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.

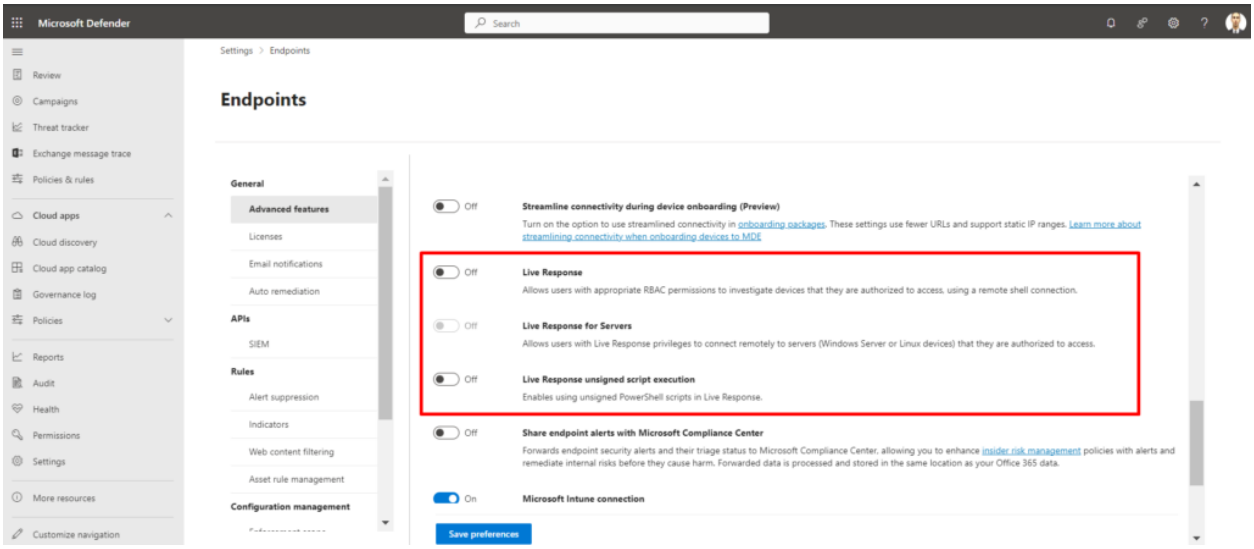
- **Windows 10 & 11**
  - Version 1909 or later
  - Version 1903 with KB4515384
  - Version 1809 (RS 5) with KB4537818
  - Version 1803 (RS 4) with KB4537795
  - Version 1709 (RS 3) with KB4537816
- **macOS** – Minimum required version: 101.43.84. Supported for Intel-based and ARM-based macOS devices.
- **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

