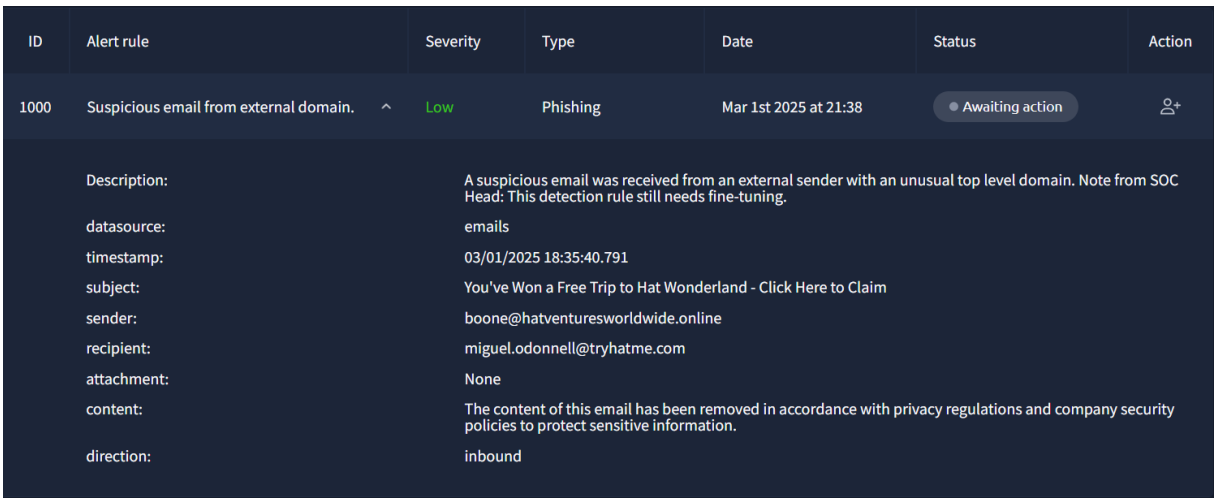
TryHackMe SOC Simulator Introduction to Phishing

Hasan Karaca

01.03.2025

İçindekiler

1- Alert 1000

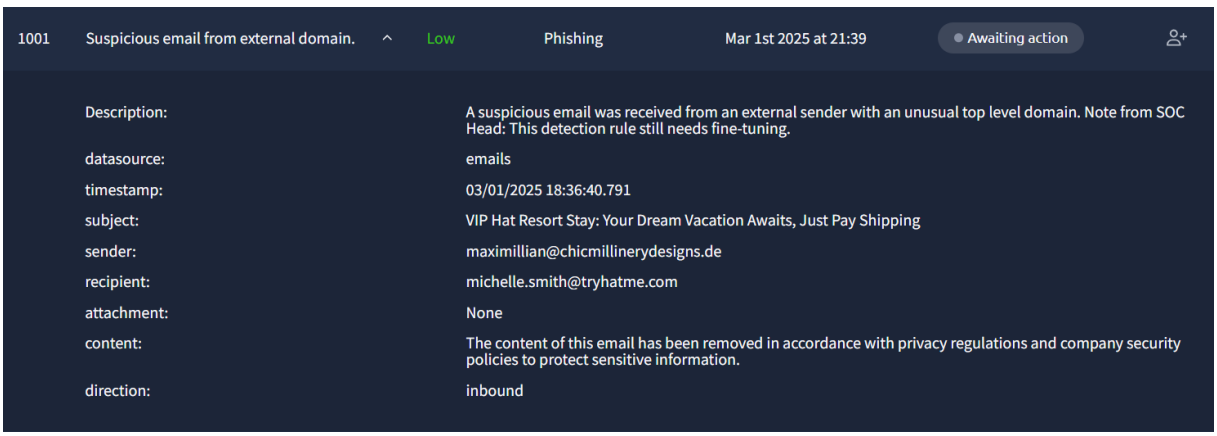


ID	Alert rule	Severity	Type	Date	Status	Action
1000	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 21:38	Awaiting action	

Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:	emails
timestamp:	03/01/2025 18:35:40.791
subject:	You've Won a Free Trip to Hat Wonderland - Click Here to Claim
sender:	boone@hatventuresworldwide.online
recipient:	miguel.odonnell@tryhatme.com
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	inbound

Phising üzerine bir alert düşüyor alaerti incelediğimde gönderen kişinin domaini viriüstotalde incelediğimde şüpheli olarak gözükmüyor mail içerisinde de herhangi bir dosya yok alert **false positive**.

2- Alert 1001

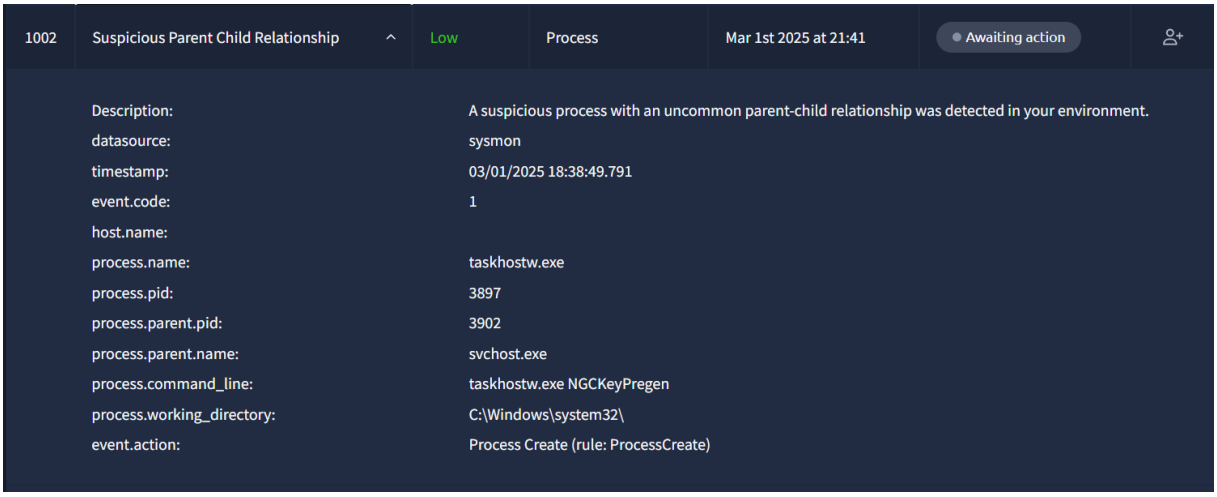


1001	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 21:39	Awaiting action	

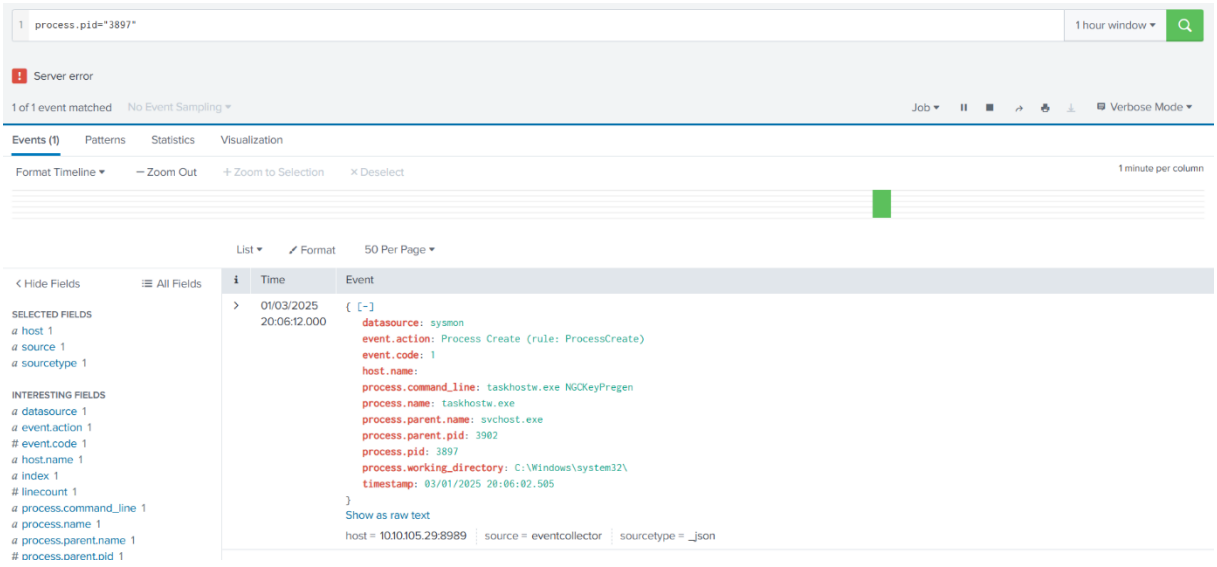
