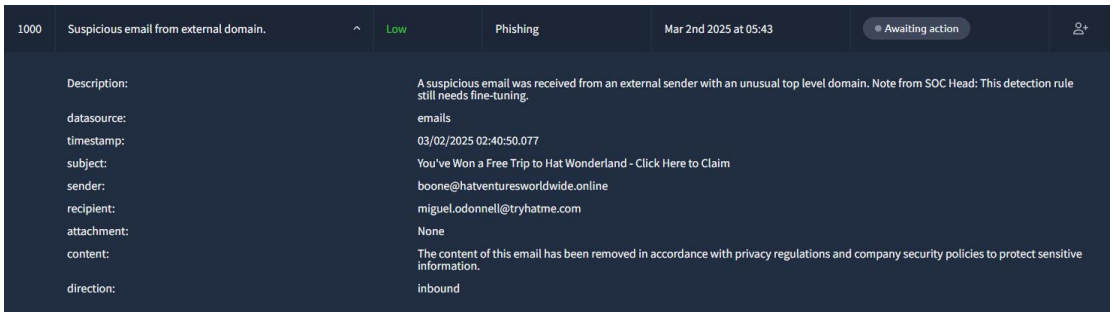
ALTAY TAKIMI

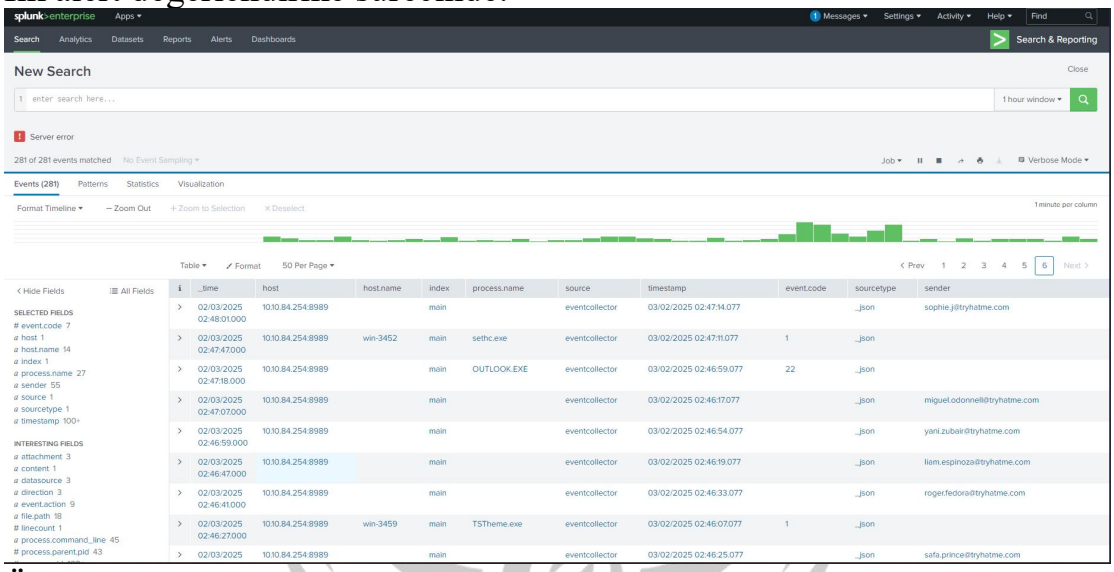
TRYHACKME SOC SIMULATOR

Gürkan Parlak
01.03.2025

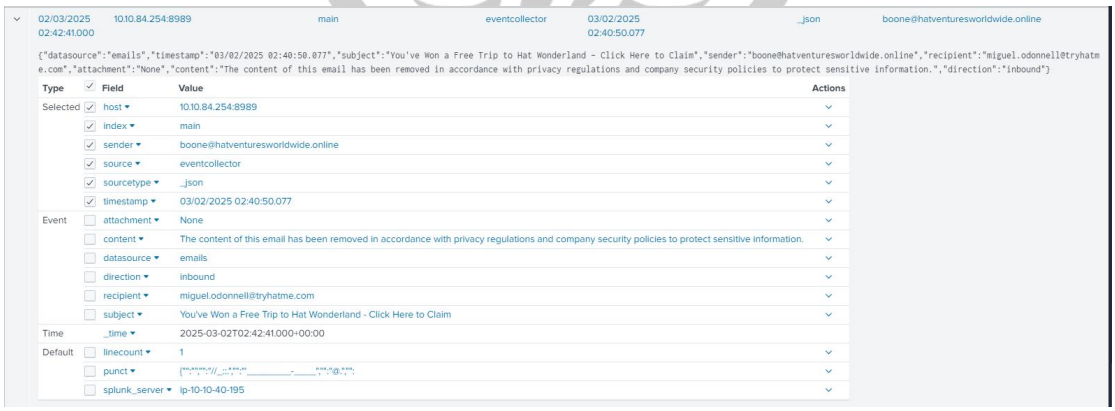
1-Alert



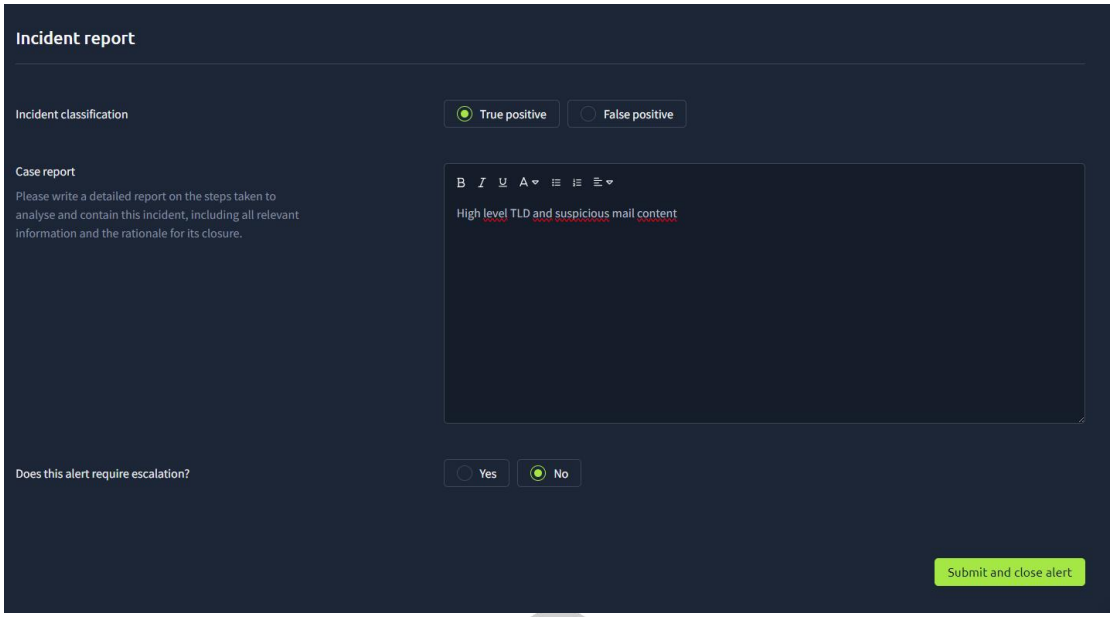
Ilk alert degerlendirme sürecinde:



