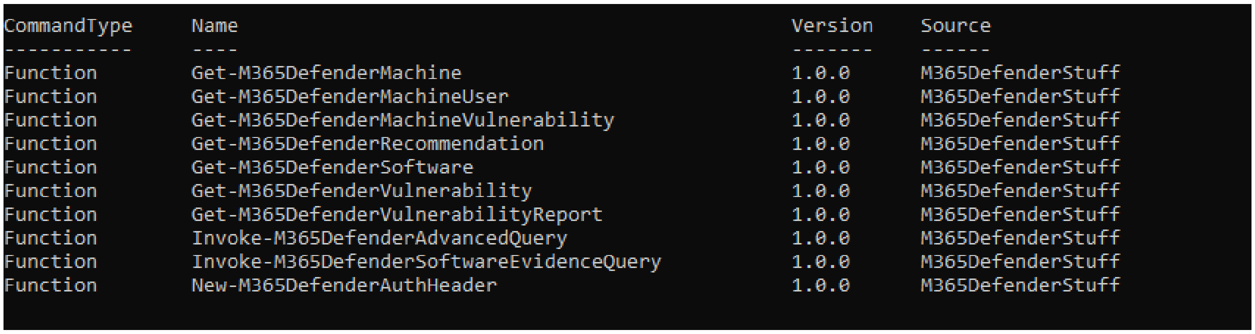
WHAT IS M365DefenderStuff MODULE ?



```
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Get-M365DefenderMachine                            1.0.0      M365DefenderStuff
Function        Get-M365DefenderMachineUser                        1.0.0      M365DefenderStuff
Function        Get-M365DefenderMachineVulnerability               1.0.0      M365DefenderStuff
Function        Get-M365DefenderRecommendation                     1.0.0      M365DefenderStuff
Function        Get-M365DefenderSoftware                           1.0.0      M365DefenderStuff
Function        Get-M365DefenderVulnerability                      1.0.0      M365DefenderStuff
Function        Get-M365DefenderVulnerabilityReport                1.0.0      M365DefenderStuff
Function        Invoke-M365DefenderAdvancedQuery                   1.0.0      M365DefenderStuff
Function        Invoke-M365DefenderSoftwareEvidenceQuery           1.0.0      M365DefenderStuff
Function        New-M365DefenderAuthHeader                         1.0.0      M365DefenderStuff
```

Microsoft continues to enhance XDR capabilities every day. To use this comprehensive security solution more effectively, the M365DefenderStuff module has been developed, providing IT professionals and security managers with essential capabilities. In this article, we'll delve into the capabilities, commands, and outputs of the M365DefenderStuff module.

Capabilities of the M365DefenderStuff Module

1. Threat Detection and Response

M365DefenderStuff enhances the threat detection and response capabilities provided by Microsoft 365 Defender. The module allows you to obtain detailed information about devices and software, helping to identify potential security vulnerabilities. For example, you can examine the security status of devices and detect weaknesses.

2. Advanced Reporting

The module offers comprehensive reporting features. You can generate detailed reports on security incidents, threats, and response actions. These reports can be customized for presentation to managers and stakeholders. Additionally, the module supports the automatic generation and email delivery of reports at specified intervals.

3. Automated Security Operations

M365DefenderStuff helps automate your security operations. For instance, when a specific threat is detected, you can ensure that certain actions are taken automatically. This might include locking user accounts, blocking specific IP addresses, or quarantining certain files.

4. Advanced Analysis

The module enables advanced threat analysis by analyzing data from Microsoft 365 Defender. It helps identify threat vectors, attack patterns, and potential vulnerabilities. These analyses allow you to enhance your security strategies to prevent future attacks.

Install M365DefenderStuff module

To be able to use my PowerShell commands, you must first install the M365DefenderStuff module from the PowerShell Gallery.

```
Install-Module M365DefenderStuff
```

TIP: to get all available commands run the following command in your PowerShell console: `Get-Command -module M365DefenderStuff`