Description:	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
datasource:	emails
timestamp:	03/01/2025 18:36:40.791
subject:	VIP Hat Resort Stay: Your Dream Vacation Awaits, Just Pay Shipping
sender:	maximillian@chicmillinerydesigns.de
recipient:	michelle.smith@tryhatme.com
attachment:	None
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	inbound

Alert üzerinde ki gönderen mailin domaini virüstotalde araştırdığımda şüpheli olarak gözükmüyor mail içerisinde herhangi bir dosya yok **false positive**.

3- Alert 1002

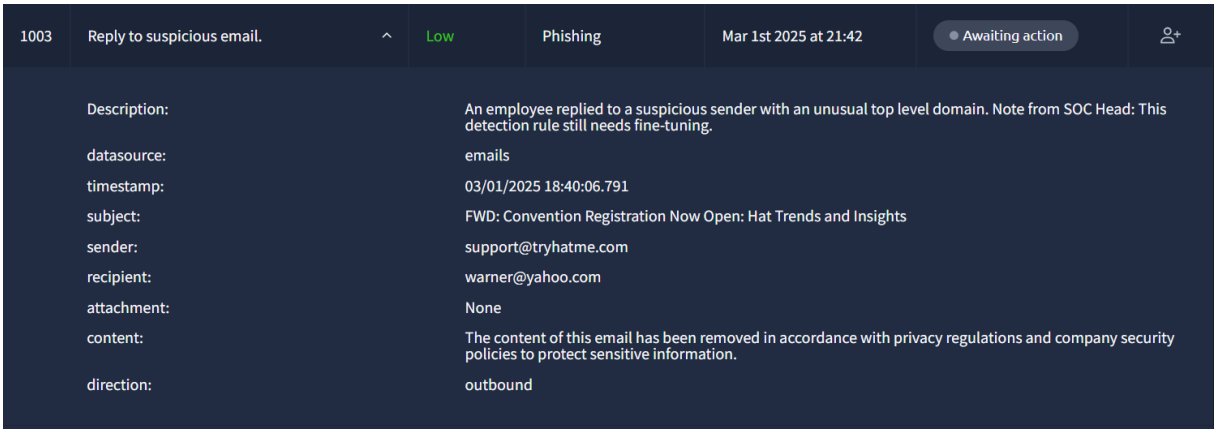


Sysmon taradfından gelen alert açıklaması alışılmadık bir ilişki şeklinde bir alert tetiklenmişlertir bu alerti splunkta aratıyorum.