Önce SIEM arayüzünü kendi filtrelemesi ile tekrar düzenledim.

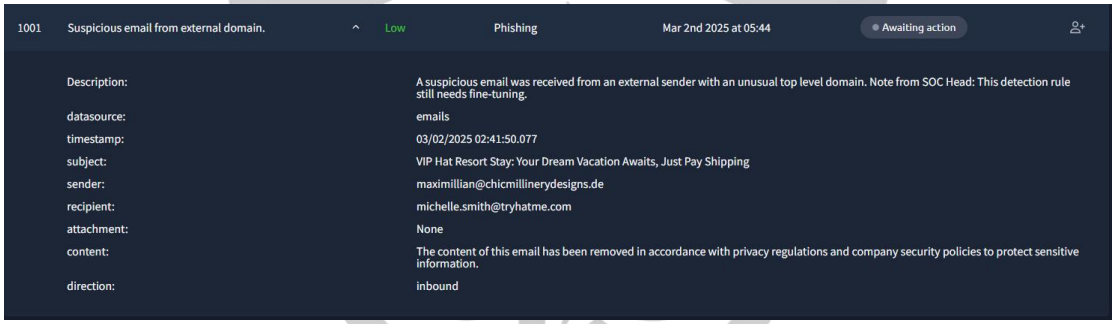


Daha sonra ilgili alertin log kaydini incelemeye aldım
Yüksek seviye bir TLD sahip olduğuna dair bir not bulunmakta. Bu sebeple phising olduğunu düşündüm ve true positive olarak değerlendirdim.