Authenticate

```
Import-Module Az.Accounts
Connect-AzAccount
```

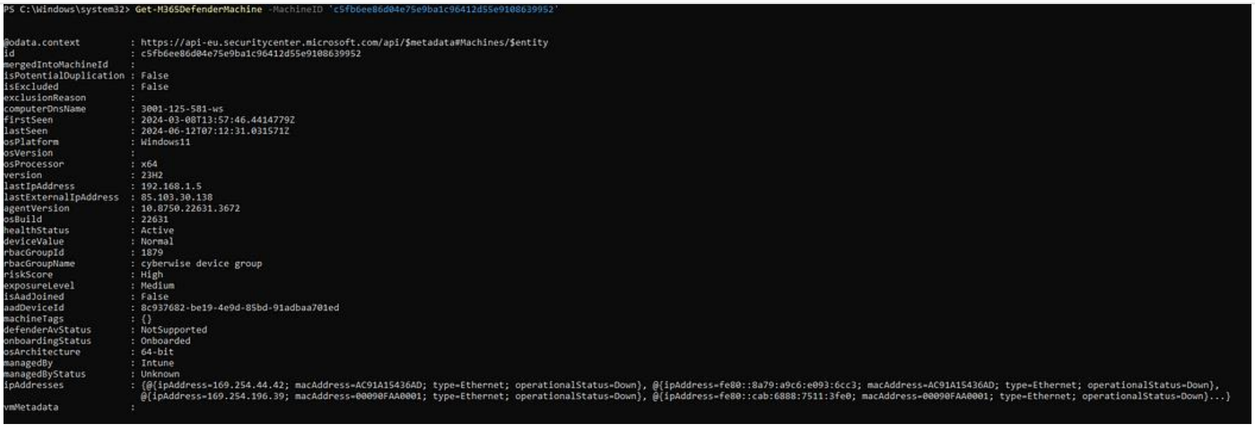
Commands of the M365DefenderStuff Module

The M365DefenderStuff module offers a wide range of commands. Here are the most commonly used commands and their descriptions:

Get-M365DefenderMachine

This command lists all devices registered with Microsoft 365 Defender and provides detailed information about them. You can view the security status and other important details of the devices.

```
Get-M365DefenderMachine

Get-M365DefenderMachine -MachineID 'c5fb6ee86d04e75e9ba1c96412d55e9108639952'
```

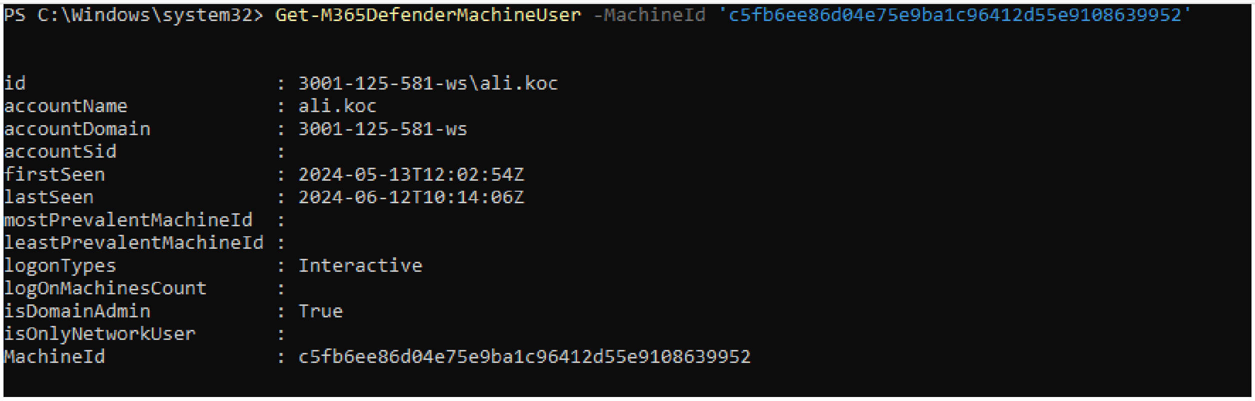


```
PS C:\Windows\system32> Get-M365DefenderMachine -MachineID 'c5fb6ee86d04e75e9ba1c96412d55e9108639952'


@odata.context           : https://api-eu.securitycenter.microsoft.com/api/$metadata#Machines/$entity
id                       : c5fb6ee86d04e75e9ba1c96412d55e9108639952
mergedIntoMachineId      :
isPotentialDuplication   : False
isExcluded               : False
exclusionReason          :
computerDnsName          : 3001-125-581-ws
firstSeen                : 2024-03-08T13:57:46.4414779Z
lastSeen                 : 2024-06-12T07:12:31.031571Z
osPlatform               : Windows11
osVersion                :
osProcessor              : x64
version                  : 23H2
lastIpAddress            : 192.168.1.5
lastExternalIpAddress    : 85.103.30.138
agentVersion             : 10.8750.22631.3672
osBuild                  : 22631
healthStatus             : Active
deviceValue              : Normal
rbacGroupId              : 1879
rbacGroupName            : cyberwise device group
riskScore                : High
exposureLevel            : Medium
isAadJoined              : False
aadDeviceId              : 8c937682-be19-4e9d-85bd-91adbaa701ed
machineTags              : {}
defenderAvStatus         : NotSupported
onboardingStatus         : Onboarded
osArchitecture           : 64-bit
managedBy                : Intune
managedByStatus          : Unknown
ipAddresses              : {@{ipAddress=169.254.44.42; macAddress=AC91A15436AD; type=Ethernet; operationalStatus=Down}, @{ipAddress=fe80::8a79:a9c6:e093:6cc3; macAddress=AC91A15436AD; type=Ethernet; operationalStatus=Down},
                           @{ipAddress=169.254.196.39; macAddress=00090FAA0001; type=Ethernet; operationalStatus=Down}, @{ipAddress=fe80::cab:6888:7511:3fe0; macAddress=00090FAA0001; type=Ethernet; operationalStatus=Down}...}
vmMetadata               :
```

