

Using Live Response in Microsoft Defender for Endpoint



Microsoft Live Response, Microsoft 365 Defender portalının içerisinde yer alan olan güçlü bir özelliktir. Live Response kullanımı ile IT ekipleri olası caselerde daha fazla data erişimi için uzaktan komut dosyası çalıştırmak için uzak bir oturum kurabilir.

Live Response kullanımı ile önceden tanımlanmış komutları çalıştırmak mümkündür ve daha da güçlü olanı özel PowerShell komut dosyalarını yükleme yapılarak istenilen komutlarda çalıştırılabilir. Kısacası Live Response, Defender for Endpoint ürününe tamamen entegre edilmiş bulut tabanlı etkileşimli bir shell ürünüdür.

Live Response ile aşağıdaki işlemleri kolaylıkla sağlayabilirsiniz ;

- Bir cihaz üzerinde araştırma çalışması yapmak için temel ve gelişmiş komutları çalıştırabilirsiniz.
- Malware örnekleri ve PowerShell komut dosyalarının çıktıları gibi dosyaları doğrudan indirebilirsiniz.
- Dosyaları arka planda indirebilirsiniz !

- Live Response Library’ e bir PowerShell komut dosyası veya yürütülebilir dosya yükleyerek ve cihazda bu dosyayı çalıştırabilirsiniz.
- Yapılan veya yapılacak çalışmalar için düzeltme eylemleri gerçekleştirebilir veya geri alma işlemleri sağlayabilirsiniz.

Gereksinimler

Bir cihaz için live response başlatmadan önce aşağıdaki gereksinimleri karşılandığından emin olmalıyız.

Cihazlar aşağıdaki Windows sürümlerinden birini çalıştırıyor olmalıdır.

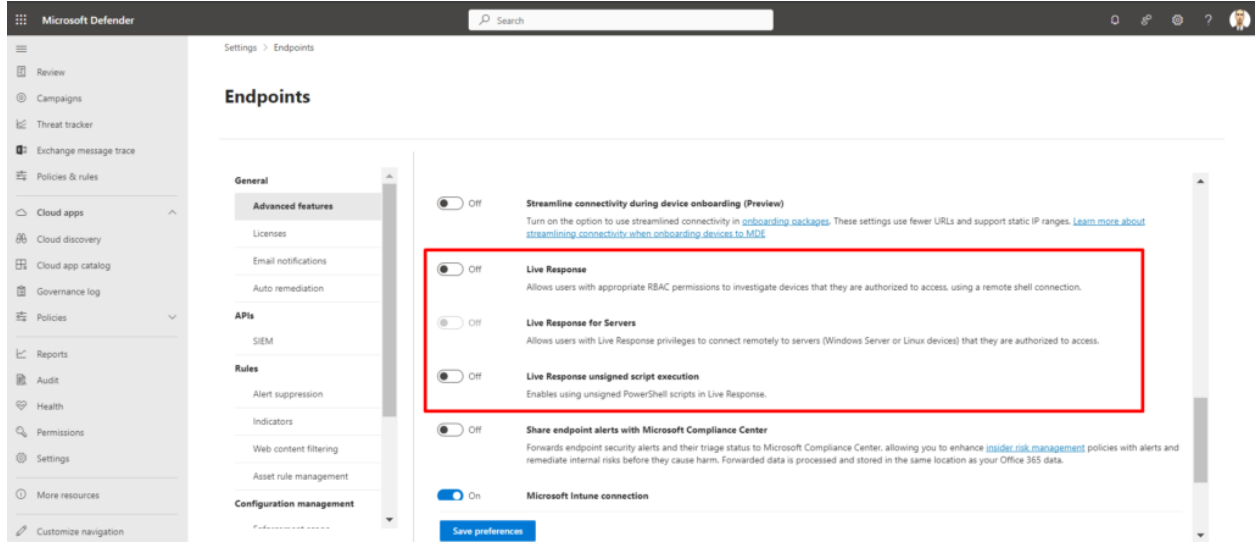
- **Windows 10 & 11**
 - [Version 1909](#) or later
 - [Version 1903](#) with [KB4515384](#)
 - [Version 1809 \(RS 5\)](#) with [KB4537818](#)
 - [Version 1803 \(RS 4\)](#) with [KB4537795](#)
 - [Version 1709 \(RS 3\)](#) with [KB4537816](#)
- **macOS** – Minimum required version: 101.43.84. Supported for Intel-based and ARM-based macOS devices.
- **Linux** – Minimum required version: 101.45.13
- **Windows Server 2012 R2** – with [KB5005292](#)
- **Windows Server 2016** – with [KB5005292](#)
- **Windows Server 2019**
 - Version 1903 or (with [KB4515384](#)) later
 - Version 1809 (with [KB4537818](#))
- **Windows Server 2022**

Enable live response from the advanced settings page.