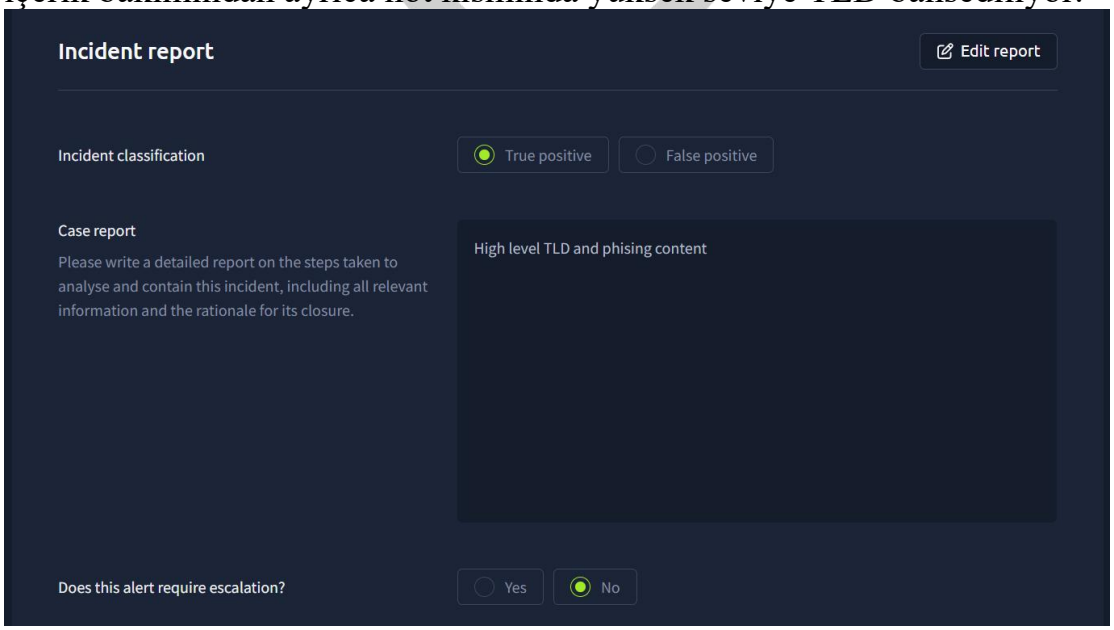


Bu şekilde bir raporlama yaptım.

2-Alert

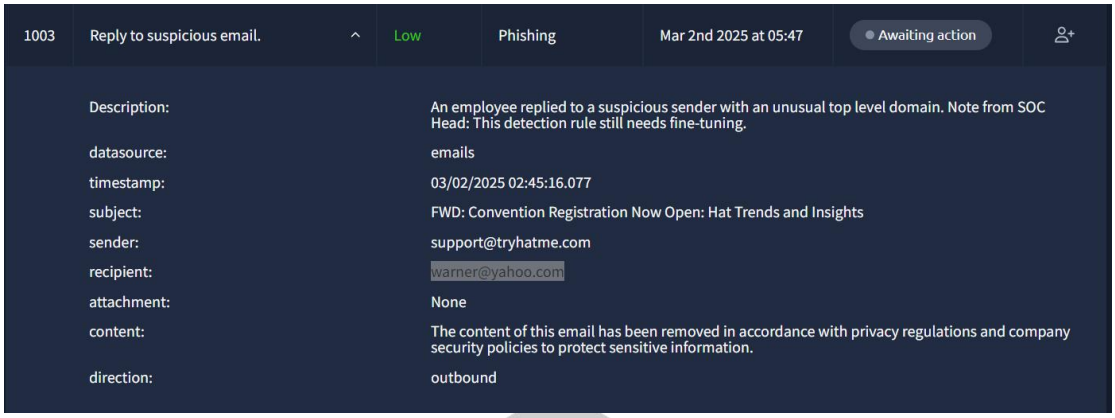


Burada da phising olduğu bariz bir şekilde belli. Mail adresinden ve içerik bakımından ayrıca not kısmında yüksek seviye TLD bahsediliyor.

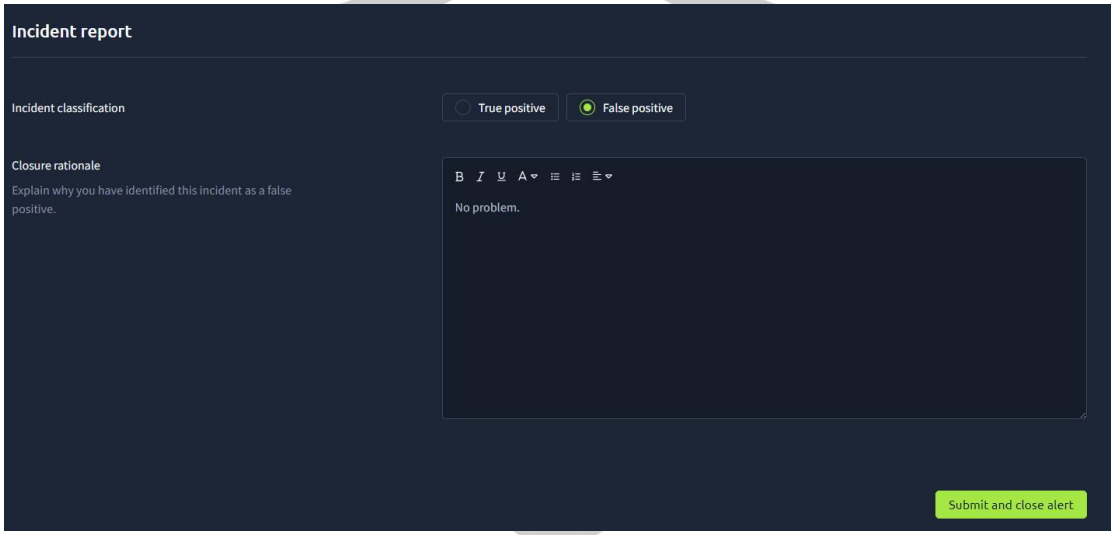


Bu şekilde raporlama yaptım

3-Alert

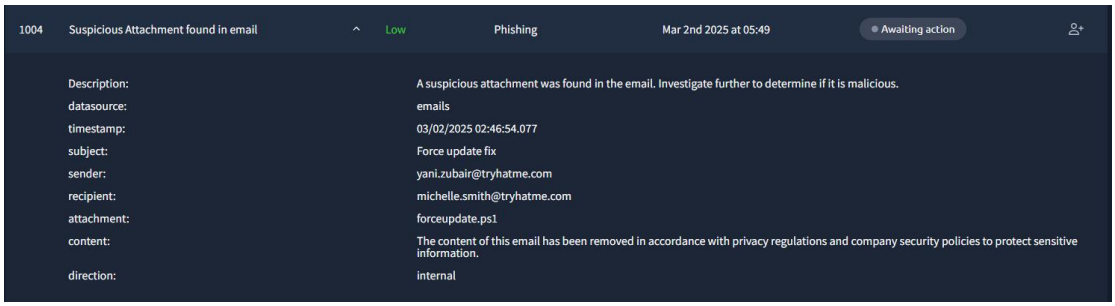


Burada herhangi önemli bir durum gözükmüyor.