Get-M365DefenderMachineUser

This command provides information about the users who have logged into a specific device. It is useful for tracking which users are logging into which devices.

```
Get-M365DefenderMachineUser -MachineId
'c5fb6ee86d04e75e9ba1c96412d55e9108639952'
```

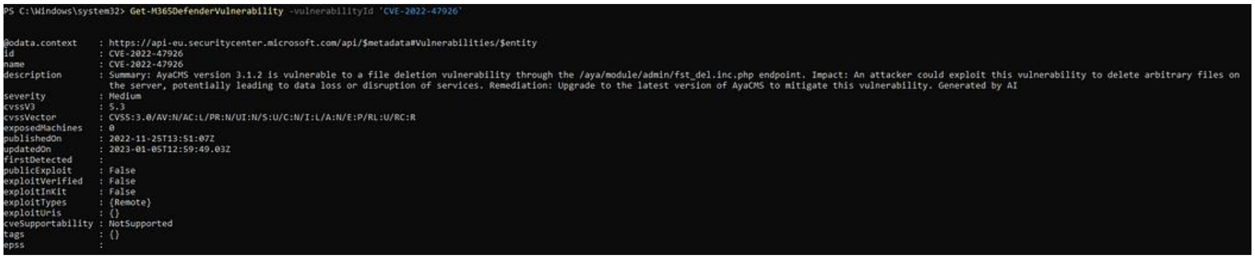


```
PS C:\Windows\system32> Get-M365DefenderMachineUser -MachineId 'c5fb6ee86d04e75e9ba1c96412d55e9108639952'


id                       : 3001-125-581-ws\ali.koc
accountName              : ali.koc
accountDomain            : 3001-125-581-ws
accountSid               :
firstSeen                : 2024-05-13T12:02:54Z
lastSeen                 : 2024-06-12T10:14:06Z
mostPrevalentMachineId   :
leastPrevalentMachineId  :
logonTypes               : Interactive
logOnMachinesCount       :
isDomainAdmin            : True
isOnlyNetworkUser        :
MachineId                : c5fb6ee86d04e75e9ba1c96412d55e9108639952
```

Get-M365DefenderMachineVulnerability

This command lists the security vulnerabilities on a specific device. You can determine the weaknesses of the device and take necessary measures.

```
# get all found vulnerabilities (can take several minutes to complete!)
Get-M365DefenderVulnerability

# get details of specific vulnerability
Get-M365DefenderVulnerability -vulnerabilityId
'c5fb6ee86d04e75e9ba1c96412d55e9108639952'
```

