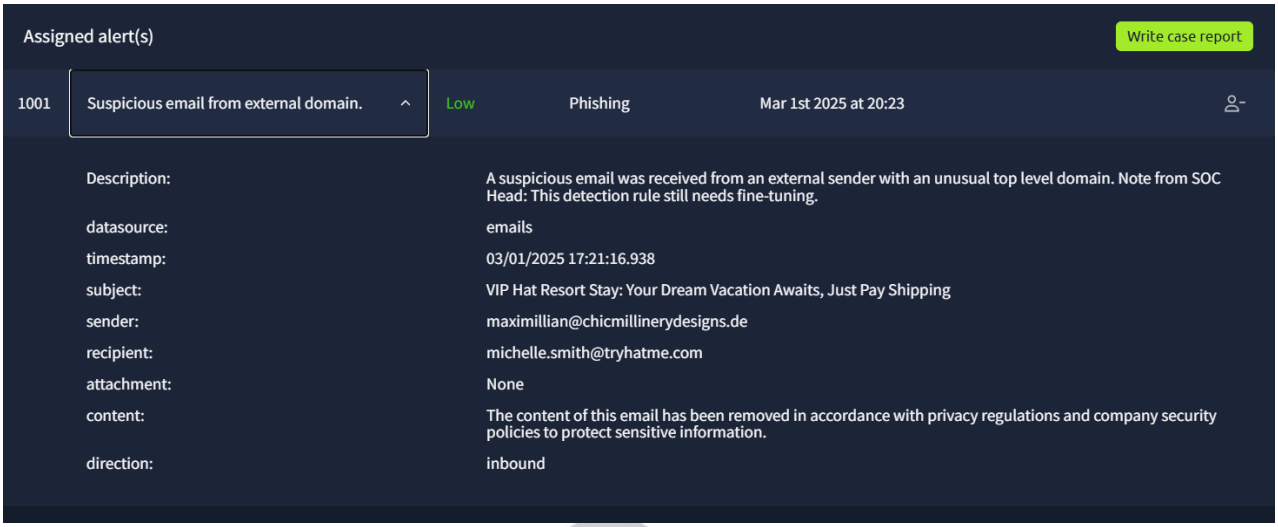
INTRO TO PHISHING

Hazırlayan

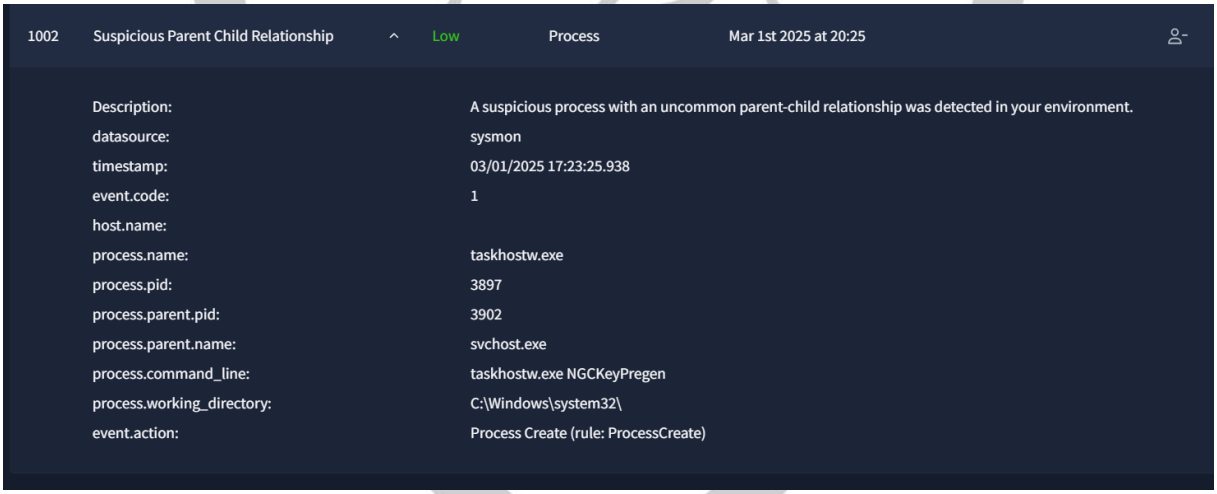
Adı: Ayşe

Soyadı: BALCI

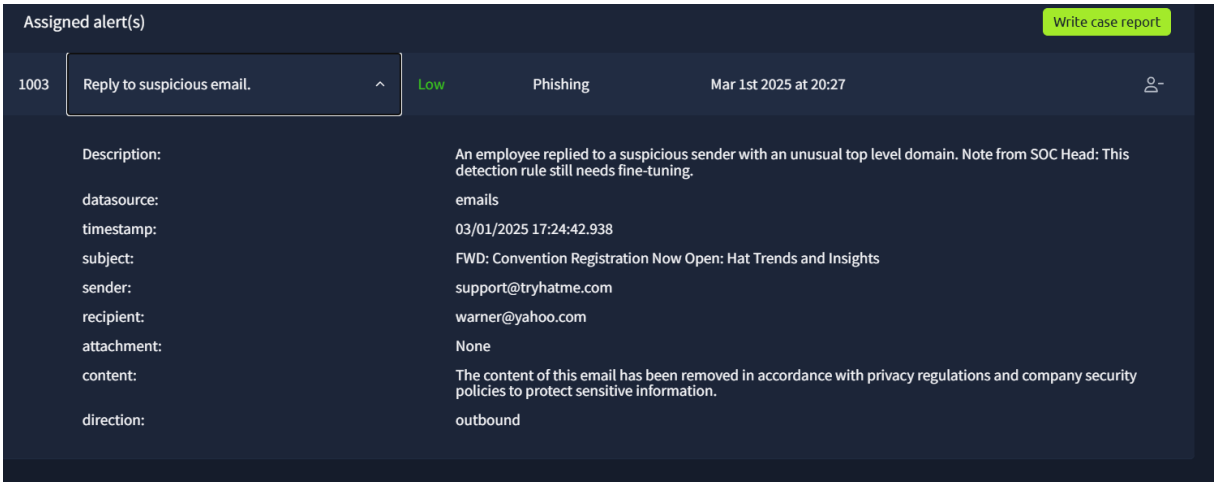
Tarih: 01/03/2025