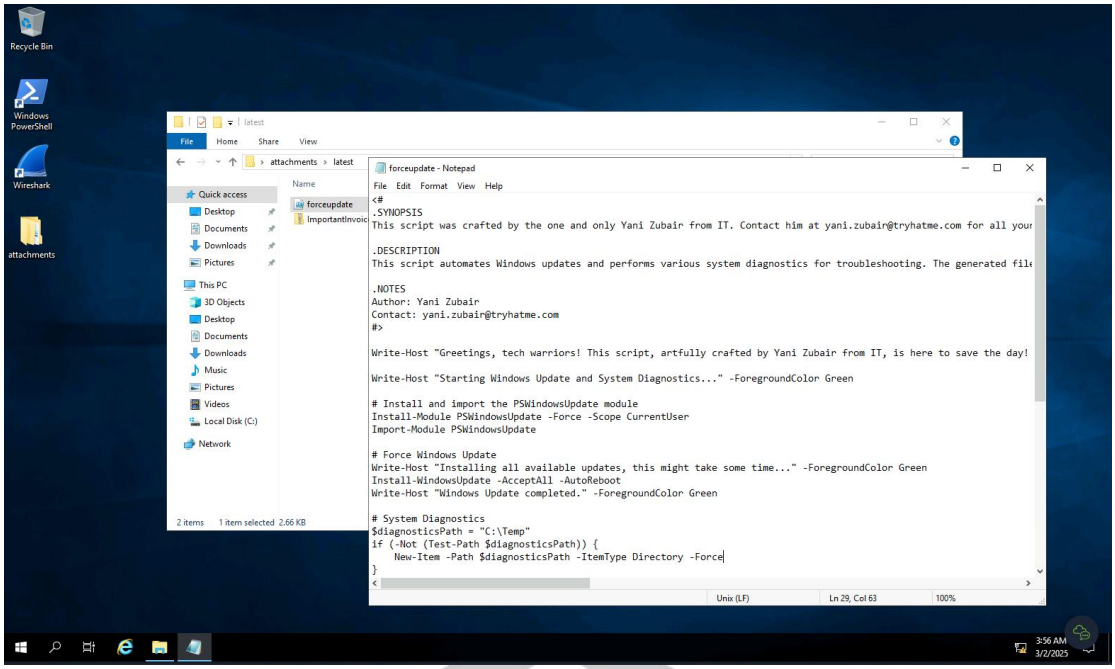


Bu şekilde raporlama yaptım.

