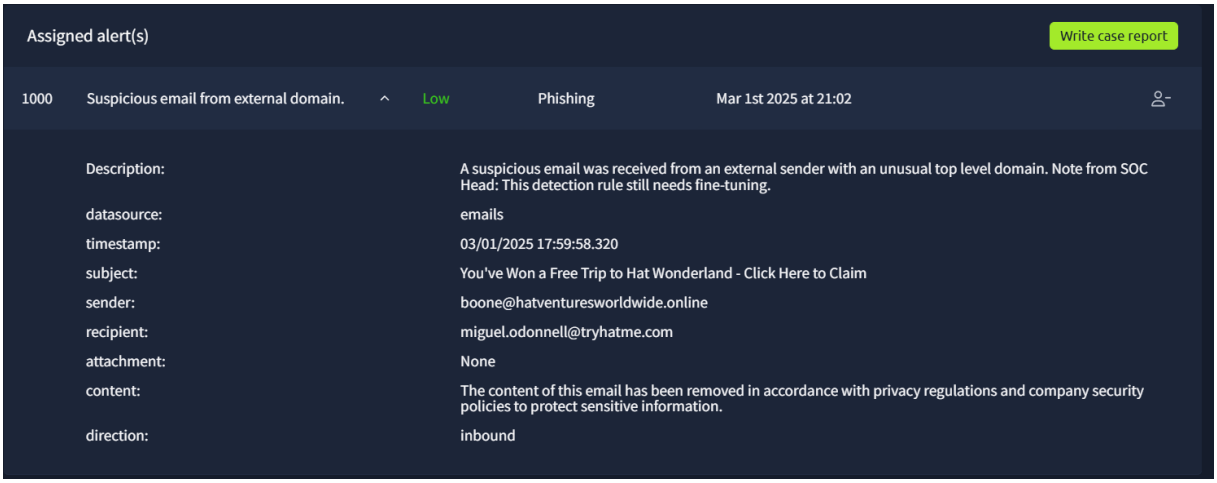
PHISHING UNFOLDING

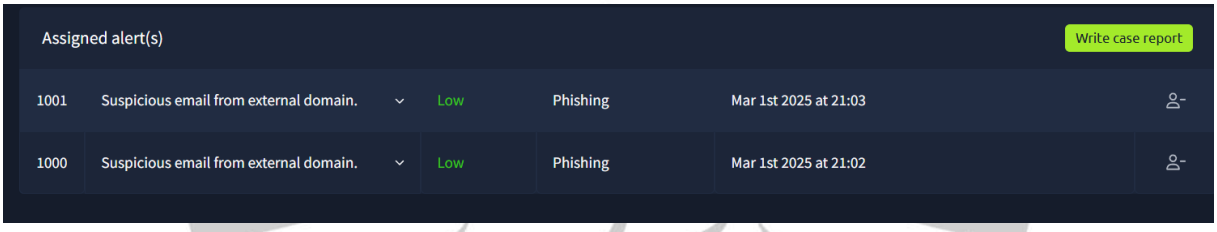
Hazırlayan

Adı: Ayşe

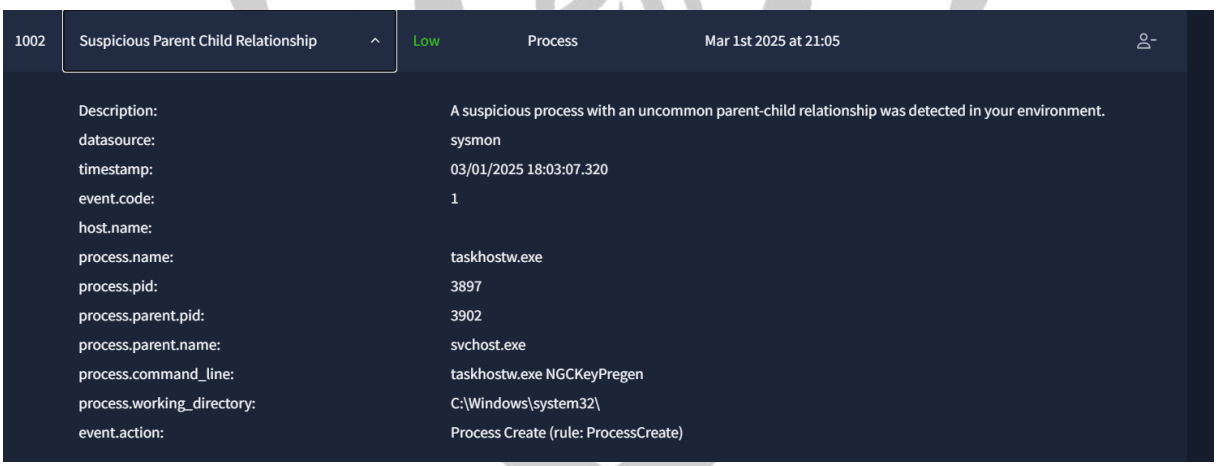
Soyadı: BALCI

Tarih: 01/03/2025