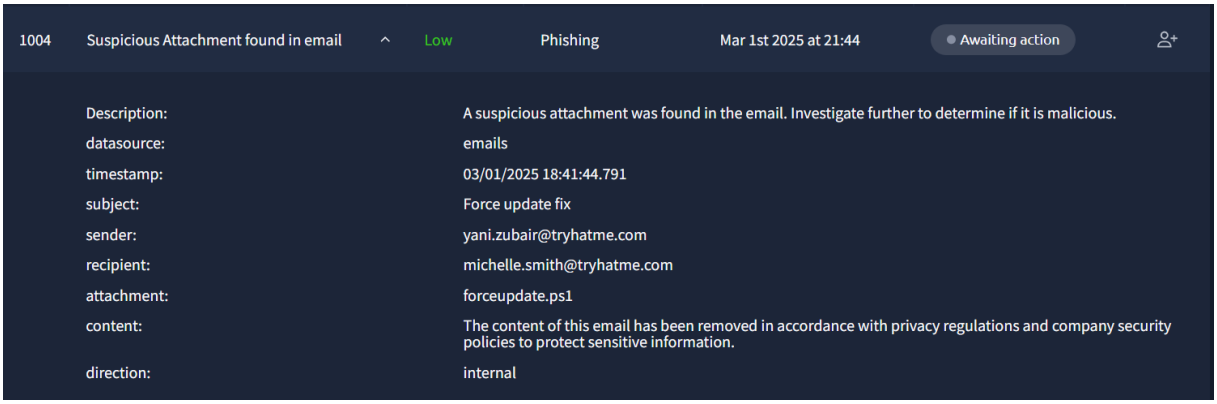
Alert içerisindeki process.pid değerini aratıyorum karşıma bir tane log düşüyor bu log da herhangi bir şüpheli bir ilişki görünmüyor taskhostw.exe zaralı herhangi bir işlem başlatmıyor bu yüzden **false positive.**

4- Alert 1003

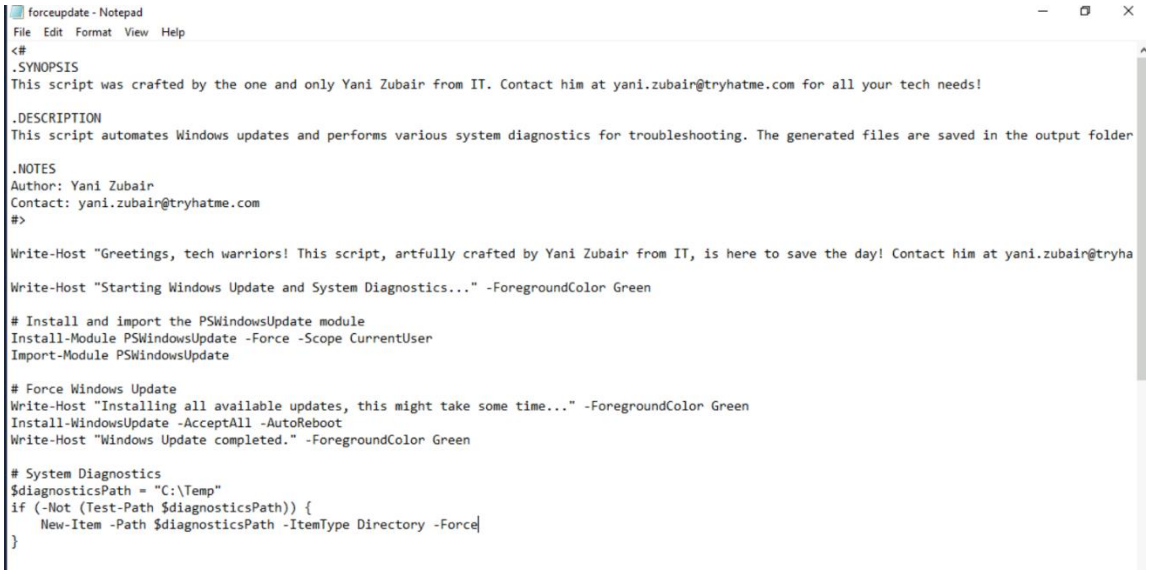


Şirketin suppotu Yahoo.com a mail atmış gönderilen dosya bulunmuyor herhang bir şüpe yok bu yüzden **false positive**