Enable live response for servers from the advanced settings page (recommended).

Enable live response unsigned script execution (optional). (İmzasız komut dosyalarını çalıştırmak, tehditlere maruz kalmanızı artırabileceğinden önerilmez. Ancak bunları kullanmanız gerekiyorsa, Gelişmiş özellikler ayarları sayfasındaki ayarı etkinleştirmeniz gerekir.)

Advanced Feature ayarlarından, Live response seçeneğinin aktif edilmesi gerekmektedir. [Advanced features settings](#)

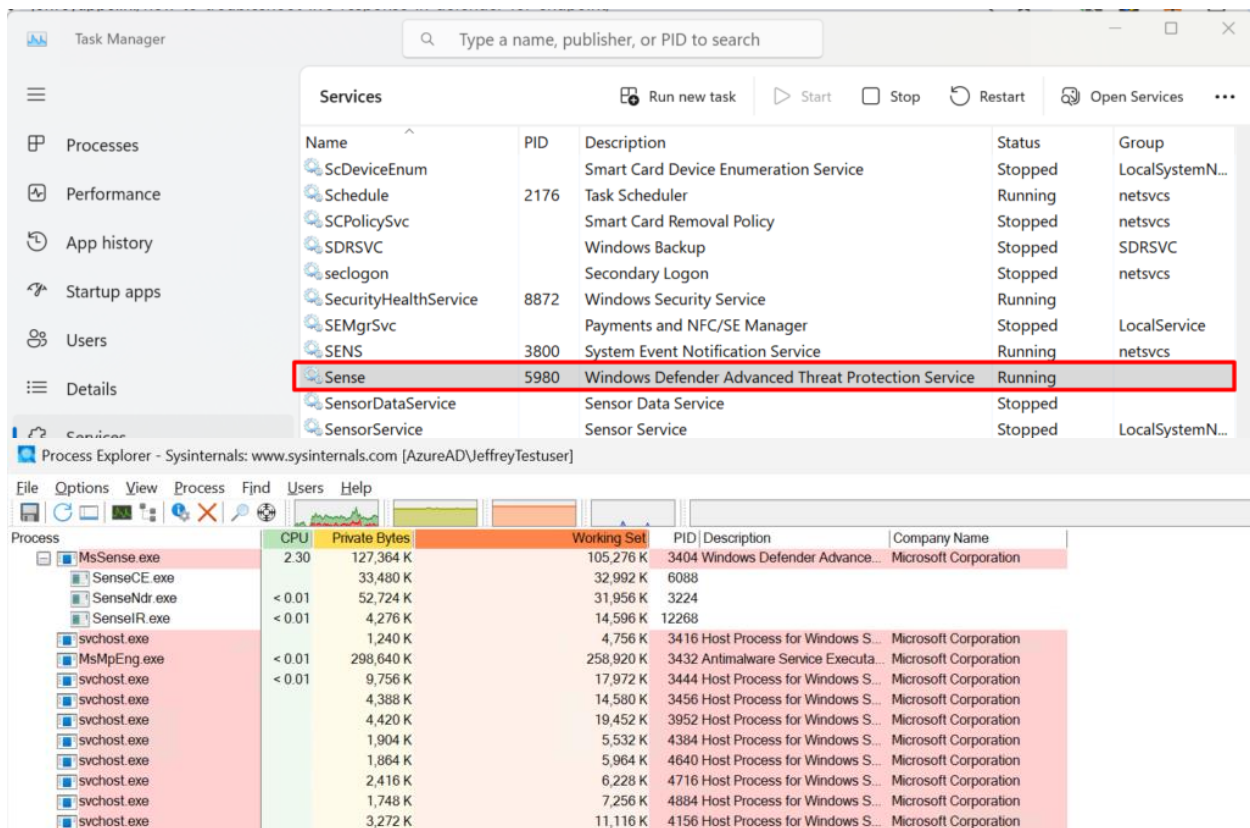


Live Response Servisleri

- **MsSense.exe:** Bu servis, Defender for Endpoint ana bileşenleri arasında gösterilen servistir. Servislerde SENSE adında bir servis olarak görebilmekteyiz.
- **SenseIR.exe:** Bu yürütülebilir dosya, Microsoft 365 Defender portalı üzerinden bir Live Response Oturumu başlatıldığında MsSense.exe dosyasının alt işlemi olarak ortaya çıkar ve çalışır.

MsSense.exe, Defender for endpoint'e cihaz doğru şekilde bağlandığında default olarak etkin bir şekilde çalışır ve durdurulamaz. Live Response bağlantısı başlatıldığında SenseIR.exe işlemini bir alt işlem olarak çalışmaktadır.

Live Response eylemlerinin çoğu SenseIR.exe işlemi aracılığıyla gerçekleştirilecektir servisin çalışır olduğu **kontrol edilmelidir**.