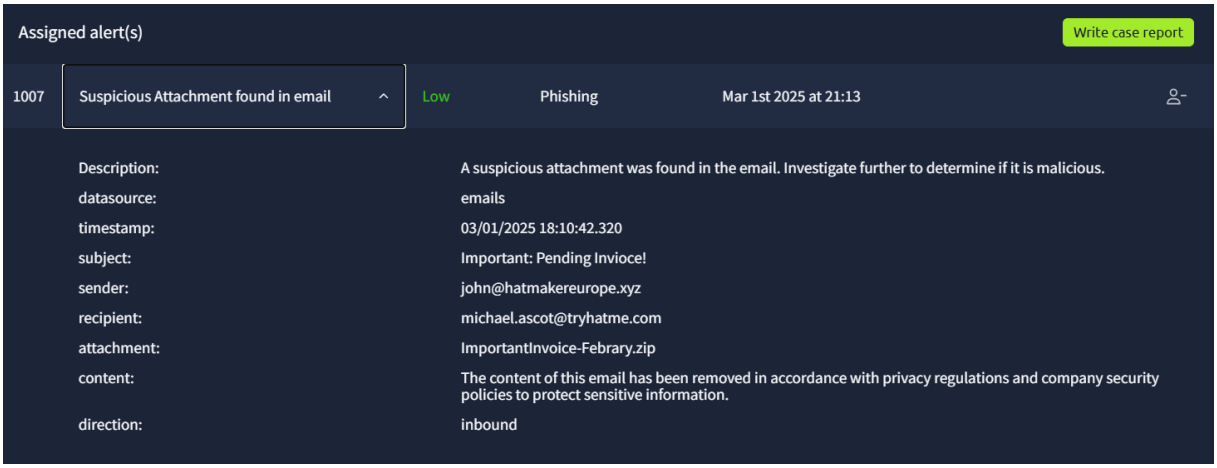


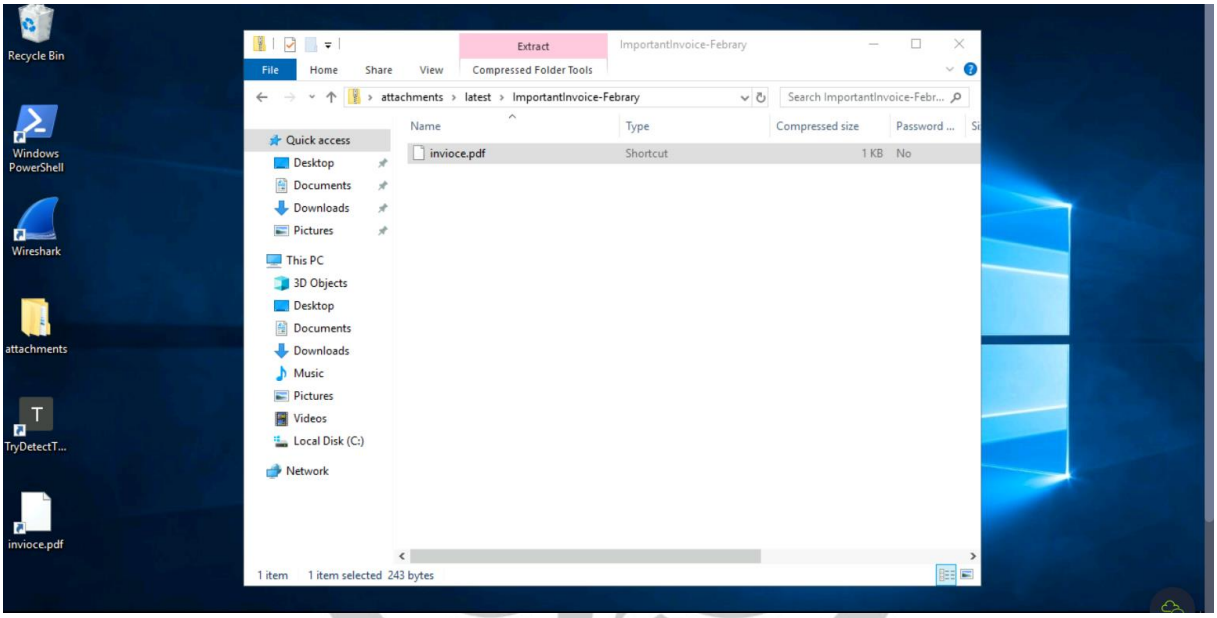


Mail domainleri taratıldığında herhangi bir şüpheli durum görülmmeiştir bu yüzden alarmlar false pozitifdir.