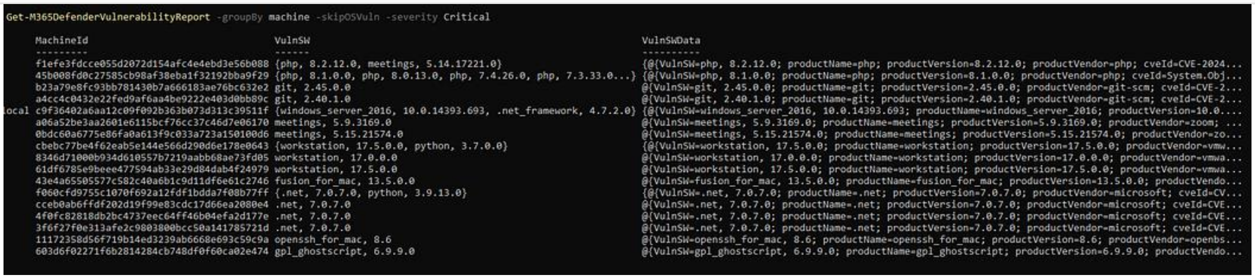


```
PS C:\Windows\system32> Get-M365DefenderVulnerability -vulnerabilityId 'CVE-2022-47926'

@odata.context    : https://api-eu.securitycenter.microsoft.com/api/$metadata#Vulnerabilities/$entity
id                : CVE-2022-47926
name              : CVE-2022-47926
description       : Summary: AyaCMS version 3.1.2 is vulnerable to a file deletion vulnerability through the /aya/module/admin/fst_del.inc.php endpoint. Impact: An attacker could exploit this vulnerability to delete arbitrary files on
                    the server, potentially leading to data loss or disruption of services. Remediation: Upgrade to the latest version of AyaCMS to mitigate this vulnerability. Generated by AI
severity          : Medium
cvssV3            : 5.3
cvssVector        : CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:U/RC:R
exposedMachines   : 0
publishedOn       : 2022-11-25T13:51:07Z
updatedOn         : 2023-01-05T12:59:49.03Z
firstDetected     :
publicExploit     : False
exploitVerified   : False
exploitInKit      : False
exploitTypes      : {Remote}
exploitUris       : {}
cveSupportability : NotSupported
tags              : {}
epss              :
```

Generate vulnerability report

This command generates a detailed report on security vulnerabilities. The report includes details of the weaknesses and recommended actions to mitigate them.

```
# get just software vulnerabilities of CTRITICAL type and group them by
machine
Get-M365DefenderVulnerabilityReport -groupBy machine -skipOSVuln -severity
Critical
```