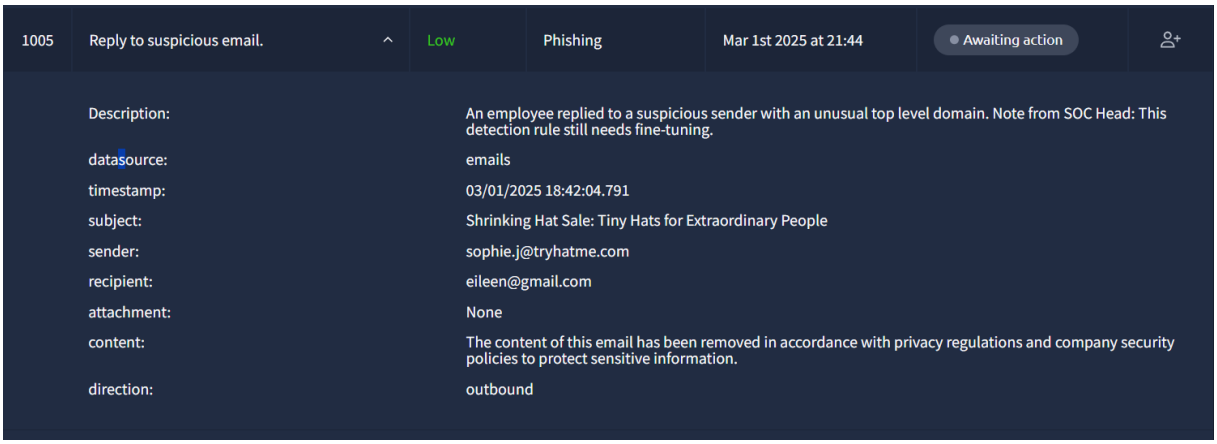
5- Alert 1004



IT ekibindeki Yani Zubair, Michelle Smith adlı çalışına forceupdate.ps1 adlı powershell scripti göndermiştir scripti wm de incelediğimide herhangi bir zaralı içerik bulunmamaktadır dosyanın içeriği Windows Güncellemelerini Yükleme, Yüklü Programları Toplama, Çalışan Süreçleri Toplama vs sistme takibi için kullanılan bir scripttir. Scriptte herhangi bir zaralı kod bulunmamaktadır bu yüzden **false positive**.