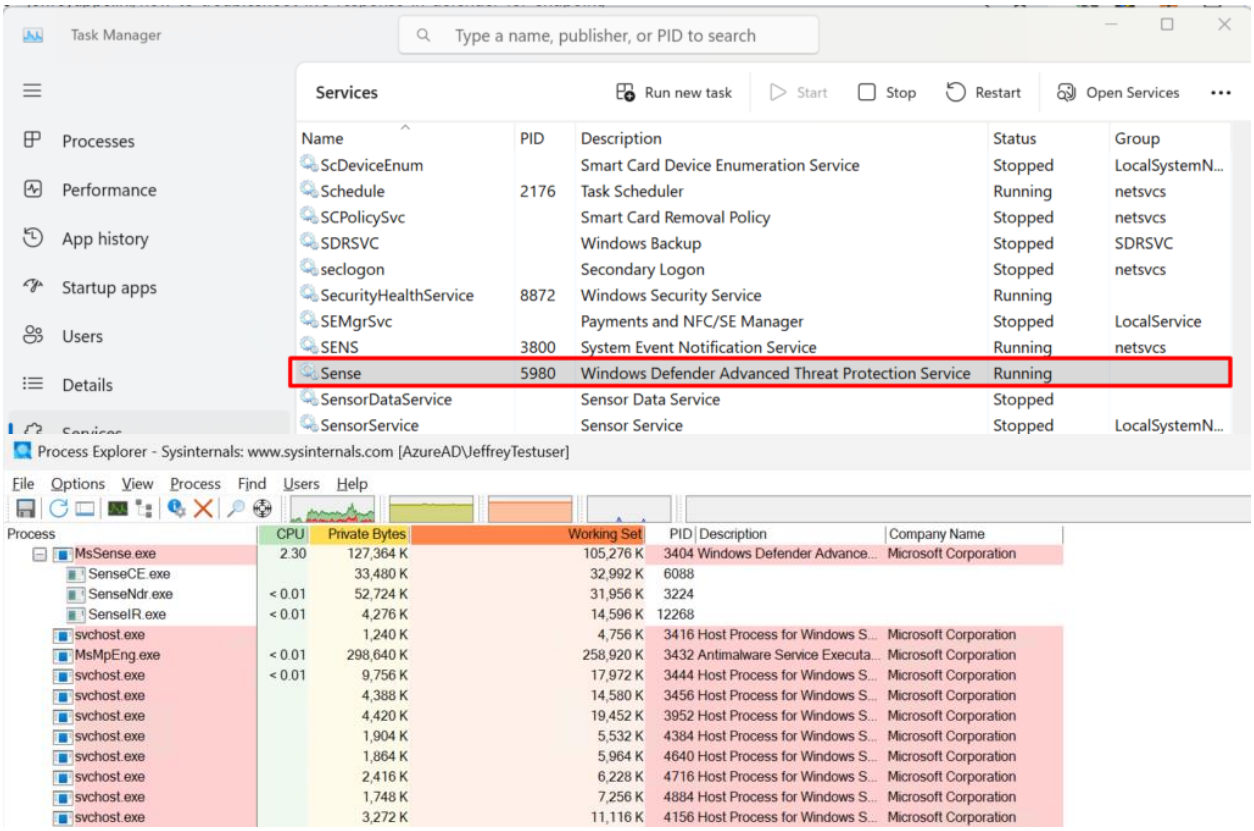


Live Response Servisleri

- **MsSense.exe:** Bu servis, Defender for Endpoint ana bileşenleri arasında gösterilen servisidir. 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
`dir`	Shows a list of files and subdirectories in a directory.	Y	Y	Y
`drivers`	Shows all drivers installed on the device.	Y	N	N
`fg <command ID>`	Place the specified job in the foreground, making it the current job. Note that `fg` takes a `command ID` available from jobs, not a PID.	Y	Y	Y
`fileinfo`	Get information about a file.	Y	Y	Y
`findfile`	Locates files by a given name on the device.	Y	Y	Y
`getfile <file_path>`	Downloads a file.	Y	Y	Y
`help`	Provides help information for live response commands.	Y	Y	Y
`jobs`	Shows currently running jobs, their ID and status.	Y	Y	Y

Command	Description	Windows and Windows Server	macOS	Linux
`persistence`	Shows all known persistence methods on the device.	Y	N	N
`processes`	Shows all processes running on the device.	Y	Y	Y
`registry`	Shows registry values.	Y	N	N
`scheduledtasks`	Shows all scheduled tasks on the device.	Y	N	N
`services`	Shows all services on the device.	Y	N	N
`startupfolders`	Shows all known files in startup folders on the device.	Y	N	N
`status`	Shows the status and output of specific command.	Y	Y	Y
`trace`	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: – 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

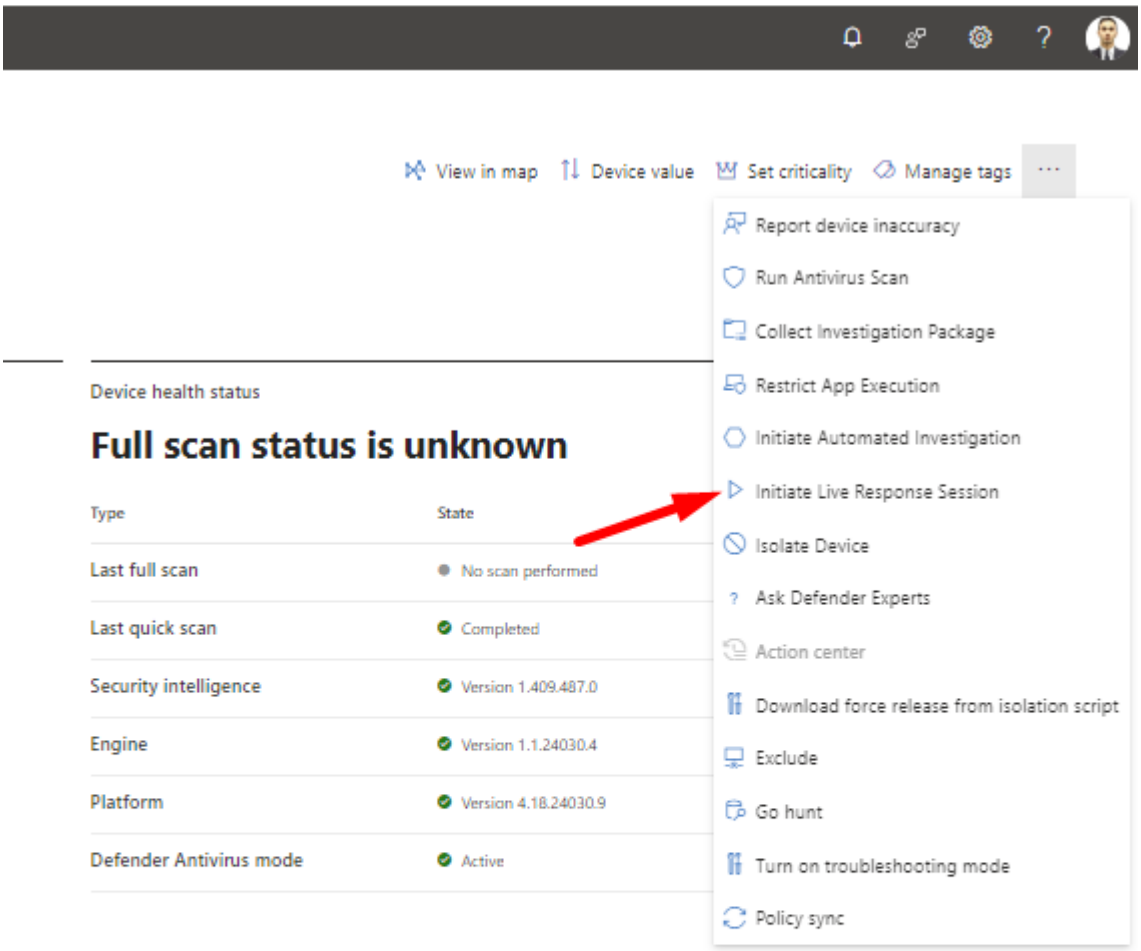
Command	Description	Windows and Windows Server	macOS	Linux
	This command has a prerequisite command. You can use the `-auto` command in conjunction with remediate to automatically run the prerequisite command.			
`scan`	Runs a quick antivirus scan to help identify and remediate malware.	N	Y	Y
`undo`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

