Microsoft 365

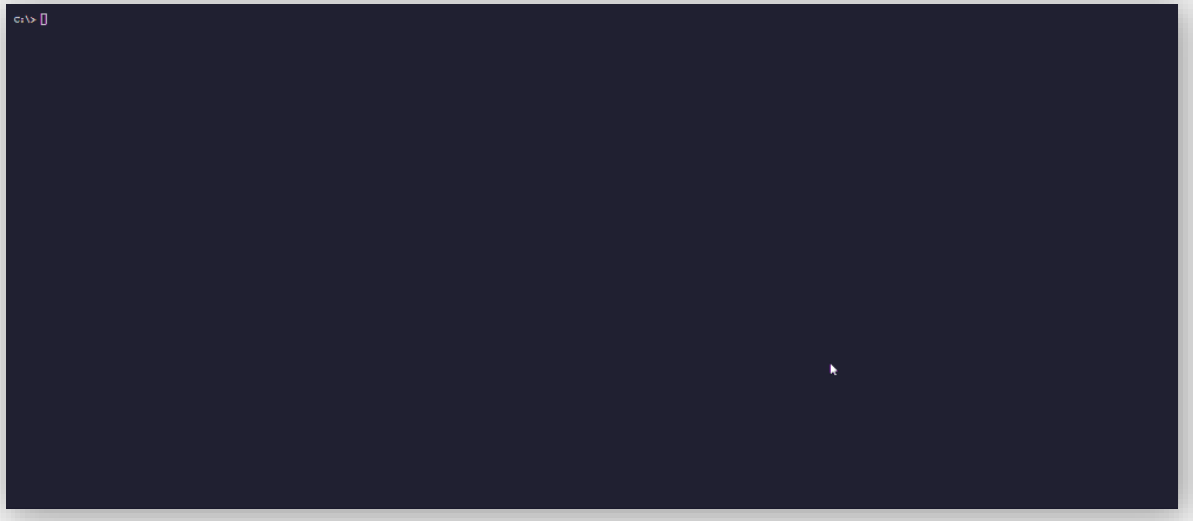
Microsoft Defender for Endpoint

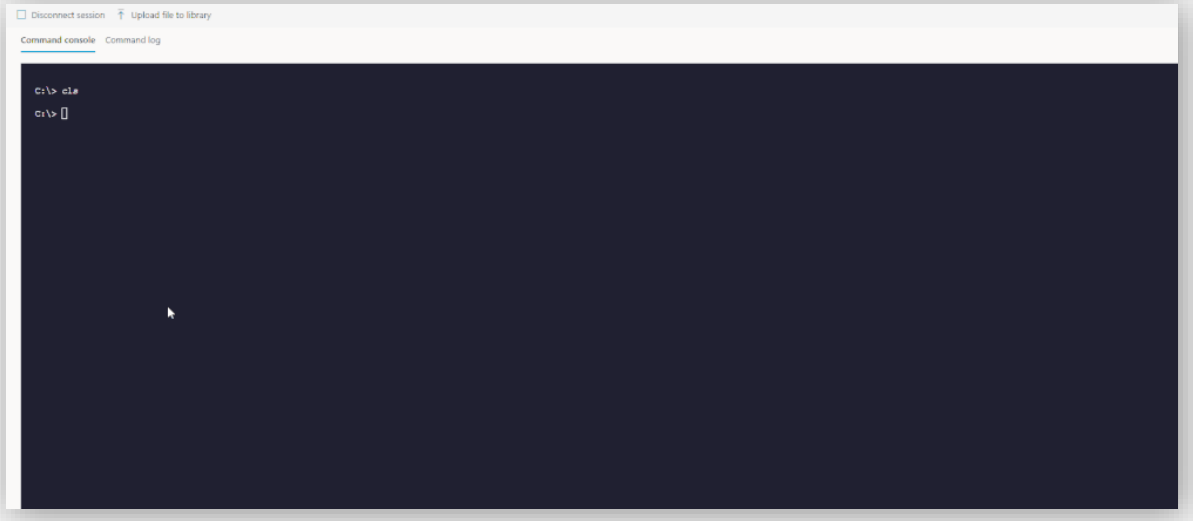
Live Response

Steve Newby
Program Manager
@steve_newby

Live Response

- Real-time live connection to a remote system
- Leverage Microsoft Defender for Endpoint Auto IR library
  - Extended remediation command + easy undo
- Full audit
- Extendable (write your own command, build your own tool)
- RBAC+ Permissions
- Git-Repo (share your tools)





Requirements

- **Verify that you're running a supported version of Windows**.
  - **Windows 10**
    - Version 1909 or later
    - Version 1903 with KB4515384
    - Version 1809 (RS 5) with with KB4537818
    - Version 1803 (RS 4) with KB4537795
    - Version 1709 (RS 3) with KB4537816
  - **Windows Server 2019 - Only applicable for Public preview**
    - Version 1903 or (with KB4515384) later
    - Version 1809 (with KB4537818)
- **Enable live response from the advanced settings page**.
- **Enable live response for servers from the advanced settings page** (recommended).
- **Ensure that the device has an Automation Remediation level assigned to it**.
- **Enable live response unsigned script execution** (optional).
- **Ensure that you have the appropriate permissions**.

Limitations

- Live response sessions are limited to 10 live response sessions at a time.
- Large-scale command execution is not supported.
- Live response session inactive timeout value is 5 minutes.
- A user can only initiate one session at a time.
- A device can only be in one session at a time.
- Live response uses the same channel as AutoIR
- The following file size limits apply:
  - getfile limit: 3 GB
  - fileinfo limit: 10 GB
  - library limit: 250 MB

Useful links

- Investigate entities on devices using live response in Microsoft Defender ATP - Windows security | Microsoft Docs
- anthonws/MDATP_PoSh_Scripts (github.com)
  - This is the memory dump
- YongRhee-MDE/LiveResponse: M365 MDATP Live Response sample scripts (github.com)
  - Numerous scripts that can be used in a Live Response session
- volatilityfoundation/volatility: An advanced memory forensics framework (github.com)
- PowerForensics

Microsoft 365

THANK YOU!