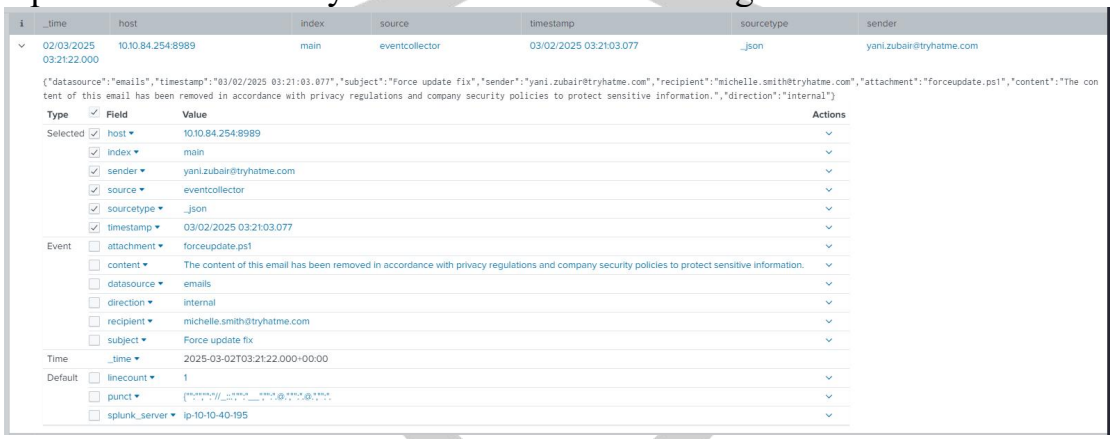
4-Alert



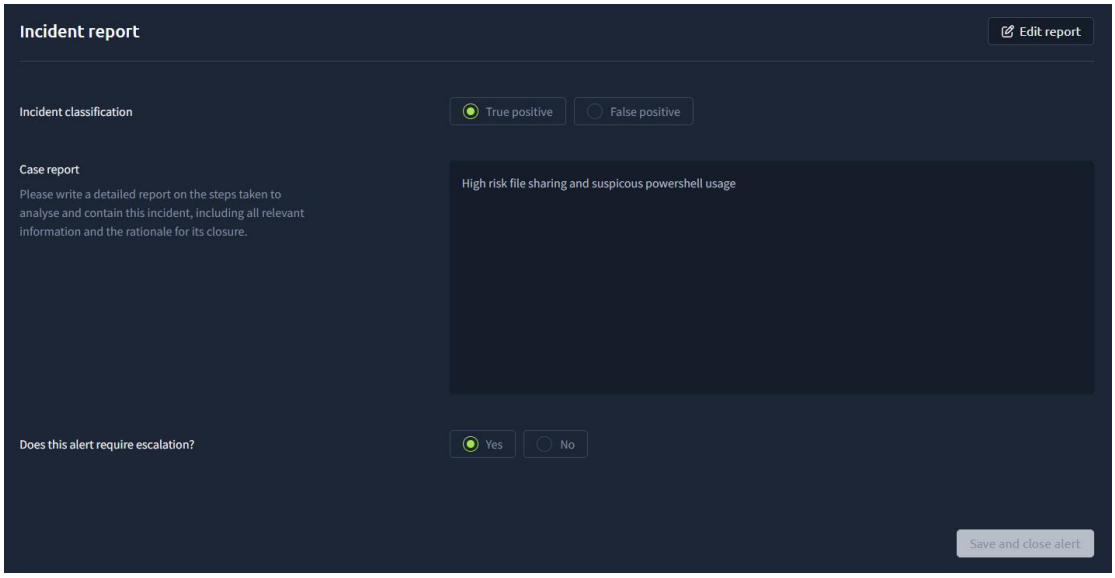
Burada true positive olarak değerlendirdim. Ancak false positive durumu varmış.



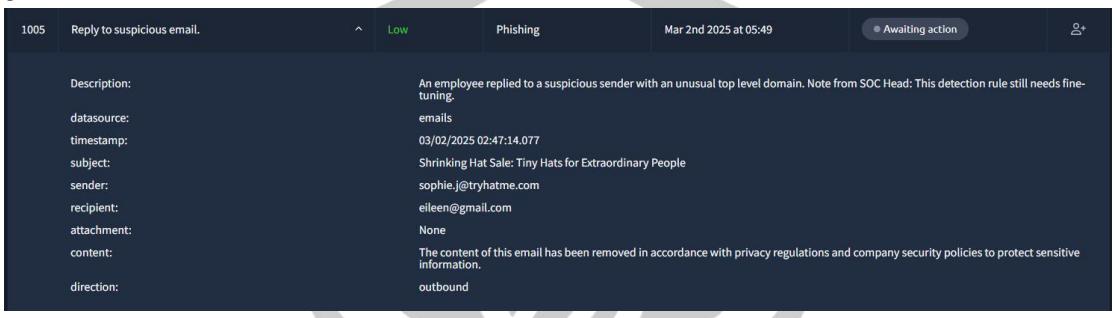
Update ile alakalı bir yetkisi kullanım durumları gözlemledim.



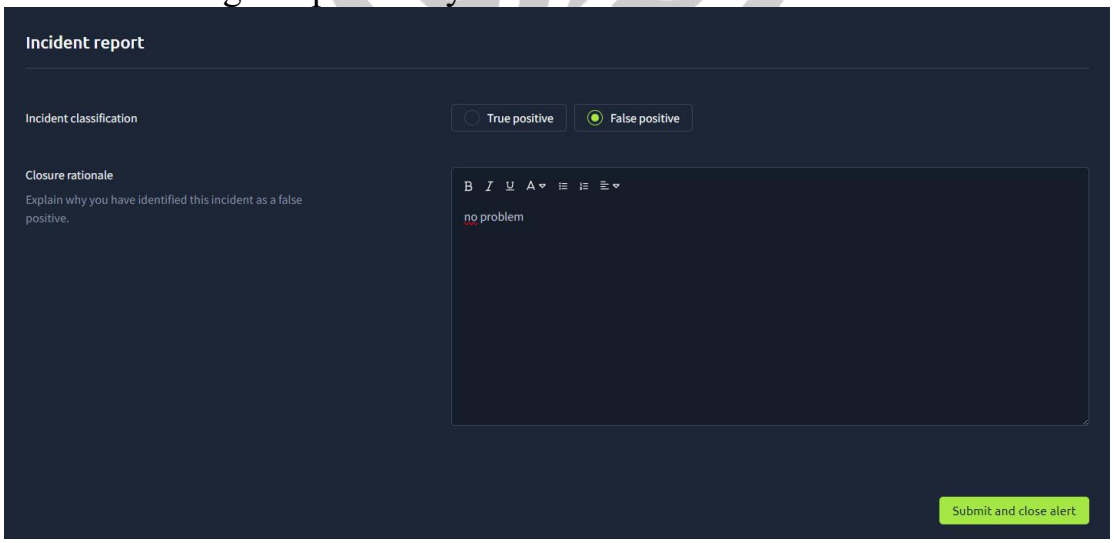
Modül Güvenliği: Install-Module PSWindowsUpdate -Force komutu, üçüncü taraf bir modülü otomatik olarak indirip yüklüyor. Eğer modül güvenilir bir kaynaktan alınmamışsa, kötü amaçlı kod içerebilir.