Kaynak : Microsoft Learn

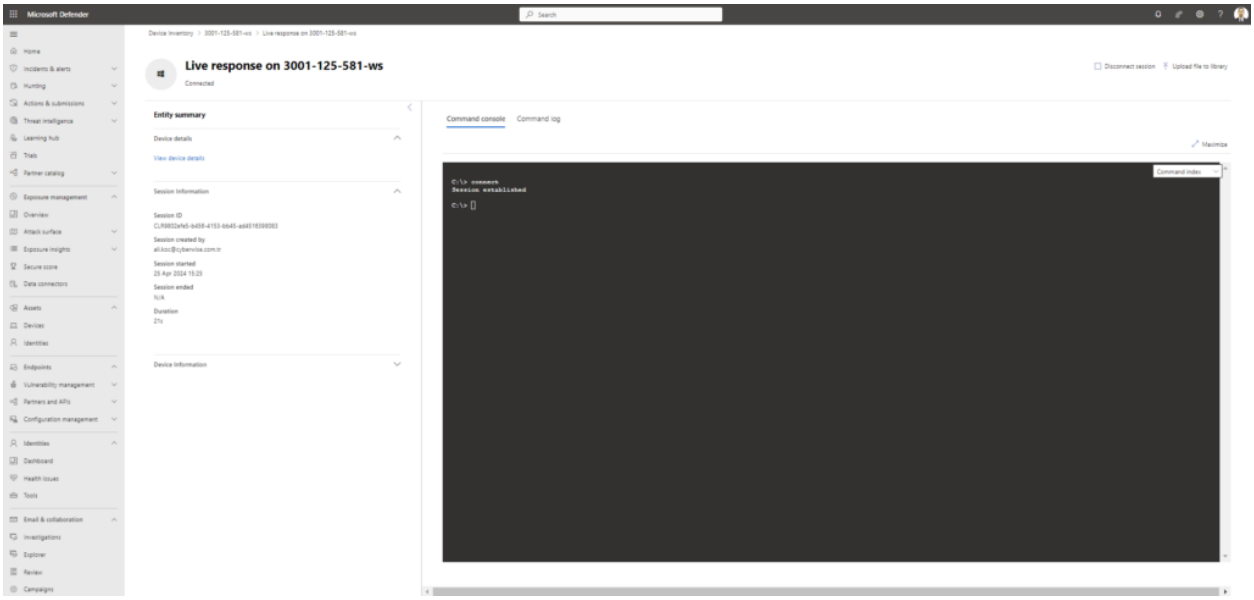
Initiating Live Response session

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.



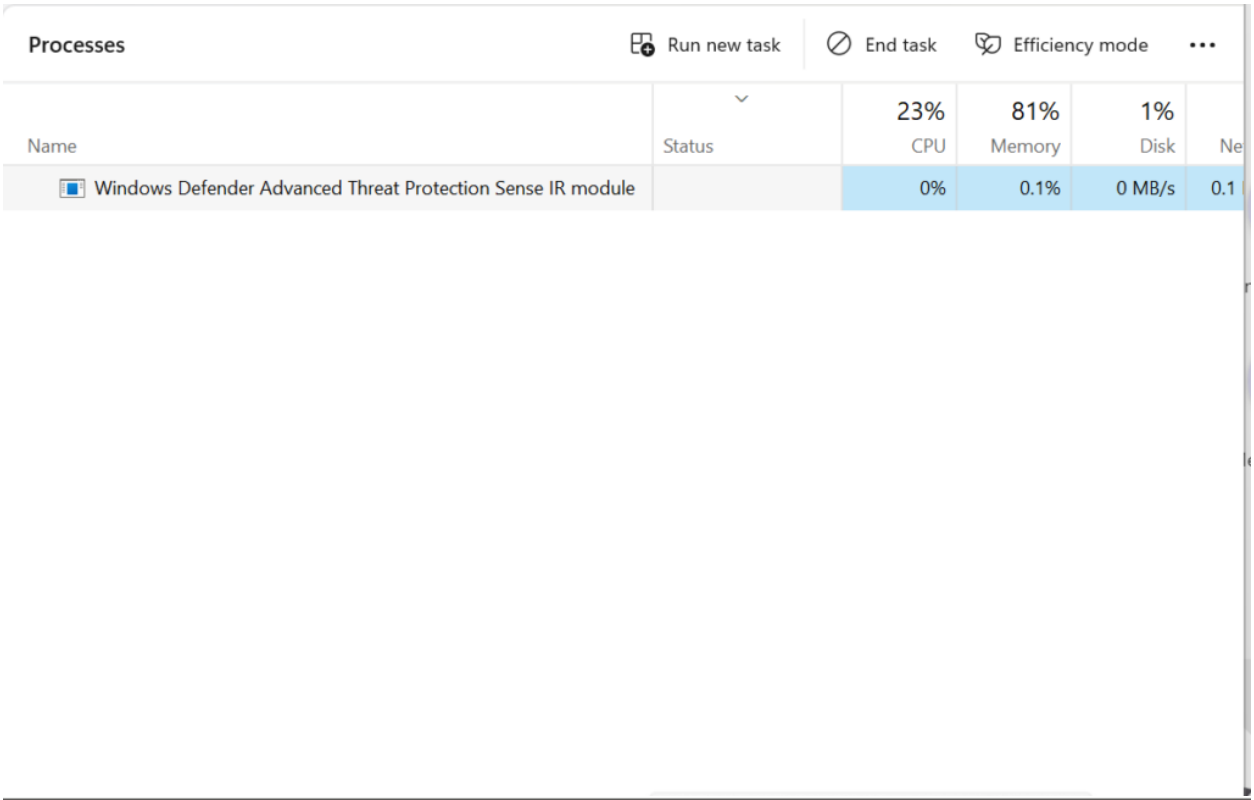
Giriş sonrası “Connect” işlemi sonrası aşağıdaki ekran ile karşılaşıyor olacaksınız.