Live Response Komutları

Command	Description	Windows and Windows Server	macOS	Linux
cd	Changes the current directory.	Y	Y	Y
cls	Clears the console screen.	Y	Y	Y
connect	Initiates a live response session to the device.	Y	Y	Y
connections	Shows all the active connections.	Y	N	N

Command	Description	Windows and Windows Server	macOS	Linux
<code>dir</code>	Shows a list of files and subdirectories in a directory.	Y	Y	Y
<code>drivers</code>	Shows all drivers installed on the device.	Y	N	N
<code>fg <command ID></code>	Place the specified job in the foreground, making it the current job. Note that <code>fg</code> takes a <code>command ID</code> available from jobs, not a <code>PID</code> .	Y	Y	Y
<code>fileinfo</code>	Get information about a file.	Y	Y	Y
<code>findfile</code>	Locates files by a given name on the device.	Y	Y	Y
<code>getfile <file_path></code>	Downloads a file.	Y	Y	Y
<code>help</code>	Provides help information for live response commands.	Y	Y	Y
<code>jobs</code>	Shows currently running jobs, their ID and status.	Y	Y	Y

Command	Description	Windows and Windows Server	macOS	Linux
<code>persistence</code>	Shows all known persistence methods on the device.	Y	N	N
<code>processes</code>	Shows all processes running on the device.	Y	Y	Y
<code>registry</code>	Shows registry values.	Y	N	N
<code>scheduledtasks</code>	Shows all scheduled tasks on the device.	Y	N	N
<code>services</code>	Shows all services on the device.	Y	N	N
<code>startupfolders</code>	Shows all known files in startup folders on the device.	Y	N	N
<code>status</code>	Shows the status and output of specific command.	Y	Y	Y
<code>trace</code>	Sets the terminal's logging mode to debug.	Y	Y	Y

Kaynak: Microsoft Learn

Live Response Gelişmiş Komutlar

Command	Description	Windows and Windows Server	macOS	Linux
analyze	Analyses the entity with various incrimination engines to reach a verdict.	Y	N	N
collect	Collects forensics package from device.	N	Y	Y
isolate	Disconnects the device from the network while retaining connectivity to the Defender for Endpoint service.	N	Y	N
release	Releases a device from network isolation.	N	Y	N
run	Runs a PowerShell script from the library on the device.	Y	Y	Y
library	Lists files that were uploaded to the live response library.	Y	Y	Y
putfile	Puts a file from the library to the device. Files are saved in a working folder and are deleted when the device restarts by default.	Y	Y	Y
remediate	Remediates an entity on the device. The remediation action varies, depending on the entity type: <ul style="list-style-type: none"> – File: delete – Process: stop, delete image file – Service: stop, delete image file – Registry entry: delete – Scheduled task: remove – Startup folder item: delete file 	Y	Y	Y






Command	Description	Windows and Windows Server	macOS	Linux
	This command has a prerequisite command. You can use the <code>-auto</code> command in conjunction with <code>remediate</code> to automatically run the prerequisite command.			
<code>scan</code>	Runs a quick antivirus scan to help identify and remediate malware.	N	Y	Y
<code>undo</code>	Restores an entity that was remediated.	Y	N	N






Kaynak : Microsoft Learn

Initiating Live Response session

Security.microsoft.com adresinden sol tarafta bulunan **Assets** menüsünden “**Devices**” butonuna tıklıyoruz ve Live Response Session’ı başlatmak istediğimiz cihaza tıklıyoruz.

Açılan ekranda sağ üstte bulunan üç nokta’ya tıklayarak “**Initiating Live Response session**” seçeneğini seçiyoruz.



