5-Alert

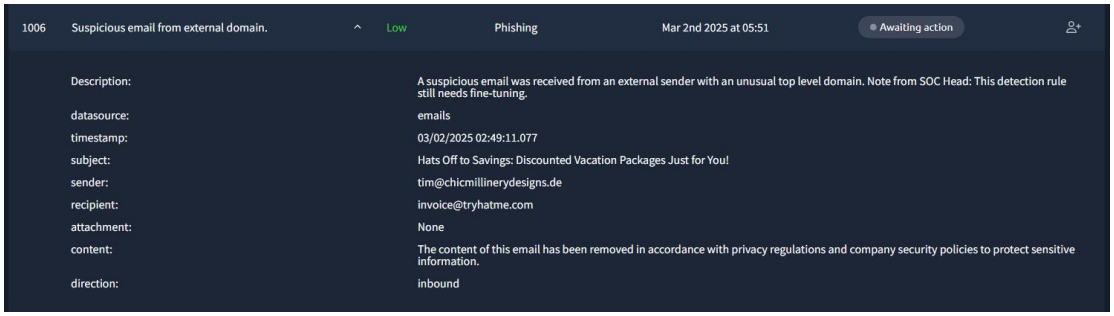


Burada herhangi bir problem yoktu.

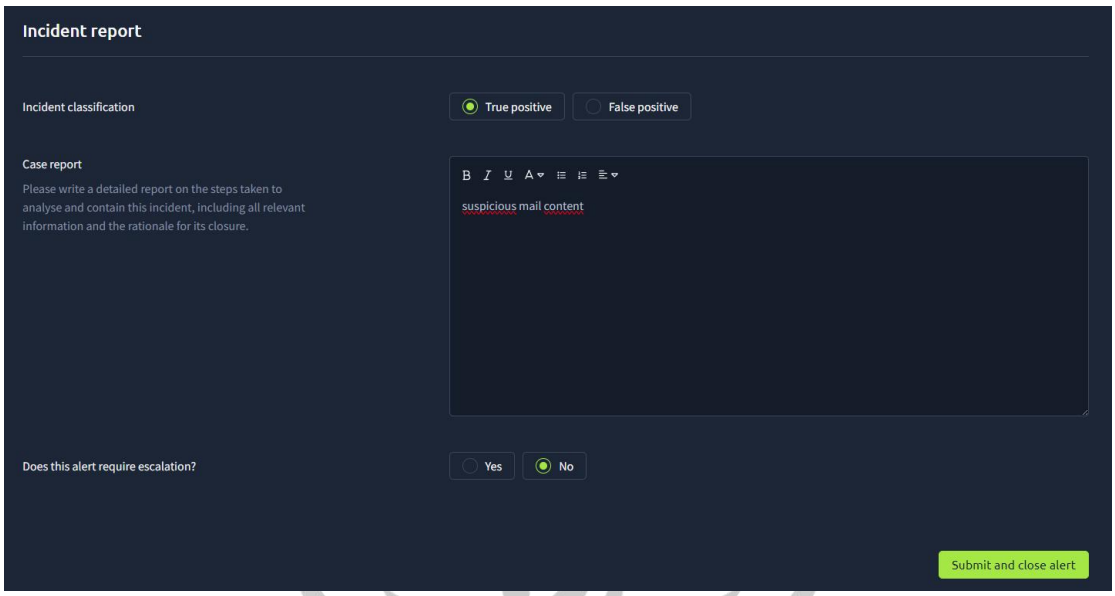


Bu şekilde raporladım.

6-Alert

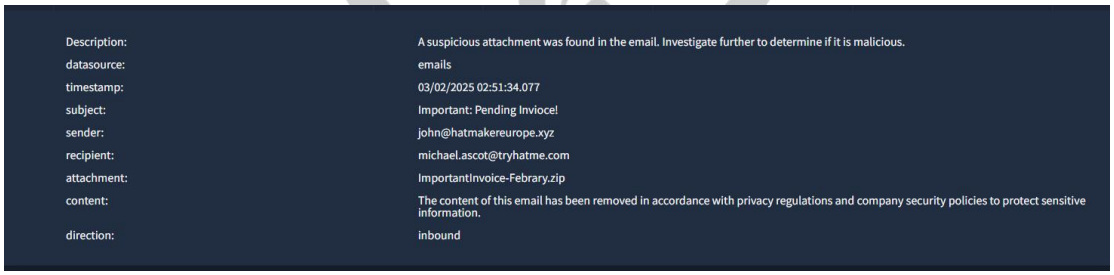


Phising olduğunu düşündüğüm bir gönderici bulunmakta. Phising olabilir.