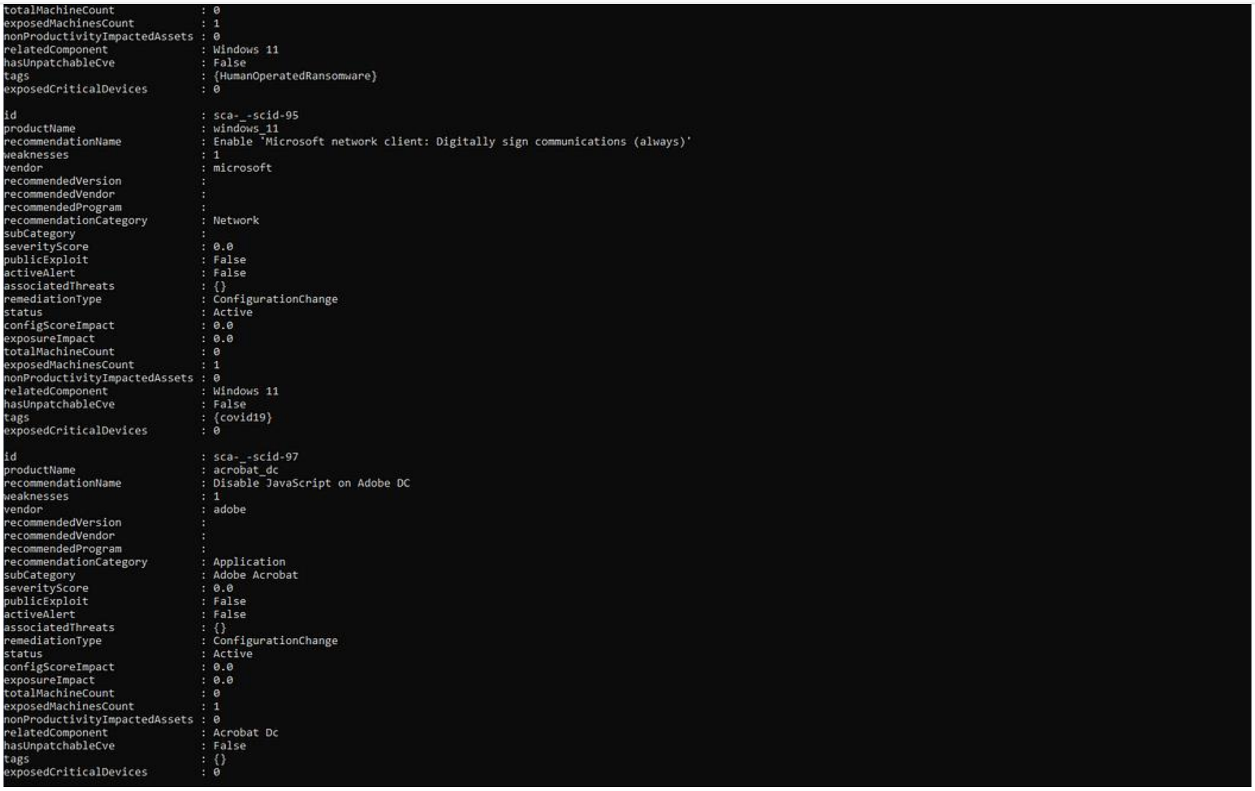
```
Get-M365DefenderVulnerabilityReport -groupBy machine -skipOSVuln -severity Critical

     MachineId                                VulnSW                                                         VulnSWData
     ---------                                ------                                                         ----------
     f1efe3fdcce055d2072d154afc4e4ebd3e56b088 {php, 8.2.12.0, meetings, 5.14.17221.0}                        {@{VulnSW=php, 8.2.12.0; productName=php; productVersion=8.2.12.0; productVendor=php; cveId=CVE-2024...
     45b008fd0c27585cb98af38eba1f32192bba9f29 {php, 8.1.0.0, php, 8.0.13.0, php, 7.4.26.0, php, 7.3.33.0...} {@{VulnSW=php, 8.1.0.0; productName=php; productVersion=8.1.0.0; productVendor=php; cveId=System.Obj...
     b23a79e8fc93bb781430b7a666183ae76bc632e2 git, 2.45.0.0                                                  @{VulnSW=git, 2.45.0.0; productName=git; productVersion=2.45.0.0; productVendor=git-scm; cveId=CVE-2...
     a4cc4c0432e22fed9af6aa4be9222e403d0bb89c git, 2.40.1.0                                                  @{VulnSW=git, 2.40.1.0; productName=git; productVersion=2.40.1.0; productVendor=git-scm; cveId=CVE-2...
local c9f36402a6aa12c09f092b363b073d313c39511f {windows_server_2016, 10.0.14393.693, .net_framework, 4.7.2.0} {@{VulnSW=windows_server_2016, 10.0.14393.693; productName=windows_server_2016; productVersion=10.0....
     a06a52be3aa2601e6115bcf76cc37c46d7e06170 meetings, 5.9.3169.0                                           @{VulnSW=meetings, 5.9.3169.0; productName=meetings; productVersion=5.9.3169.0; productVendor=zoom; ...
     0bdc60a6775e86fa0a613f9c033a723a150100d6 meetings, 5.15.21574.0                                         @{VulnSW=meetings, 5.15.21574.0; productName=meetings; productVersion=5.15.21574.0; productVendor=zo...
     cbebc77be4f62eab5e144e566d290d6e178e0643 {workstation, 17.5.0.0, python, 3.7.0.0}                       {@{VulnSW=workstation, 17.5.0.0; productName=workstation; productVersion=17.5.0.0; productVendor=vmw...
     8346d71000b934d610557b7219aabb68ae73fd05 workstation, 17.0.0.0                                          @{VulnSW=workstation, 17.0.0.0; productName=workstation; productVersion=17.0.0.0; productVendor=vmwa...
     61df6785e9beee477594ab33e29d84dab4f24979 workstation, 17.5.0.0                                          @{VulnSW=workstation, 17.5.0.0; productName=workstation; productVersion=17.5.0.0; productVendor=vmwa...
     43e4a65505577c582c40a6b1c9d11df6e61c2746 fusion_for_mac, 13.5.0.0                                       @{VulnSW=fusion_for_mac, 13.5.0.0; productName=fusion_for_mac; productVersion=13.5.0.0; productVendo...
     f060cfd9755c1070f692a12fdf1bdda7f08b77ff {.net, 7.0.7.0, python, 3.9.13.0}                              {@{VulnSW=.net, 7.0.7.0; productName=.net; productVersion=7.0.7.0; productVendor=microsoft; cveId=CV...
     cceb0ab6ffdf202d19f99e83cdc17d66ea2080e4 .net, 7.0.7.0                                                  @{VulnSW=.net, 7.0.7.0; productName=.net; productVersion=7.0.7.0; productVendor=microsoft; cveId=CVE...
     4f0fc82818db2bc4737eec64ff46b04efa2d177e .net, 7.0.7.0                                                  @{VulnSW=.net, 7.0.7.0; productName=.net; productVersion=7.0.7.0; productVendor=microsoft; cveId=CVE...
     3f6f27f0e313afe2c9803800bcc50a141785721d .net, 7.0.7.0                                                  @{VulnSW=.net, 7.0.7.0; productName=.net; productVersion=7.0.7.0; productVendor=microsoft; cveId=CVE...
     11172358d56f719b14ed3239ab6668e693c59c9a openssh_for_mac, 8.6                                           @{VulnSW=openssh_for_mac, 8.6; productName=openssh_for_mac; productVersion=8.6; productVendor=openbs...
     603d6f02271f6b2814284cb748df0f60ca02e474 gpl_ghostscript, 6.9.9.0                                       @{VulnSW=gpl_ghostscript, 6.9.9.0; productName=gpl_ghostscript; productVersion=6.9.9.0; productVendo...
```