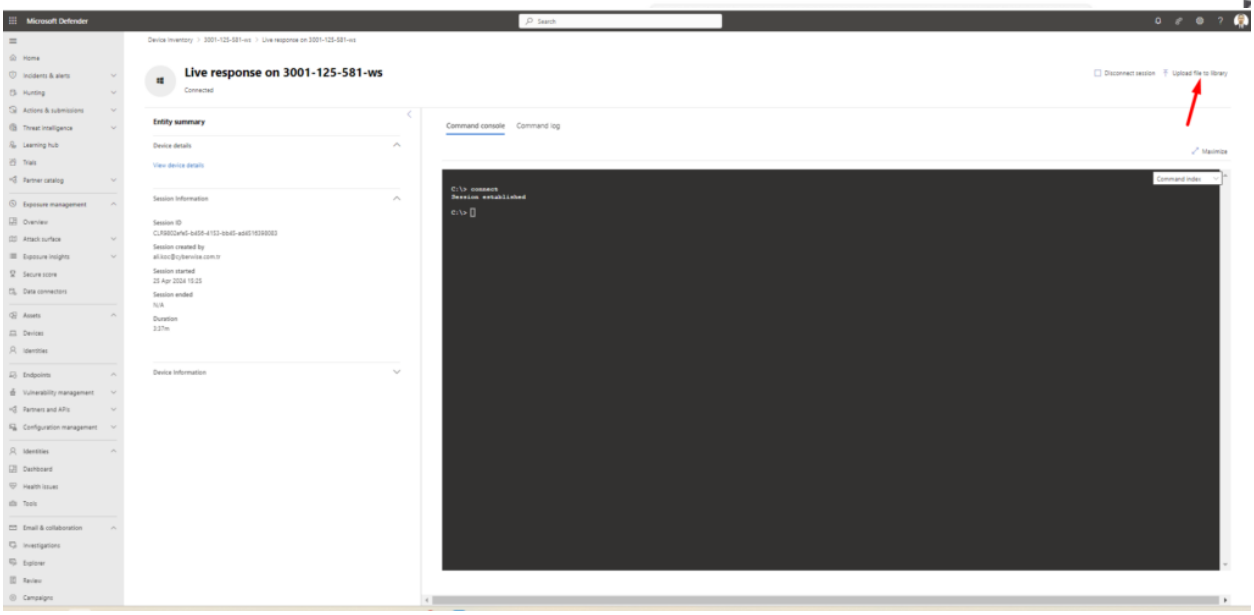


Her Live Response oturumu benzersiz bir Oturum Kimliği oluşturur. Bu kimlik, denetim/izleme ve ek işlem eylemleri için kullanılır. Oturum Kimliği, Live Response ekranında sol panelde görüntüleyebilirsiniz.

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.





