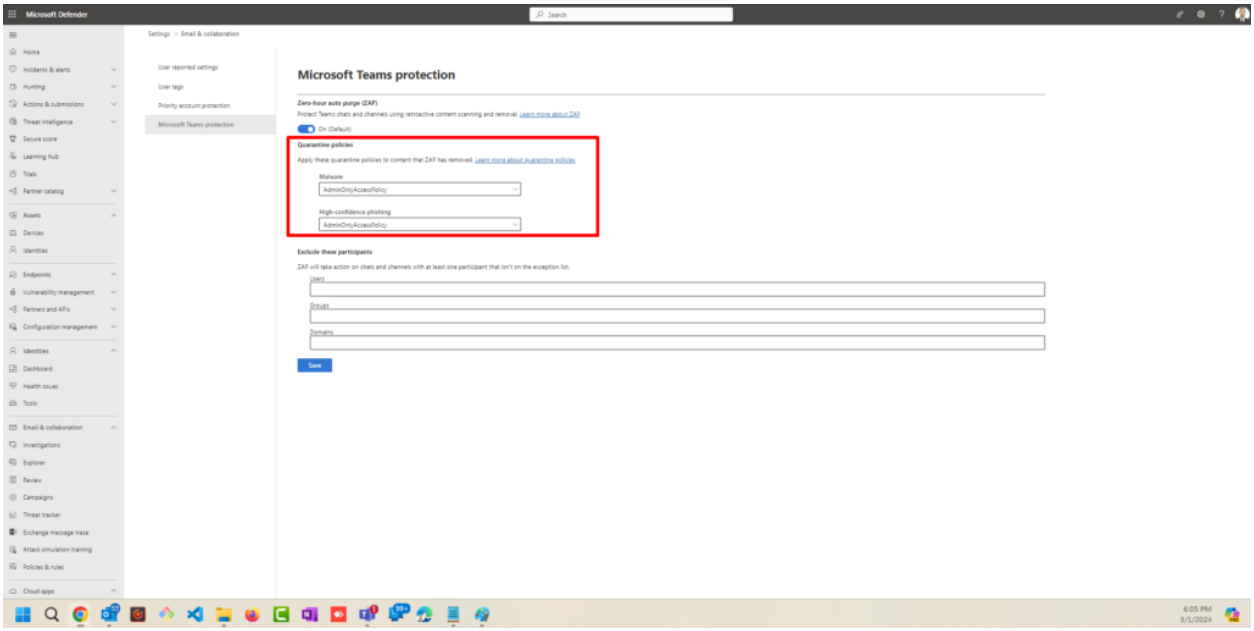
Teams aracılığıyla gönderilen mesajlar ZAP'a dayalı olarak karantinaya alınmakta. Bu, yöneticilerin karantina yoluyla yüksek güvenliğe sahip kimlik avını kontrol etmesine olanak tanımaktadır. Bu tarz eylem sağlanırsa mu mesajların engellenmesi öngörülmektedir.

Teams Message Entity Panel ile, tüm metadataların SecOps amaçları doğrultusunda depolandığı yeni bir alana sahip oluyoruz. Son olarak Microsoft Defender for Office 365 Plan 2 özelliklerinden olan Saldırı Simulasyonu artık Teams aracılığıyla da Sosyal Mühendislik testlerini yapmamıza olanak sağlıyor.

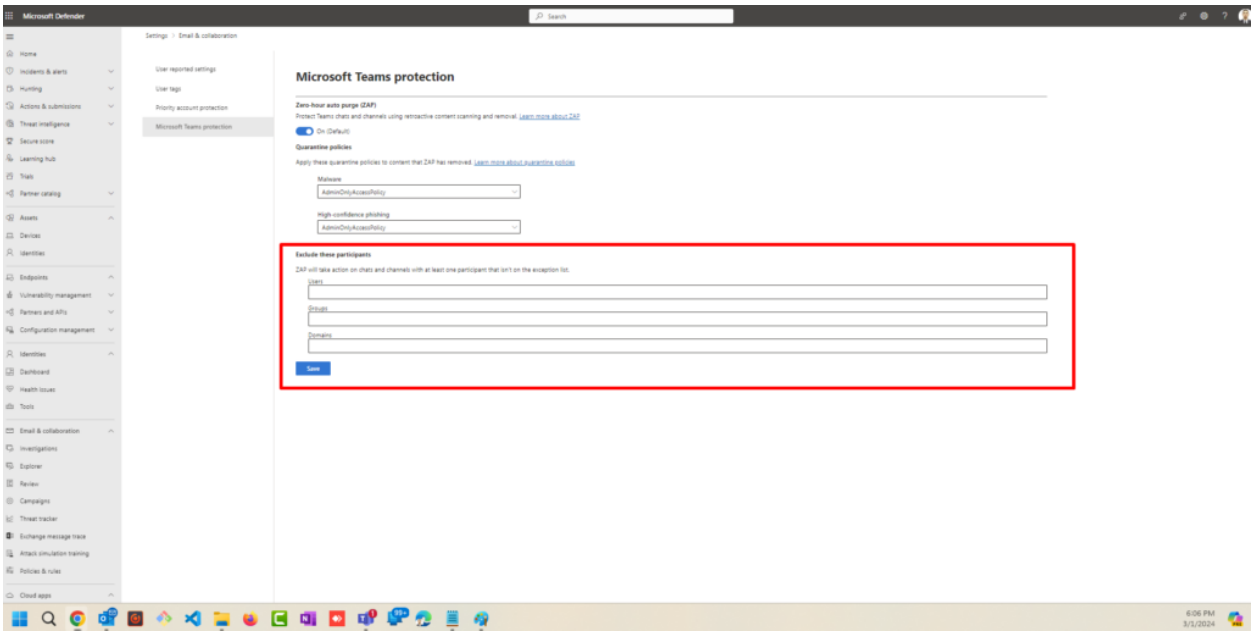
ZAP özelliği Microsoft 365 E5 ve Plan 2 kullanıcılar için kullanılabilir durumda. Yapılandırmak için aşağıdaki adımları izleyebilirsiniz.