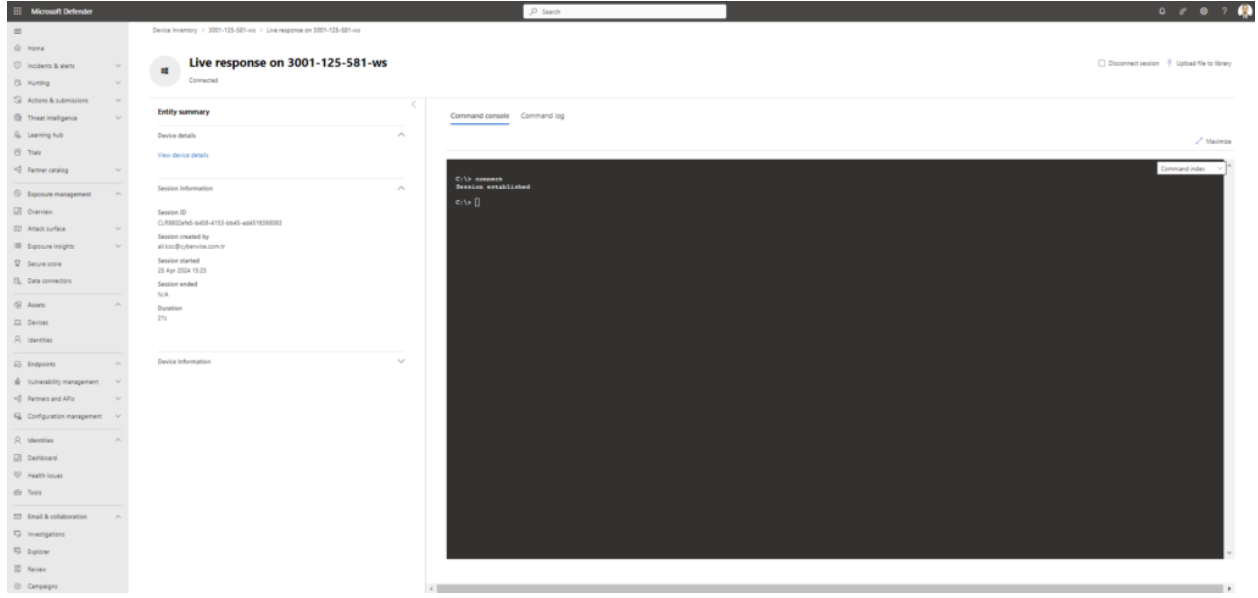
Device health status

Full scan status is unknown

Type	State
Last full scan	No scan performed
Last quick scan	Completed
Security intelligence	Version 1.409.487.0
Engine	Version 1.1.24030.4
Platform	Version 4.18.24030.9
Defender Antivirus mode	Active



Giriş sonrası “Connect” işlemi sonrası aşağıdaki ekran ile karşılaşılıyor olacaksınız.



Her Live Response oturumu benzersiz bir Oturum Kimliği oluşturur. Bu kimlik, denetim/izleme ve ek işlem eylemleri için kullanılır. Oturum Kimliği, Live Response ekranında sol panelde görüntüleyebilirsiniz.

Yukarıda daha önceden belirtildiği gibi, Live Response komutları özel olarak yüklenen PowerShell komut dosyalarıyla genişletilebilir. Her dosyanın merkezi kütüphaneye yüklenmesi gerekir. Bu etkileşimli bir PowerShell oturumu değildir; genel olarak, PowerShell.exe ve gerektiğinde ek hizmetler için SenseIR.exe'nin başka bir alt süreci oluşacaktır.

PowerShell komut dosyasını doğrudan çalıştırırken, SenseIR.exe'nin yeni bir PowerShell alt işlemi ile çalışacaktır.

Processes					
		Run new task	End task	Efficiency mode	...
Name	Status	23% CPU	81% Memory	1% Disk	Ne
Windows Defender Advanced Threat Protection Sense IR module		0%	0.1%	0 MB/s	0.1

Microsoft Defender

Device inventory > 3001-125-581-ws > Live response on 3001-125-581-ws

Live response on 3001-125-581-ws

Connected

Entity summary

Device details

View device details

Session information

Session ID: C15802d4e5-6455-4153-9d45-6d6153380303

Session created by: al@ms.com

Session started: 25 Apr 2024 13:25

Session ended: N/A

Duration: 3:37m

Device information

Command console

Command log

Command console

Session established

Command input

Disconnect session

Upload file to library

Maximize

Known limitations

Live Response hizmeti, belirtilen işlemleri çalıştırırken bazı sınırlamalara sahiptir. Live Response kullanılırken aşağıdaki sınırlamalar geçerlidir:

- Tek seferde 25 Live Response Session'ı yapılabilir
- Bir oturumda 30 dakika bir etkinlik olmazsa otomatik kapanır.

- Bireysel Live Response komutlarının 10 dakika zaman sınırı vardır.
- Getfile, findfile ve run komutlarında 30 dakikalık bir sınır vardır.
- Tek bir kullanıcı 10 eş zamanlı oturum başlatabilir.
- Bir cihaza aynı anda yalnızca bir oturum yapılabilir.

Büyük komut dosyaları/aramalar/uygulamalar çalıştırırken dikkatli olunması gerekmektedir. Oturum başlatıldığında 30 dakika sonra potansiyel bir zaman aşımı olacaktır.

Aşağıdaki dosya boyutlarını referans alabilirsiniz;

- `getfile` limit: 3 GB
- `fileinfo` limit: 30 GB
- `library` limit: 250 MB

Listing and exporting processes

Bir powershell dosyasını içeri aktararak çalıştırabilir ve bilgileri alabilirsiniz.