Known limitations

Live Response hizmeti, belirtilen işlemleriçalıştırırken 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

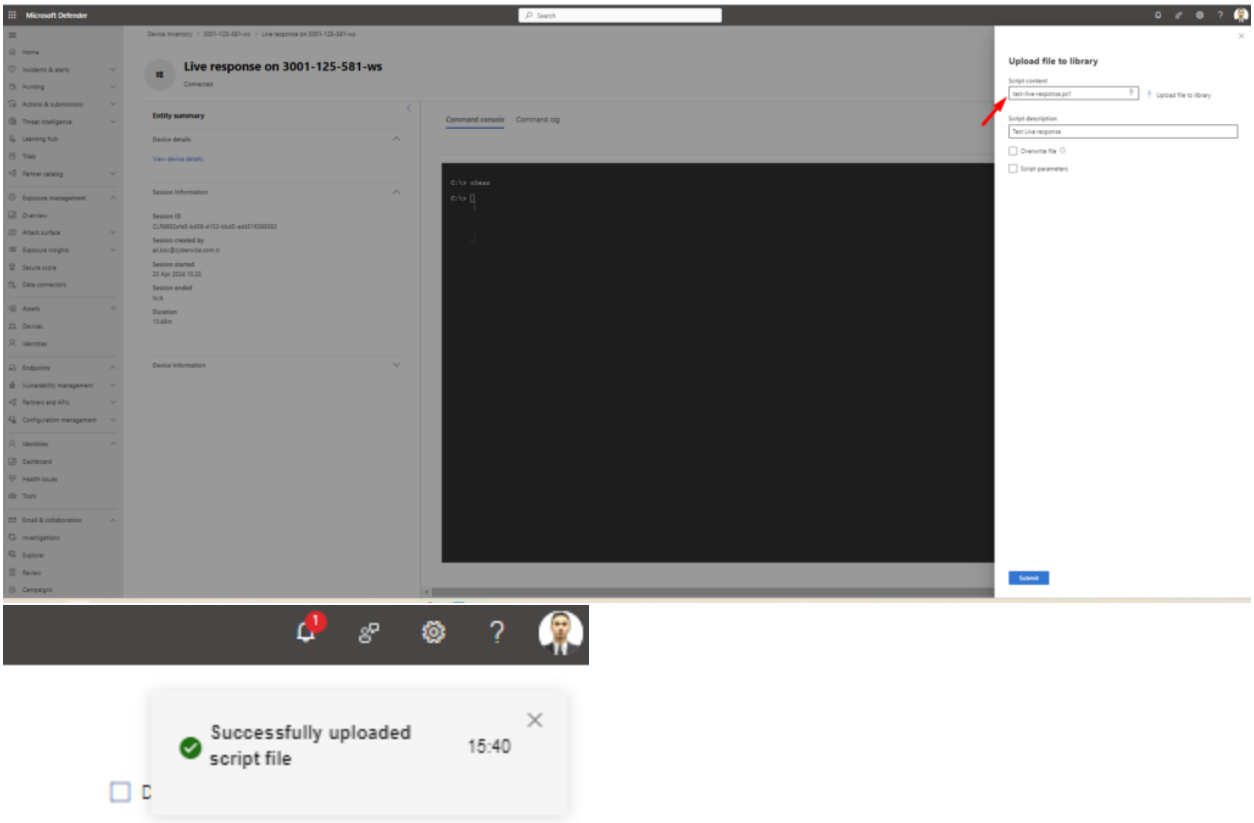
Listing and exporting processes

Bir powershell dosyasını içeri aktararak çalıştırabilir ve bilgileri alabilirsiniz.

```
# Calışan 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;

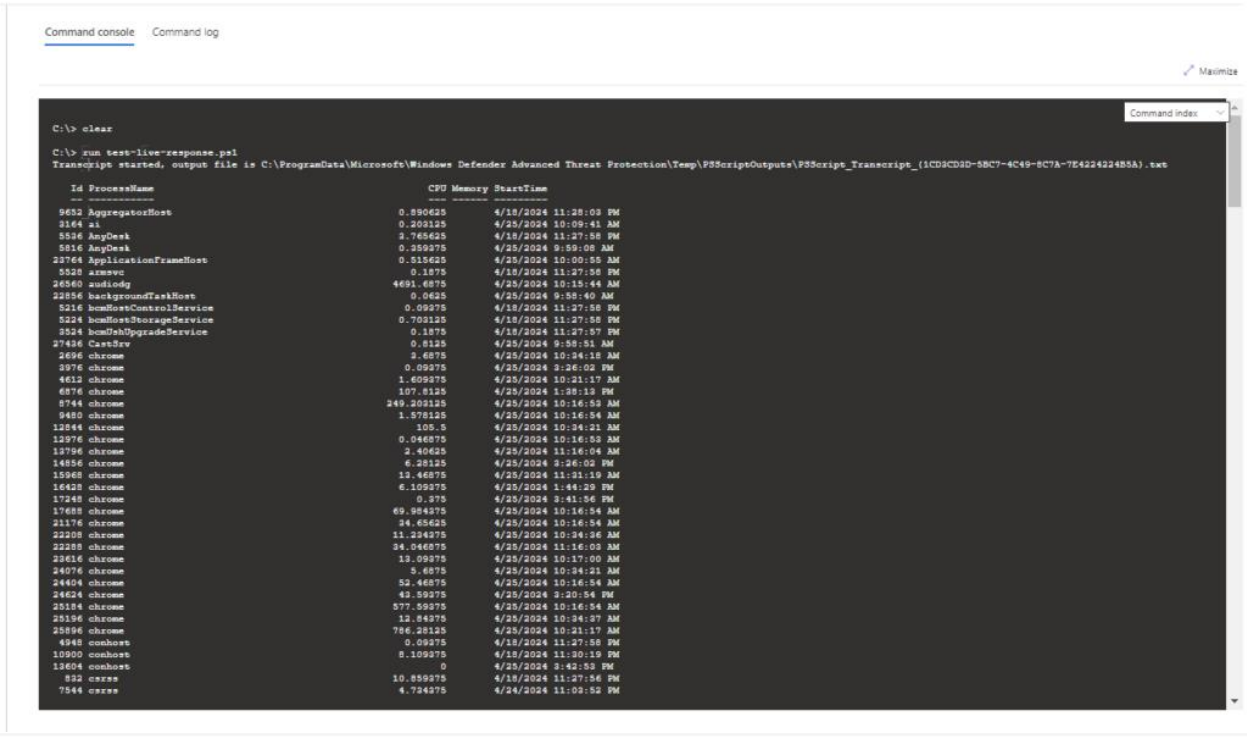


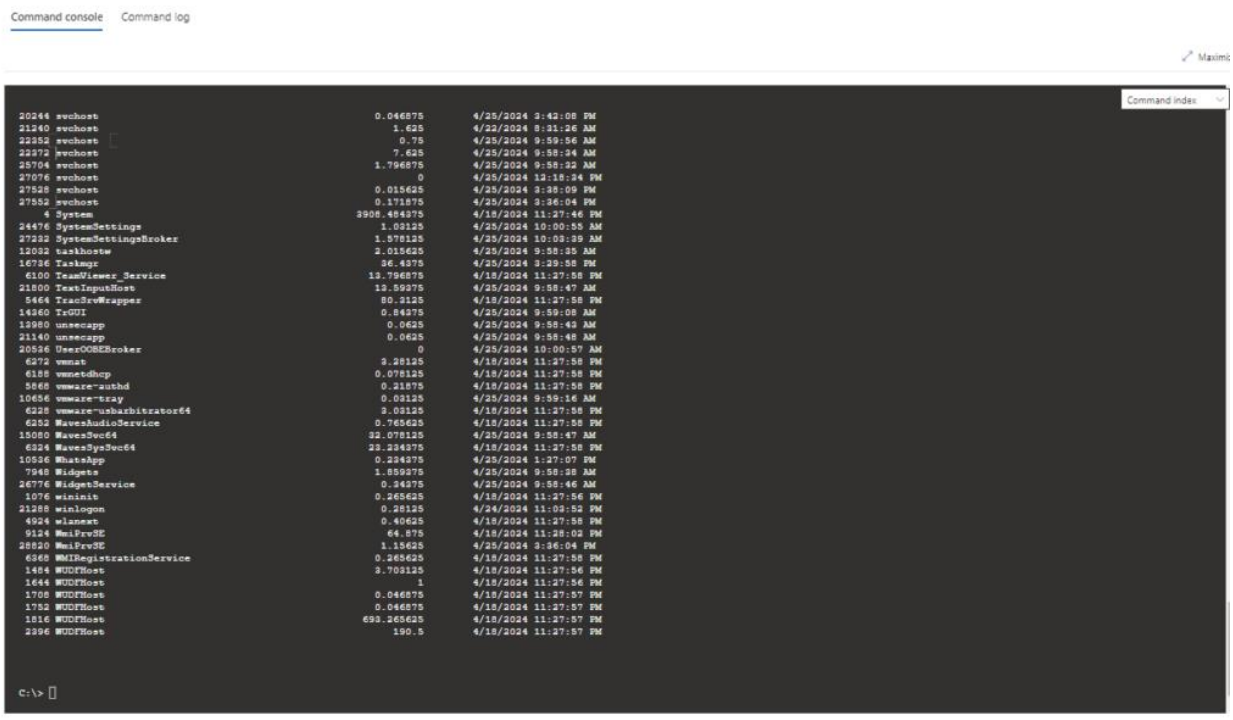
