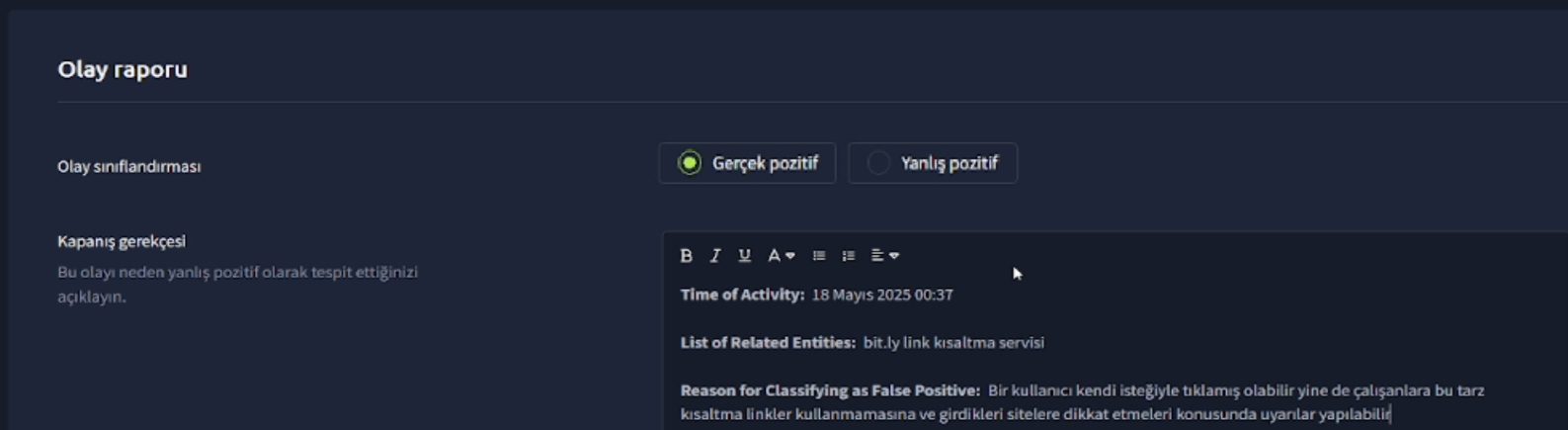
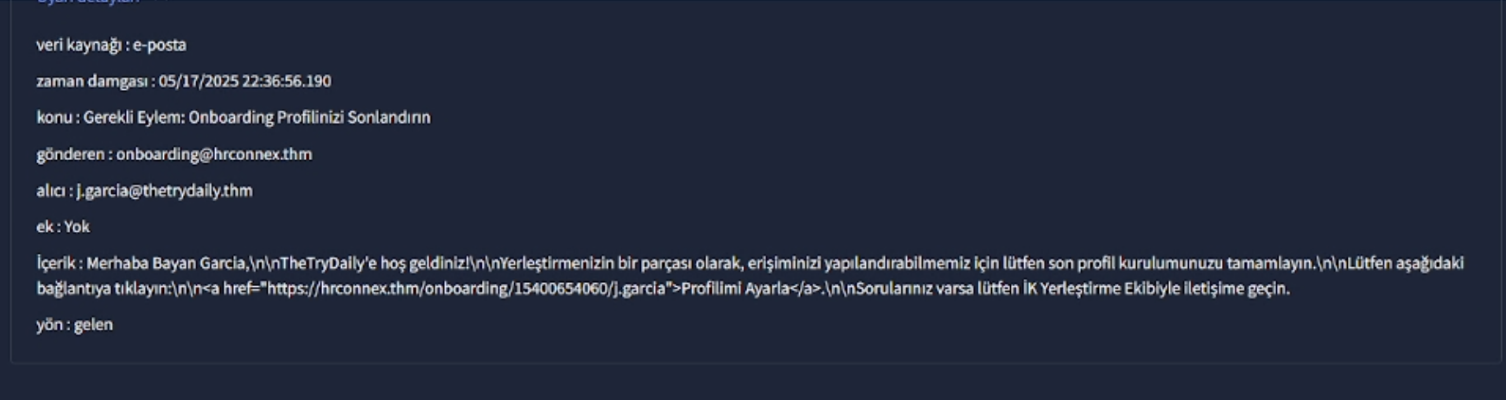
SOC SIMULATION

1.  İlk başta phising mailleri ile ilgili bir alert aldım tam incelerken bir alert daha aldım şirketimizdeki bir kullanıcı bit.ly uzantılı bir kısaltma linke tıkladığı hakkında daha sonra bu biraz daha riskli olduğu için ilk olarak linke tıklama uyarısını ele aldım.

 Daha sonra ipleri incelediğimde gerçekten kısaltma link url sağlayıcısı olan bit.ly ye ait olduğunu gördüm fakat yine de zararlı bir siteye yönlendirme ihtimali de bulunduğundan ötürü tp olarak değerlendirip vaka raporumu oluşturdum.

 Daha sonra ise phising maillerini ele aldım ve baktım ki herkese aynı firmadan benzer şekilde e postalar gönderilerek bit.ly uzantılı maillere tıklamaları için ikna yöntemi kullanarak phising denemesi yapıldığını fark ettim ve bu 4 mail alertini de tp olarak değerlendirip ticketi kapattım. Başka alert düşmedi