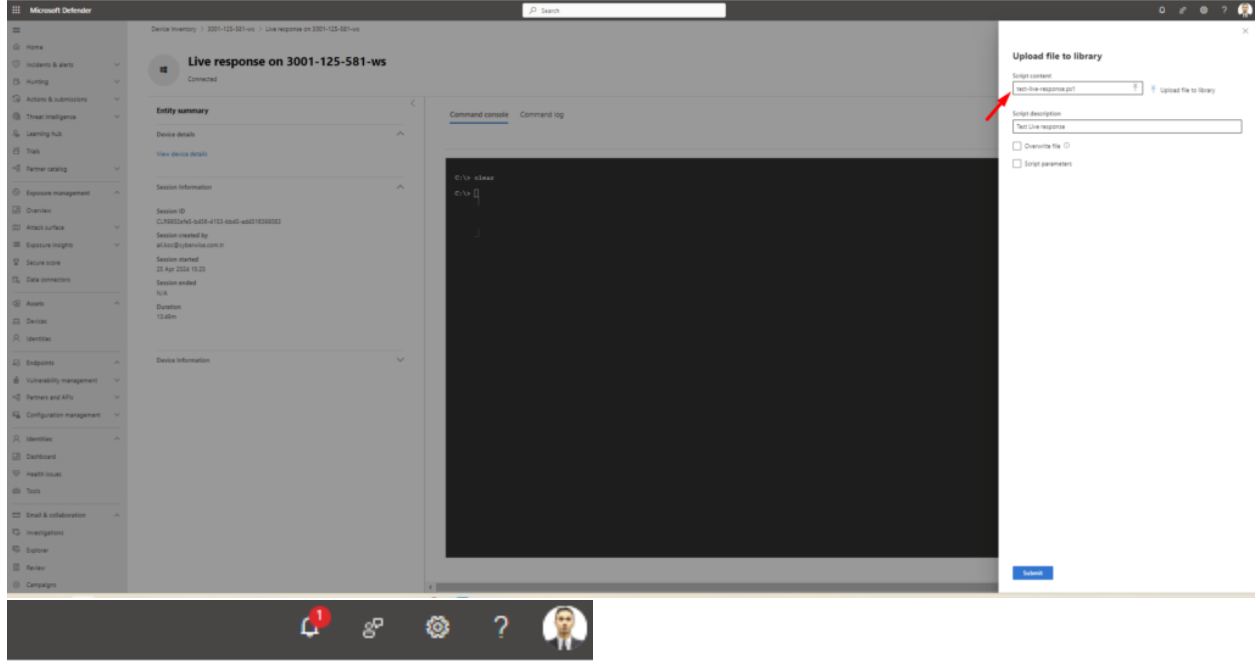
```
# Çalışan tüm processleri bana getir
```

```
$processes = Get-Process | Select-Object Id, ProcessName, CPU, Memory, StartTime
```

```
# Display process information
```

```
$processes | Format-Table -AutoSize
```

Örnek olarak yukarıdaki bir powershell komutunun içeri aktarılması süreçlerini takip edersek;



Yukarıdaki buton ile içeri aktarım yapıldıktan sonra “Successfully uploaded Script File” ibaresini görünüyoruz.

sonrasında aşağıdaki komutu çalıştırarak içe aktarılmış olan powershell dosyasını çalıştırabiliriz.