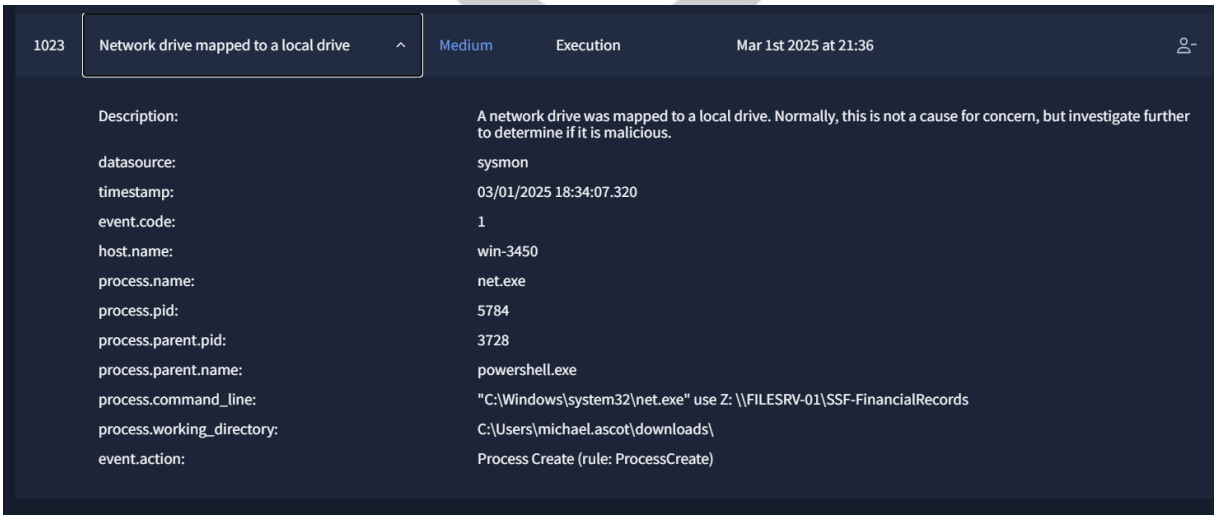


Taskhostw svchost tarafından bazı durumlarda çalıştırılabilir. Ayrıca working directory taskhostw nin default olarak bulunduğu klasördür. Bu yüzden alarm false pozitifdir.