Karantina politikalarını belirleyebilirsiniz



Exclude etmek istediğiniz Userlar , Grouplar veya Domain'leri belirleyebilirsiniz;

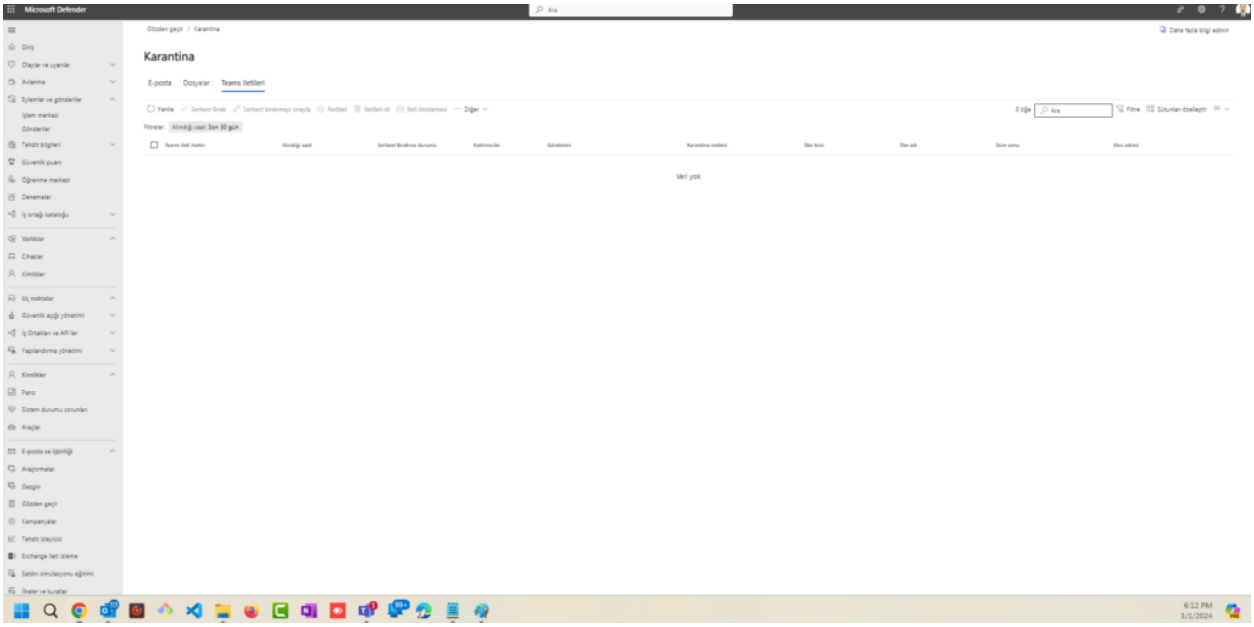


ZAP koruması Teams için varsayılan olarak açıktır.

ZAP, Teams sohbetlerindeki yalnızca iç iletiler için kullanılabilir. Şu anda external mesajlar Microsoft Teams'deki ZAP özelliği tarafından desteklenmemektedir.

Teams mesajları gruplarda birden fazla kişiye ulaştığı için , olası ZAP inceleme durumunda , mesaj sohbetteki herkes için engellenmektedir.

Karantinaya alınan mesajları >E-mail & Collabration > Review >Quarantine sekmesinden görüntüleyebilir, izin verebilir veya silebilirsiniz.



Bir sonraki blog yazısında Microsoft Teams DLP hakkında yapılacak olan çalışmaları içeriyor olacaktır.

Bilgilendirme kaynakları: learn.microsoft.com/ , jeffreyappel.nl