Yukarıdaki buton ile içeri aktarım yapıldıktan sonra “Successfuly uploaded Script File” ibaresini görüntülüyoruz.

sonrasında aşağıdaki komutu çalıştırarak içe aktarılmış olan powershell dosyasını çalıştırabiliriz.

run test-live-response.ps1

Komut sonrası aktifte çalışan tüm processleri görüntüleyebiliriz.



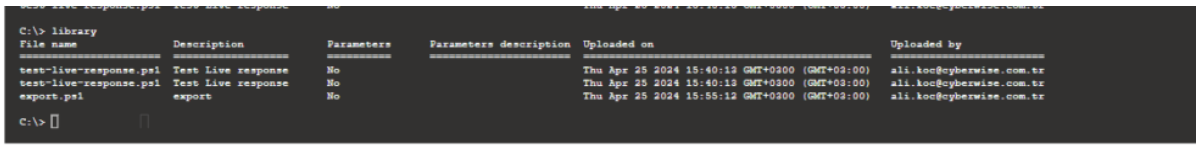


Eğer oluşan bu çıktıyı export etmek isterseniz, yine bir export ps1 calıstırmanız gerekmektedir.

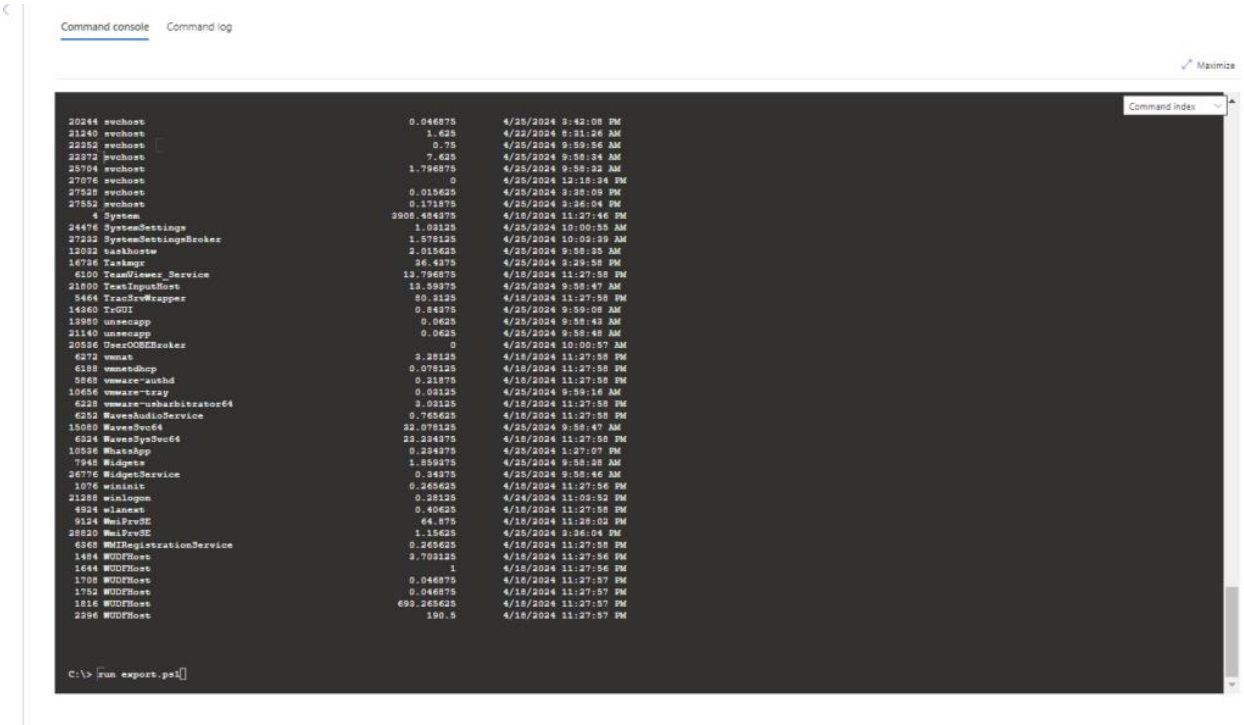
$processes = Get-Process | Select-Object Id, ProcessName, CPU, Memory, StartTime