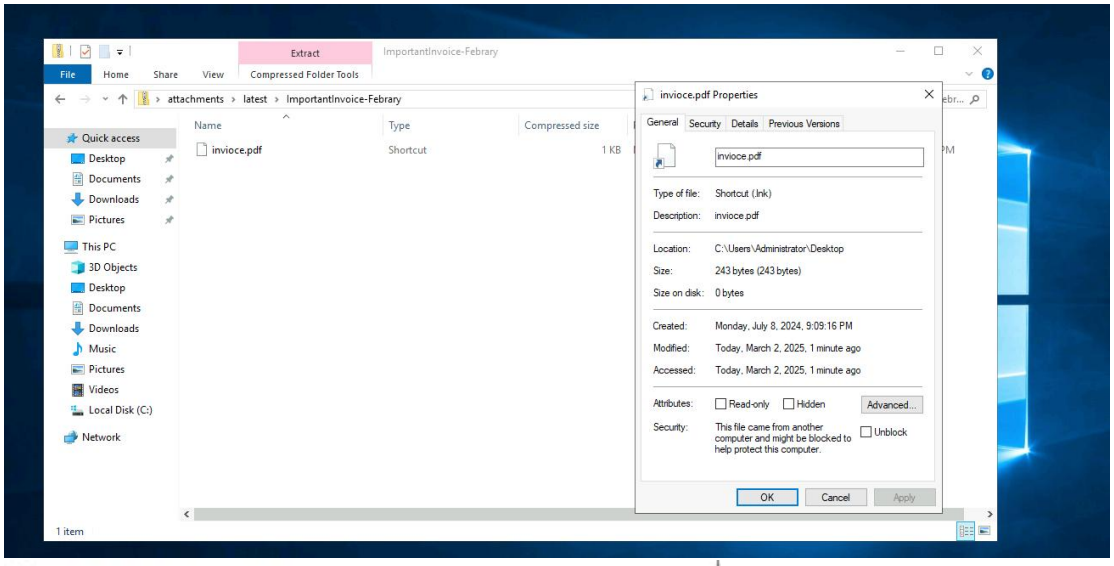


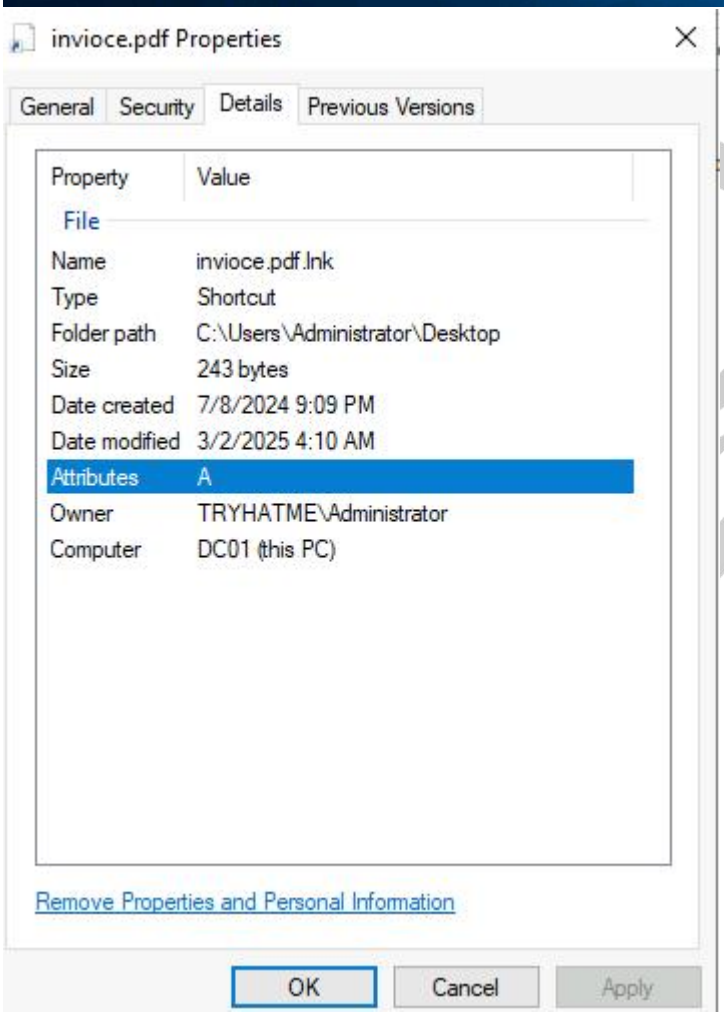
Bu şekilde raporladım.