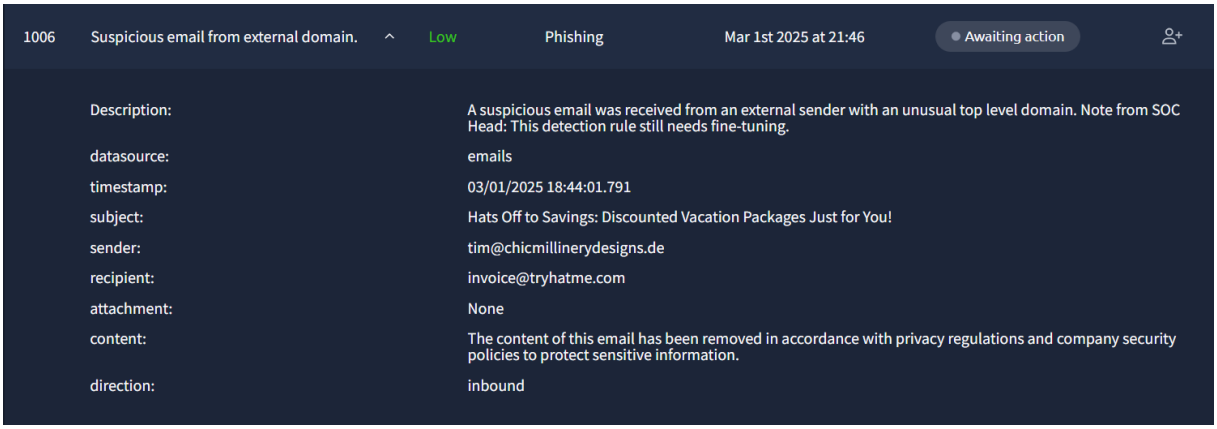


6- Alert 1005



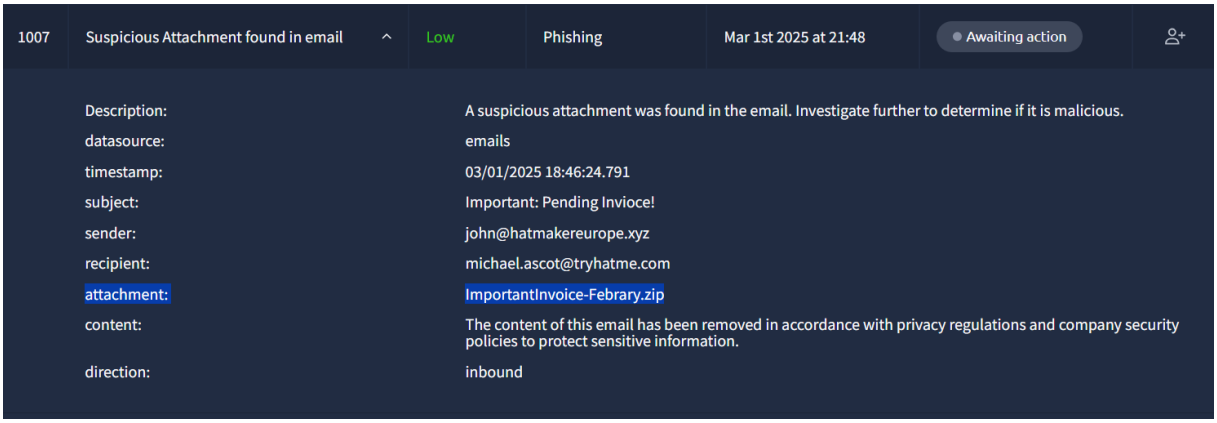
Sophie J HR çalışanı eileen@gmail.com mail adresine mail yollamıştır herhangi bir dosya yok şüpheli bir faliyet tespit edilmedi bu yüzden **false positive**

7- Alert 1006

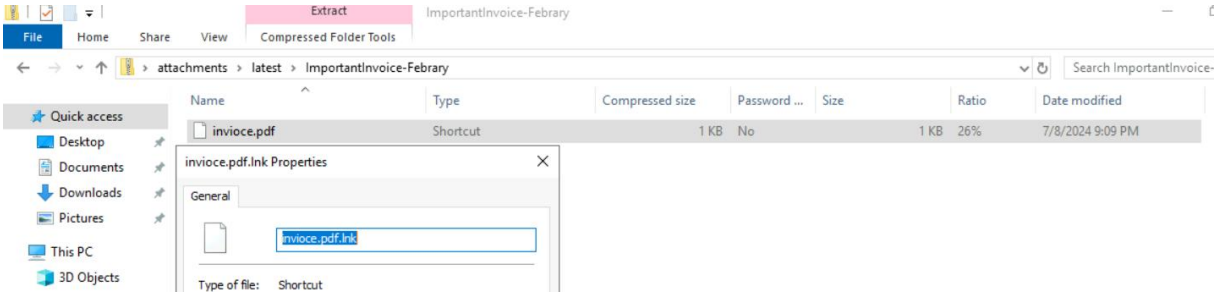


Alerti incelediğimde gönderen kişinin domaini virüstotalde arattığımda şüpheli olarak gözükmüyor mail içerisinde de herhangi bir dosya yok alert **false positive.**