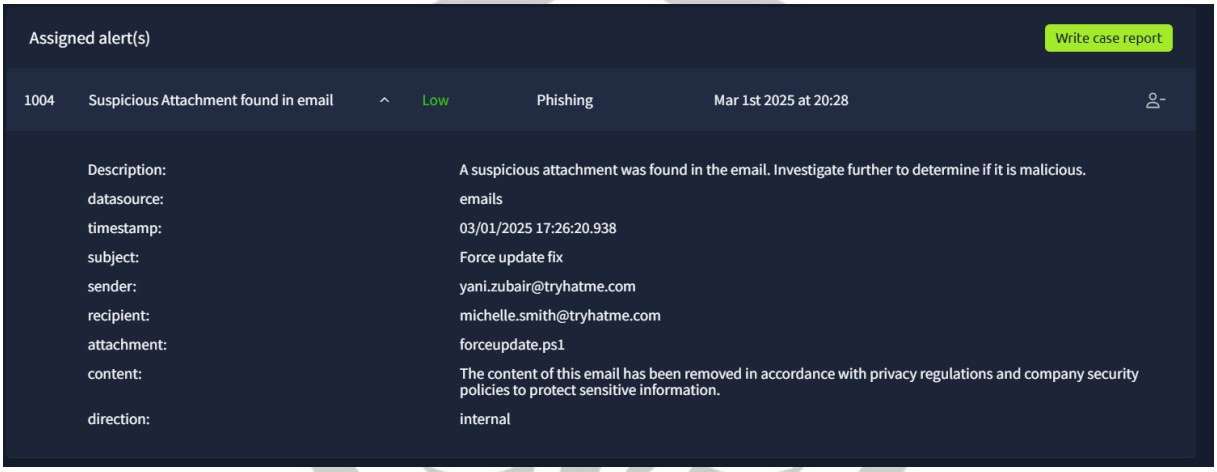
Göndericinin domaini ve ip adresi virustotal, abuseipdb gibi sitelerde aratıldıktan sonra herhangi bir şüpheli durumla karşılaşılmadı bu yüzden bu Alert False Positive.