run test-live-response.ps1

Komut sonrası aktifte çalışan tüm processleri görüntüleyebiliriz.

```
Command console Command log Maximize

C:\> clear

C:\> run test-live-response.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\F5ScriptOutputs\F5Script_Transcript_(1CD3CD3D-5BC7-4C49-BC7A-7E422422485A).txt

  Id ProcessName CPU Memory StartTime
  --
9632 AggregatoHost 0.590425 4/18/2024 11:28:03 PM
3164 ai 0.202125 4/25/2024 10:09:41 AM
5536 AnyDesk 3.745625 4/18/2024 11:27:58 PM
5536 AnyDesk 0.269275 4/25/2024 9:59:08 AM
23764 ApplicationFrameHost 0.515625 4/25/2024 10:00:55 AM
5528 asmcsv 0.1875 4/18/2024 11:27:58 PM
26560 audiody 4691.6875 4/25/2024 10:15:44 AM
22556 backgroundTaskHost 0.0625 4/25/2024 9:58:40 AM
5216 hsmHostControlService 0.09275 4/18/2024 11:27:58 PM
5224 hsmHostStorageService 0.703125 4/18/2024 11:27:58 PM
3524 hsmHostUpgradeService 0.1875 4/18/2024 11:27:57 PM
27436 CashDev 0.8125 4/25/2024 9:58:35 AM
2696 chrome 3.6875 4/25/2024 10:54:18 AM
3976 chrome 0.09275 4/25/2024 3:26:02 PM
4612 chrome 1.609275 4/25/2024 10:21:17 AM
6876 chrome 107.3125 4/25/2024 1:38:13 PM
8744 chrome 249.203125 4/25/2024 10:16:53 AM
9480 chrome 1.578125 4/25/2024 10:16:54 AM
12544 chrome 105.5 4/25/2024 10:16:54 AM
13976 chrome 0.046875 4/25/2024 10:16:53 AM
15796 chrome 2.40625 4/25/2024 11:16:04 AM
14856 chrome 6.28125 4/25/2024 3:26:02 PM
15360 chrome 13.46875 4/25/2024 11:21:19 AM
16420 chrome 6.109275 4/25/2024 1:40:29 AM
17248 chrome 0.375 4/25/2024 3:41:56 PM
17680 chrome 69.954375 4/25/2024 10:16:54 AM
21176 chrome 34.63625 4/25/2024 10:16:54 AM
22208 chrome 11.234375 4/25/2024 10:16:53 AM
22288 chrome 34.046875 4/25/2024 11:16:03 AM
23616 chrome 13.09375 4/25/2024 10:17:00 AM
24076 chrome 5.6875 4/25/2024 10:16:54 AM
24404 chrome 53.446875 4/25/2024 10:16:54 AM
24624 chrome 43.59375 4/25/2024 3:20:54 PM
25136 chrome 577.59375 4/25/2024 10:16:54 AM
25196 chrome 12.54375 4/25/2024 10:16:54 AM
25896 chrome 786.28125 4/25/2024 10:21:17 AM
4948 conhost 0.09275 4/18/2024 11:27:58 PM
10900 conhost 0.109275 4/18/2024 11:30:19 PM
13604 conhost 0 4/25/2024 3:42:55 PM
852 csrss 10.859275 4/18/2024 11:27:58 PM
7544 csrss 4.724275 4/24/2024 11:09:52 PM
```

```
Command console Command log Maximize

20244 svchost 0.046875 4/25/2024 3:42:08 PM
21240 svchost 1.625 4/25/2024 9:11:20 AM
22832 svchost 0.75 4/25/2024 9:58:54 AM
22872 svchost 7.625 4/25/2024 9:58:34 AM
25704 svchost 1.796875 4/25/2024 9:58:32 AM
27076 svchost 0 4/25/2024 12:18:34 PM
27520 svchost 0.015625 4/25/2024 3:38:08 PM
27552 svchost 0.171875 4/25/2024 3:36:04 PM
4 System 3908.484375 4/18/2024 11:27:46 PM
24476 SystemSettings 1.03125 4/25/2024 10:00:55 AM
27232 SystemSettingsBroker 1.578125 4/25/2024 10:00:55 AM
12032 taskhoste 2.015625 4/25/2024 9:58:35 AM
16736 Taskmgr 36.4375 4/25/2024 3:29:58 PM
6100 TeamViewer_Service 13.796875 4/18/2024 11:27:58 PM
21800 TestInputHost 12.59375 4/25/2024 9:58:47 AM
14604 TeamViewerAppex 80.3125 4/18/2024 11:27:58 PM
14360 TeGDI 0.84375 4/25/2024 9:59:08 AM
13980 unsecapp 0.0625 4/25/2024 9:58:43 AM
21140 unsecapp 0.0625 4/25/2024 9:58:48 AM
20536 UserOOBBroker 0 4/25/2024 10:00:57 AM
4272 vmact 3.28125 4/18/2024 11:27:58 PM
6188 vmactdhp 0.078125 4/18/2024 11:27:58 PM
5868 vmware-authd 0.31875 4/18/2024 11:27:58 PM
10688 vmware-tray 0.03125 4/25/2024 9:59:16 AM
4228 vmware-usbArbitrator64 3.03125 4/18/2024 11:27:58 PM
6252 WavesAudioService 0.765625 4/18/2024 11:27:58 PM
15080 WavesSec64 32.078125 4/25/2024 9:58:47 AM
6824 WavesSysSec64 23.264375 4/18/2024 11:27:58 PM
10836 Whatapp 0.224375 4/25/2024 1:27:07 PM
7948 Widgets 1.559275 4/25/2024 9:59:38 AM
26776 WidgetService 0.34375 4/25/2024 9:59:46 AM
1076 wininit 0.268625 4/18/2024 11:27:58 PM
21288 winlogon 0.26125 4/24/2024 11:08:52 PM
4924 wlanet 0.40625 4/18/2024 11:27:58 PM
9124 WmiPrvSE 64.875 4/18/2024 11:28:02 PM
28820 WmiPrvSE 1.15625 4/25/2024 3:36:04 PM
4368 WMIRegistrationService 0.246875 4/18/2024 11:27:58 PM
1484 WDDHost 3.703125 4/18/2024 11:27:58 PM
1644 WDDHost 1 4/18/2024 11:27:58 PM
1708 WDDHost 0.046875 4/18/2024 11:27:57 PM
1732 WDDHost 0.046875 4/18/2024 11:27:57 PM
1816 WDDHost 693.265625 4/18/2024 11:27:57 PM
2396 WDDHost 190.5 4/18/2024 11:27:57 PM

C:\>
```