$textFilePath = “C:\Path\To\Your\alikoctest.txt”

$processes | Out-File -FilePath $textFilePath
Write-Host “Process information exported to: $textFilePath”

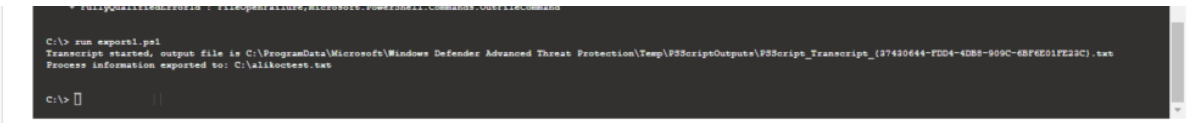
içe aktarım sonrası “library” komutu ile içeride kullanılabilir ps1 dökümanlarını görmenizi sağlayacaktır.



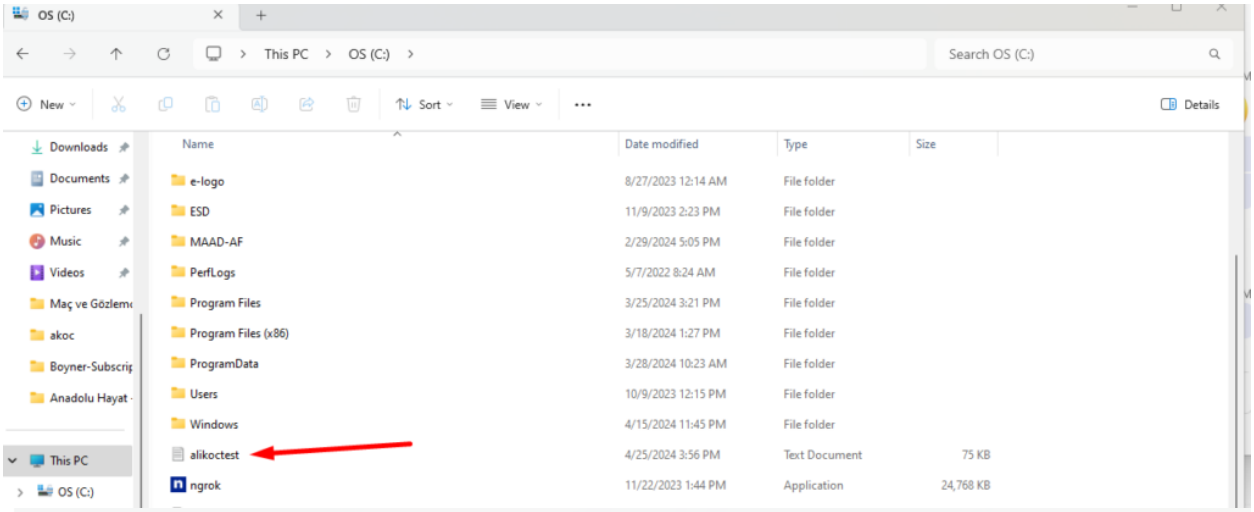
Daha sonra run export.ps1 komutunu çalıştırarak export ediyoruz.

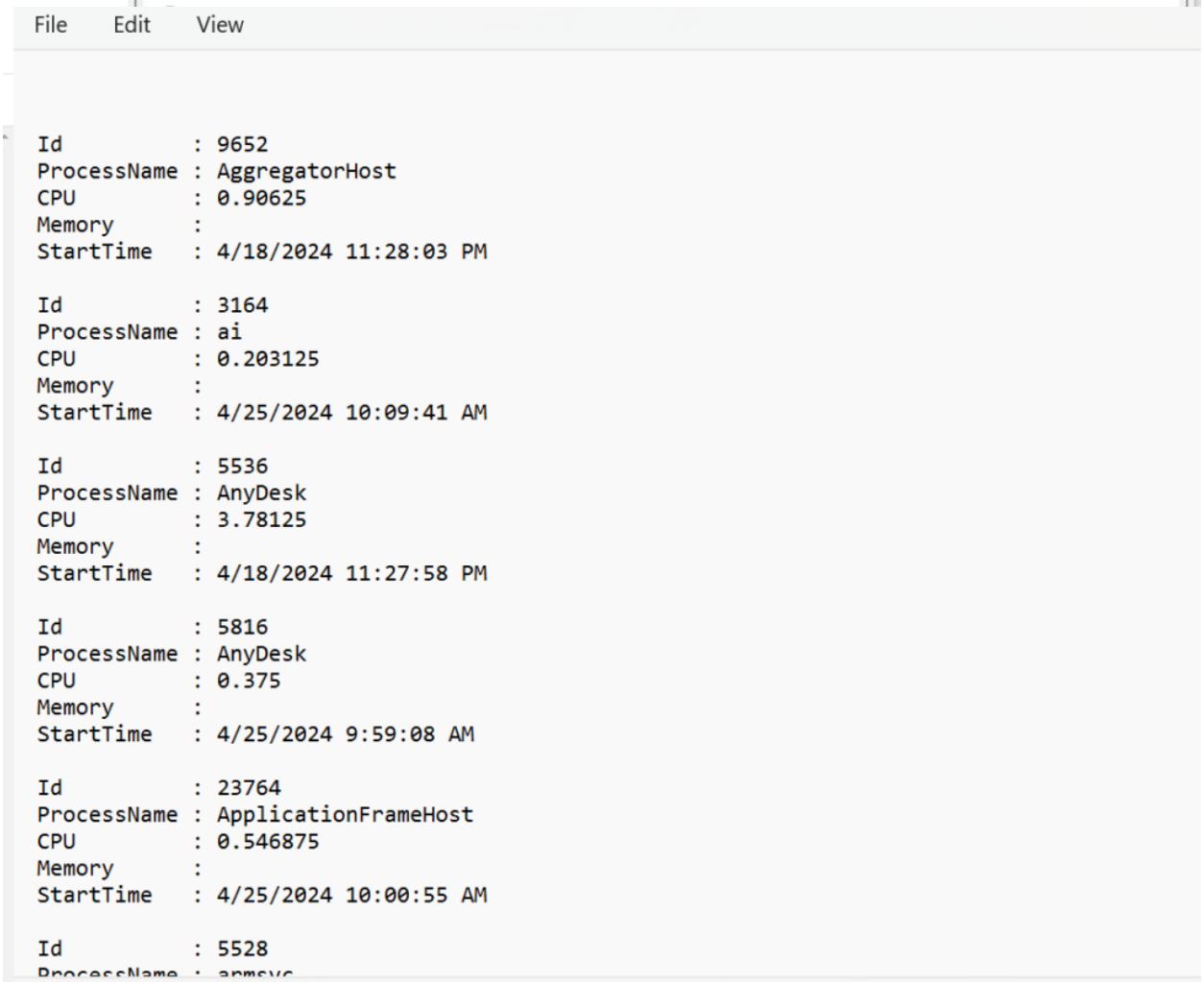


yapılan işlemin tamamlandığını görüyoruz.



İlgili pathe gittiğimizde ilgili dosyaya erişebilirsiniz.





Live Response özelliğinin işlevselliği ve çeşitli amaçlar için çok yönlülüğü hakkında çalışmaları 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 zenginleştirerek kullanabiliriz. İçe aktarılan powershell komutlarında dikkat edilmesi gereken önemli nokta, bu cihazlar üzerinde bilgi toplama amaçlı yapılacak olan komutları içermelidir.

Thanks to Microsoft Learn and jeffreyappel