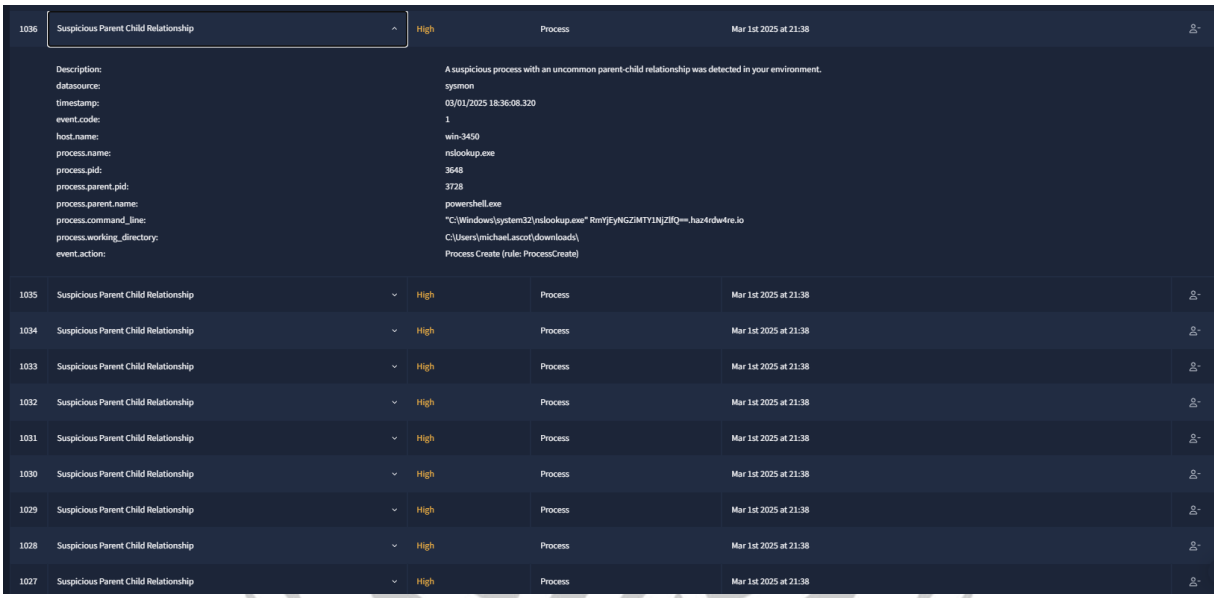


Domain virustotal üzerinde kontrol edildiğine şüpheli olarak göründü ayrıca analyst vm makinesinde attachments klasöründe zip dosyası bulundu içeriği çıkarıldığında ise bir lnk dosyası olarak görünüyor fakat uzantısı .pdf bu yüzden bu alarm true pozitifidir.