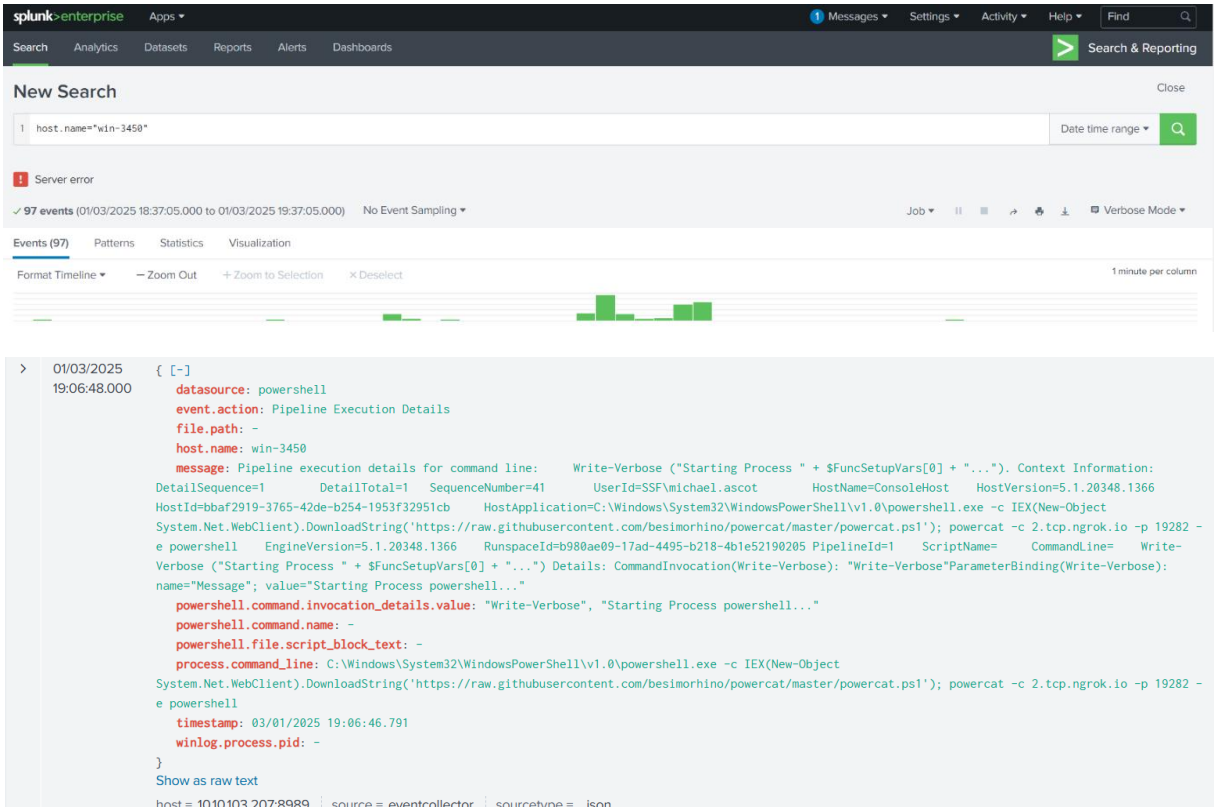
8- Alert 1007



Alertte gönderilen dosyayı vm de görüntülediğimde zipin içeirisnde .pdf uzantılı görülücek şekilde gizlenmiş .lnk uzantılı Windows kısayol dosyası bulunuyor.



Maili alan kullanıcının giriş yaptığı cihazın id sini Documentation altında ki Company Information kısmında öğreniyorum ve splunk üzerinde aratıyorum.



Bu adımdan sonra alertin tetiklendiği saatten sonra logları inceliyorum ve powershell üzerinden githubtan powercat.ps1 adında bir powershell scripti indirdiriyor bu script powershell tabanlı bir netcat aracıdır. Bu komut 19282 portu üzerinden reverse Shell bağlantısı oluşturuyor. Bu alert **true positive**