Eğer oluşan bu çıktıyı export etmek isterseniz, yine bir export ps1 çalıştırmanız gerekmektedir.

```
$processes = Get-Process | Select-Object Id, ProcessName, CPU, Memory, StartTime
$textFilePath = "C:\Path\To\Your\alikoctest.txt"
```

\$processes | Out-File -FilePath \$textFilePath
Write-Host "Process information exported to: \$textFilePath"

içe aktarım sonrası "library" komutu ile içeride kullanılabilir ps1 dökümanlarını görmeyi sağlayacaktır.

```
C:\> library
```

File name	Description	Parameters	Parameters description	Uploaded on	Uploaded by
test-live-response.ps1	Test Live response	No		Thu Apr 25 2024 15:40:12 GMT+0200 (GMT+02:00)	ali.koc@cyberwise.com.tr
test-live-response.ps1	Test Live response	No		Thu Apr 25 2024 15:40:12 GMT+0200 (GMT+02:00)	ali.koc@cyberwise.com.tr
export.ps1	export	No		Thu Apr 25 2024 15:55:12 GMT+0200 (GMT+02:00)	ali.koc@cyberwise.com.tr

```
C:\>
```

Daha sonra run export.ps1 komutunu çalıştırarak export ediyoruz.

```
Command console Command log
```

```
20244 svchost 0.046075 4/25/2024 9:42:08 PM
21440 svchost 1.625 4/25/2024 9:51:26 AM
22352 svchost 0.75 4/25/2024 9:59:56 AM
22372 svchost 7.625 4/25/2024 9:58:34 AM
25704 svchost 1.796975 4/25/2024 9:58:32 AM
27076 svchost 0 4/25/2024 12:18:04 PM
27528 svchost 0.015625 4/25/2024 9:58:09 PM
27552 svchost 0.171875 4/25/2024 9:58:04 PM
* System 3908.484375 4/18/2024 11:27:46 PM
24476 SystemSettings 1.03125 4/25/2024 10:00:55 AM
27222 SystemSettingsBroker 1.578125 4/25/2024 10:03:39 AM
12032 taskhostw 2.015625 4/25/2024 9:58:35 AM
16736 Taskmgr 26.8375 4/25/2024 9:29:58 PM
6100 TaskIndex_Service 12.796975 4/18/2024 11:27:58 PM
21800 TestInputHost 13.59375 4/25/2024 9:58:47 AM
5464 TransrvWrapper 80.1125 4/18/2024 11:27:58 PM
34460 TracUI 0.84375 4/25/2024 9:58:08 AM
13980 unsecapp 0.0625 4/25/2024 9:58:43 AM
21140 unsecapp 0.0625 4/25/2024 9:58:48 AM
20536 UserOOBBroker 0 4/25/2024 10:00:57 AM
6272 vmact 2.28125 4/18/2024 11:27:58 PM
6188 vmactdubp 0.078125 4/18/2024 11:27:58 PM
5568 vmact-authd 0.21875 4/18/2024 11:27:58 PM
10656 vmact-tray 0.03125 4/25/2024 9:59:16 AM
6228 vmact-subscribitor64 2.03125 4/18/2024 11:27:58 PM
6252 WavesAudioService 0.765625 4/18/2024 11:27:58 PM
15080 WavesSvc64 22.078125 4/25/2024 9:58:47 AM
6224 WavesSvc64 22.284375 4/18/2024 11:27:58 PM
10336 WhatApp 0.284375 4/25/2024 11:27:57 PM
7848 Widgets 1.859375 4/25/2024 9:58:38 AM
26776 WidgetsService 0.34375 4/25/2024 9:58:46 AM
1076 wininit 0.265625 4/18/2024 11:27:56 PM
21288 winlogon 0.28125 4/24/2024 11:03:52 PM
4924 wlanext 0.40625 4/18/2024 11:27:58 PM
9124 WinPrvSE 64.875 4/18/2024 11:28:02 PM
28820 WinPrvSE 1.15625 4/25/2024 9:58:04 PM
6368 WMIRegistrationService 0.265625 4/18/2024 11:27:58 PM
1484 WUDFHost 2.703125 4/18/2024 11:27:56 PM
1648 WUDFHost 1 4/18/2024 11:27:56 PM
1708 WUDFHost 0.046075 4/18/2024 11:27:57 PM
1752 WUDFHost 0.046075 4/18/2024 11:27:57 PM
1816 WUDFHost 693.265625 4/18/2024 11:27:57 PM
2256 WUDFHost 190.5 4/18/2024 11:27:57 PM

C:\> /run export.ps1
```