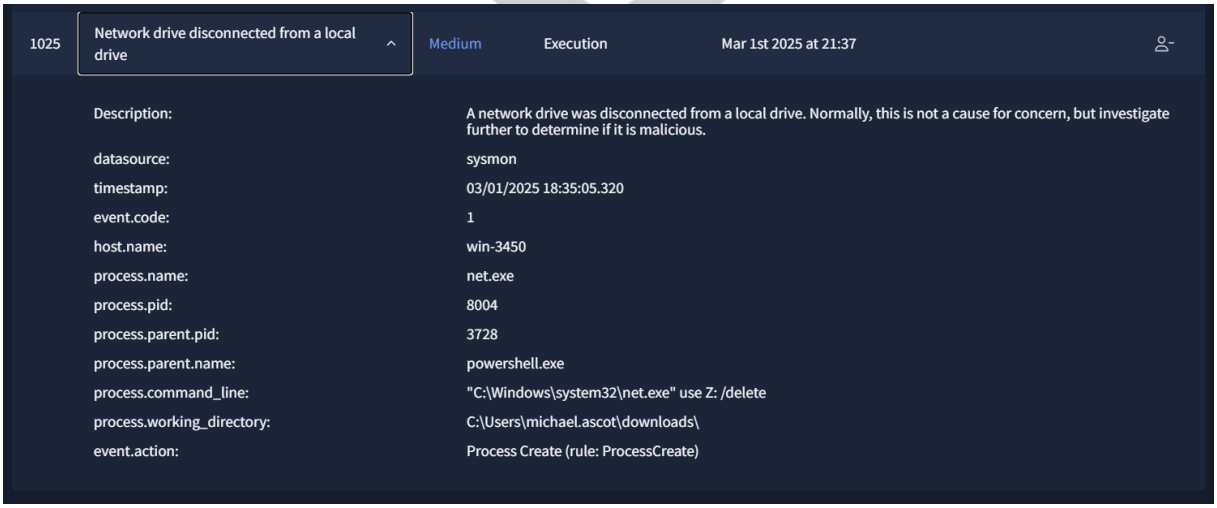


net.exe, ağ paylaşım bağlantıları ve oturum yönetimi için kullanılan bir Windows aracıdır. Burada, PowerShell üzerinden başlatılması olağandışı olup, kötü amaçlı bir betik veya

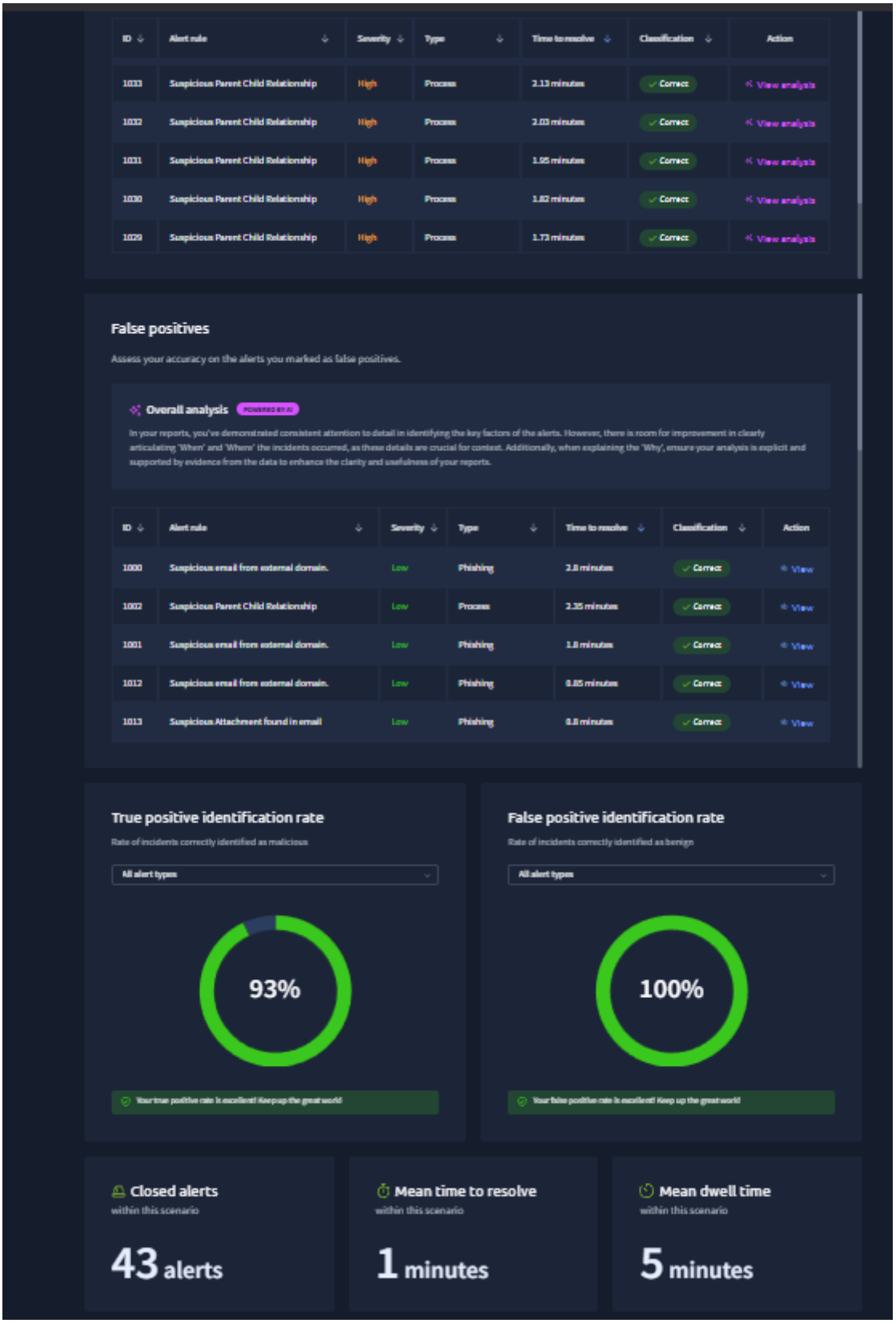
otomatik bir sürecin çalıştırılmış olabileceğini düşündürmektedir. Komut satırında "use Z: \FILESRV-01\SSF-FinancialRecords" geçmesi, bir ağ sürücüsüne bağlantı kurmaya çalışıldığını gösterir. Bu işlem genellikle manuel yapılırken, PowerShell üzerinden çalıştırılması yetkisiz erişim veya veri sızdırma girişimi olabilir. Ayrıca, "C:\Users\michael.ascot\downloads dizininden çalıştırılması, indirilen bir kötü amaçlı dosyanın tetiklenmiş olabileceğini gösterir. Güvenilir sistem işlemleri genellikle C:\Windows\System32 gibi sistem dizinlerinden çalıştırılır, bu nedenle "downloads" klasöründe başlatılan bir işlem şüpheli kabul edilebilir.