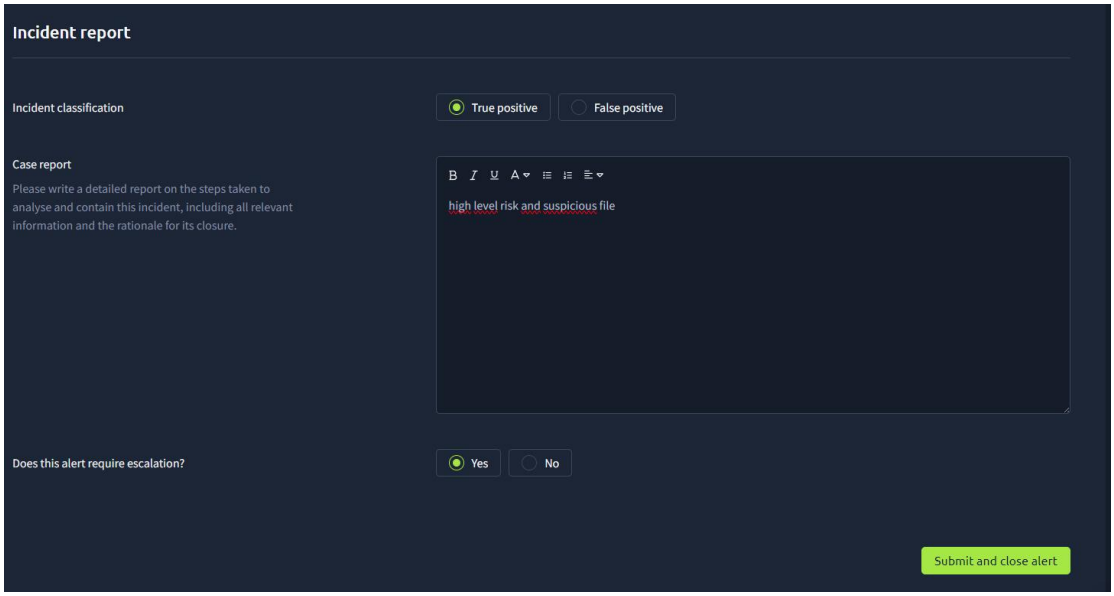
7-Alert



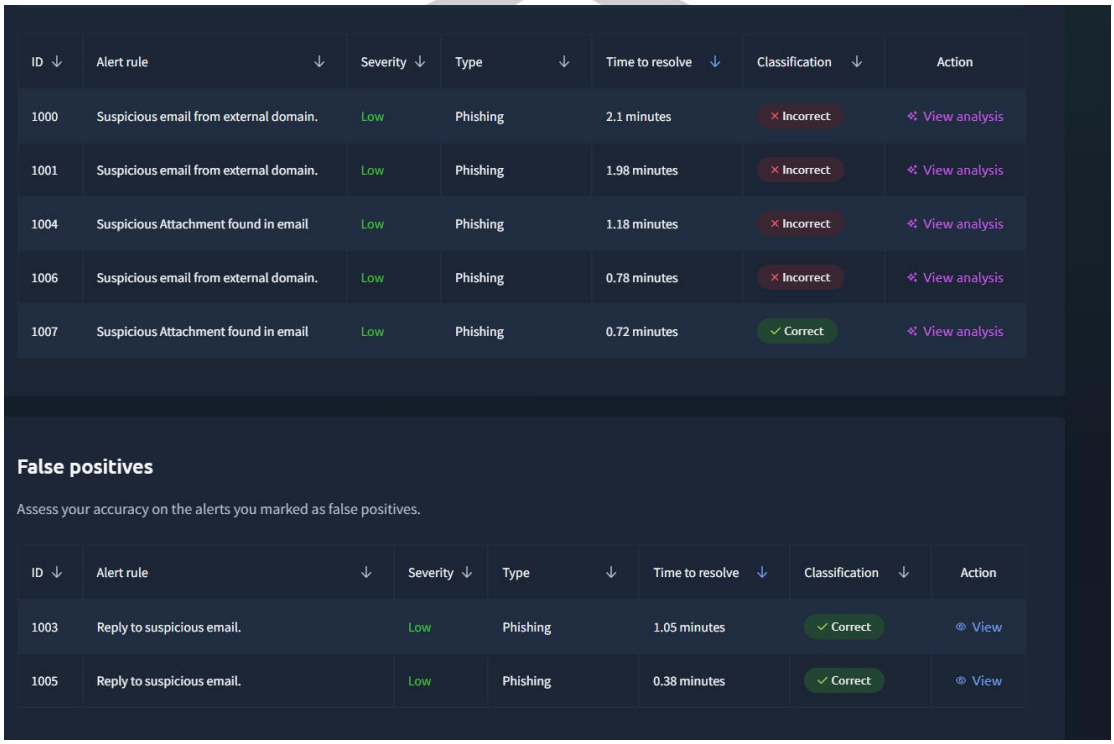
Burada pdf uzantılı gözüken ancak pdf uzantısı olmayan bir dosya gönderilmiş. Son derece şüpheli ve yüksek riskli.


ImportantInvoice-Febrary
Extract
File
Home
Share
View
Compressed Folder Tools
attachments › latest › ImportantInvoice-Febrary
Quick access
Desktop
Documents
Downloads
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Type
Compressed size
invioce.pdf
Shortcut
1 KB
1 item
invioce.pdf Properties
General
Security
Details
Previous Versions
invioce.pdf
Type of file: Shortcut (.lnk)
Description: invioce.pdf
Location: C:\Users\Administrator\Desktop
Size: 243 bytes (243 bytes)
Size on disk: 0 bytes
Created: Monday, July 8, 2024, 9:09:16 PM
Modified: Today, March 2, 2025, 1 minute ago
Accessed: Today, March 2, 2025, 1 minute ago
Attributes: Read-only Hidden Advanced...
Security: This file came from another computer and might be blocked to help protect this computer. Unblock
OK
Cancel
Apply


invioce.pdf Properties
General
Security
Details
Previous Versions
Property
Value
File
Name
invioce.pdf.lnk
Type
Shortcut
Folder path
C:\Users\Administrator\Desktop
Size
243 bytes
Date created
7/8/2024 9:09 PM
Date modified
3/2/2025 4:10 AM
Attributes
A
Owner
TRYHATME\Administrator
Computer
DC01 (this PC)
Remove Properties and Personal Information
OK
Cancel
Apply



Bu şekilde açıklama yaptım.



Sonuç tablosu.