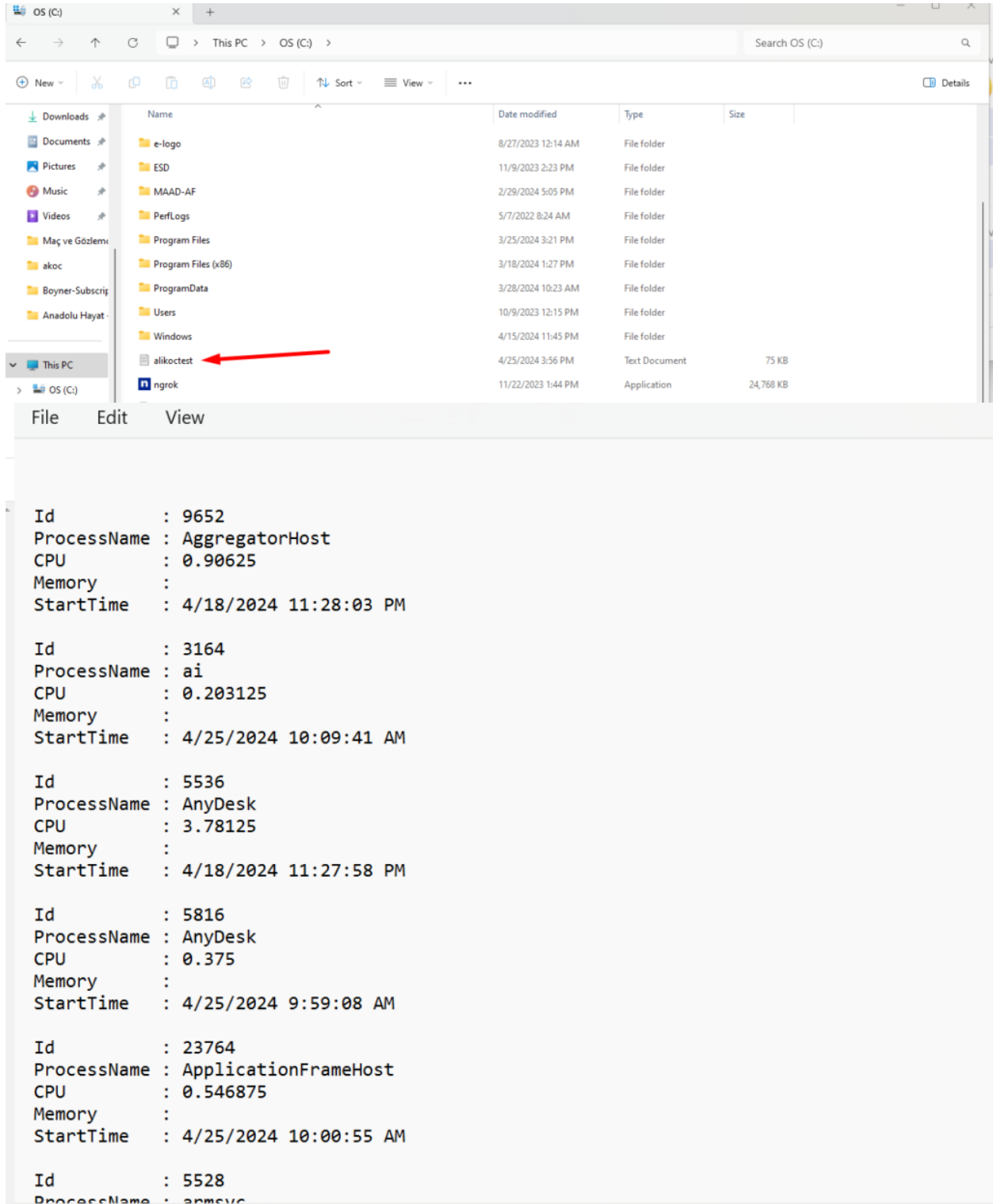
yapılan işlemin tamamlandığını görüyoruz.

```
C:\> run export.ps1
```

```
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_Transcript_137430444-FDD4-4DB8-B09C-6BF6E01FE23C.txt
Process information exported to: C:\alikoctest.txt

C:\>
```

İlgili pathe gittiğimizde ilgili dosyaya erişebilirsiniz.



Live Response özelliğinin işlevselliği ve çeşitli amaçlar için çok yönlülüğü hakkında çalışmalarını içeren blog yazısını tamamlamış bulunmaktayız.

Benzer şekilde, olay müdahale sürecinizde faydalı olabilecek diğer PowerShell komut dosyalarını geliştirebilir ve oluşturabilirsiniz. Yukarıda belirtilmiş olan komut dosyalarını farklı

parametrelerle zenginleřtirerek kullanabiliriz. İe aktarılan powershell komutlarında dikkat edilmesi gereken önemli nokta, bu cihazlar üzerinde bilgi toplama amaçlı yapılacak olan komutları içermelidir.

Thanks to Microsoft Learn and jeffreyappel