PowerShell'in nslookup.exe çalıştırması standart bir davranış değildir ve DNS Tunneling gibi kötü amaçlı faaliyetlere işaret edebilir. Veri sızdırma (exfiltration) veya C2 iletişimi için kullanılma ihtimali yüksektir. Sysmon, bu olayı "Process Create" olarak işaretlemiştir, çünkü PowerShell üzerinden başlatılmıştır. Komut satırında şifrelenmiş veya Base64 kodlanmış bir alan adına (haz4rdw4re.io) yapılan sorgu şüpheli görünmektedir. Ayrıca, sürecin "C:\Users\michael.ascot\downloads\exfiltration" dizininden çalıştırılması, veri sızdırma operasyonuna işaret edebilir. Bu unsurlar bir araya geldiğinde, olay True Positive (TP) olarak değerlendirilmelidir.



Önceki şüpheli aktivitenin ardından `net.exe`, Z: sürücüsünü kaldırmak için `use Z: /delete` komutuyla çalıştırılmıştır. Normalde manuel yapılan bu işlem, PowerShell üzerinden downloads klasöründe başlatılmıştır, bu da otomatik bir betik veya kötü amaçlı yazılım ihtimalini artırır. Downloads klasörü, zararlı yazılımların çalıştırıldığı yaygın bir dizin olduğundan bu durum şüpheli kabul edilir. Önceki `net.exe` işlemiyle bağlantılı olup kötü amaçlı bir sürecin parçası olabilir.



Simülasyon bittiğinde bize gösterdiği istatikler ve kapatılan alertler burada görünüyor.