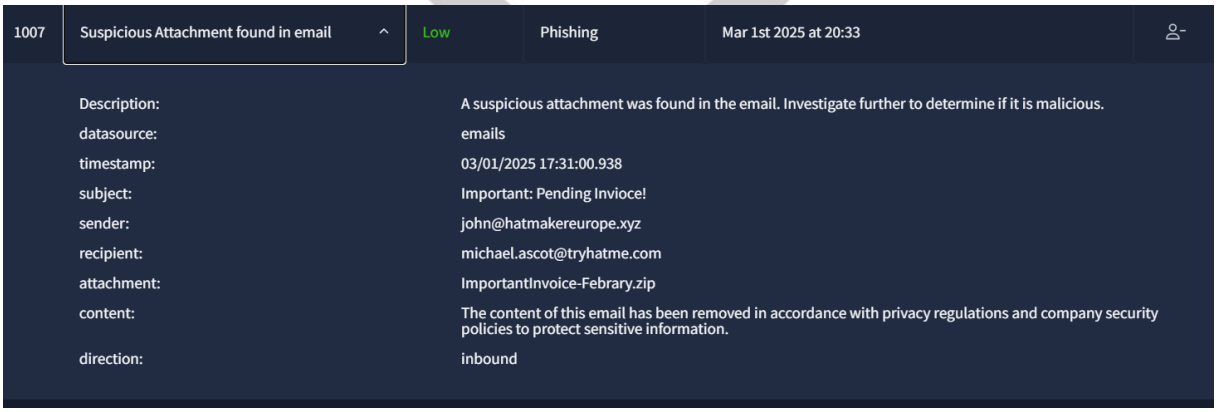
taskhostw.exe, Windows'un görev yöneticisi olup genellikle DLL tabanlı görevleri çalıştırır. svchost.exe, sistem hizmetlerini yöneten bir süreçtir ve bazı durumlarda taskhostw.exe'nin ebeveyni olabilir. NGCKeyPregen, Windows Hello ve TPM ile ilgili bir bileşen olup, şifreleme anahtarlarını yönetmek için çağrılabilir. Eğer Windows Hello aktifse, bu işlem normaldir. Ayrıca çalışma klasörü normal olduğu için alarm false pozitifdir.



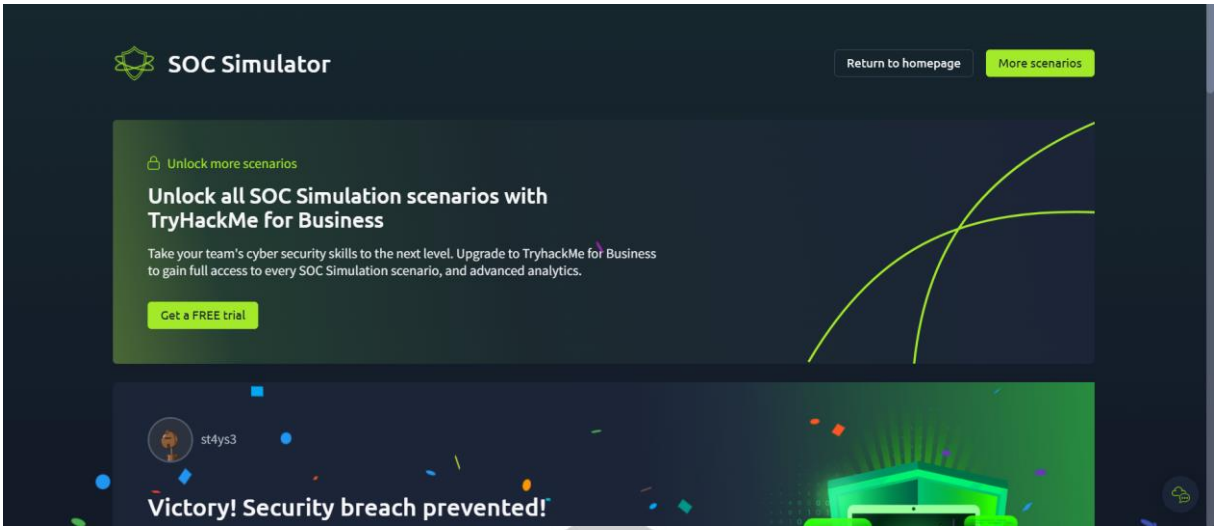
Documentation kısmında şirket mailleri vardır ve sender maili şirketten gelen bir mail adresi olduğu için alarm false pozitifdir.



Analyst VM kısmında forceupdate.ps1 dosyasının içeriği incelendi şüpheli bir durum görülmedi ayrıca sender maili şirketin IT yetkilisine atanmış bir mail olduğu için alarm false poziitifdir.



Domain virustotal üzerinde kontrol edildiğine şüpheli olarak göründü ayrıca analyst vm makinesinde attachments klasöründe zip dosyası bulundu içeriği çıkarıldığında ise bir lnk dosyası olarak görünüyor fakat uzantısı .pdf bu yüzden bu alarm true pozitifidir.



Alarmlar kapatıldıktan sonra ilk senaryo bitmiş oluyor ve simülatör bu ekrana gitmiş oluyor.