Get-M365DefenderRecommendation

This command provides recommendations to improve security status and mitigate threats. You can view the security advice provided by Microsoft 365 Defender.

```
# get all security recommendations
Get-M365DefenderRecommendation

# get security recommendations just for Putty software.
Get-M365DefenderRecommendation -productName 'putty'
```

```
# get all security recommendations for given machine.
Get-M365DefenderRecommendation -machineId
'c5fb6ee86d04e75e9ba1c96412d55e9108639952'
```

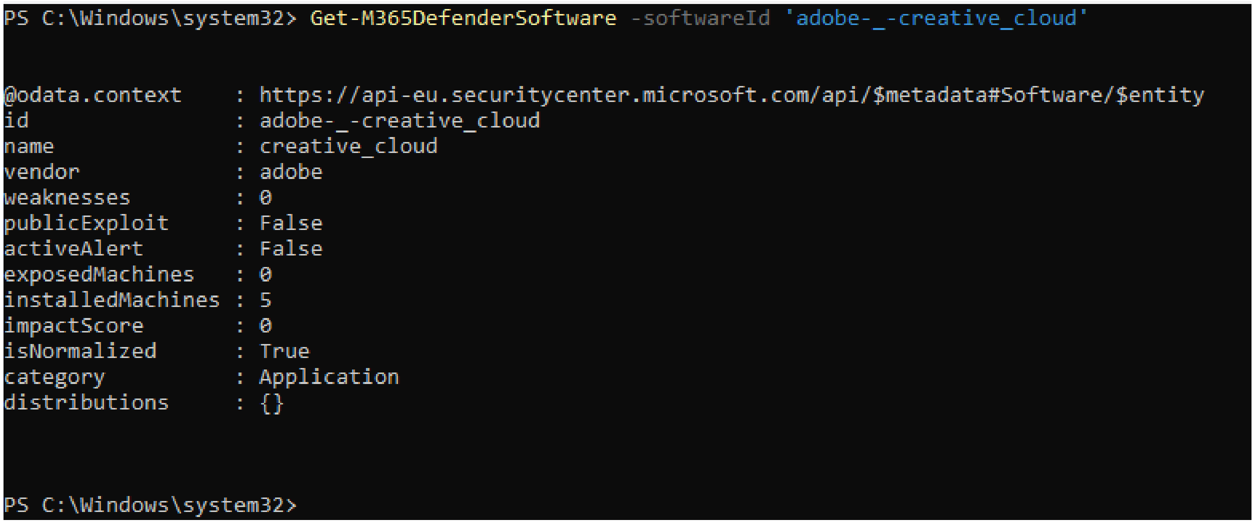


```
totalMachineCount            : 0
exposedMachinesCount         : 1
nonProductivityImpactedAssets : 0
relatedComponent             : Windows 11
hasUnpatchableCve            : False
tags                         : {HumanOperatedRansomware}
exposedCriticalDevices       : 0

id                           : sca-_-scid-95
productName                  : windows_11
recommendationName           : Enable 'Microsoft network client: Digitally sign communications (always)'
weaknesses                   : 1
vendor                       : microsoft
recommendedVersion           :
recommendedVendor            :
recommendedProgram           :
recommendationCategory       : Network
subCategory                  :
severityScore                : 0.0
publicExploit                : False
activeAlert                  : False
associatedThreats            : {}
remediationType              : ConfigurationChange
status                       : Active
configScoreImpact            : 0.0
exposureImpact               : 0.0
totalMachineCount            : 0
exposedMachinesCount         : 1
nonProductivityImpactedAssets : 0
relatedComponent             : Windows 11
hasUnpatchableCve            : False
tags                         : {covid19}
exposedCriticalDevices       : 0

id                           : sca-_-scid-97
productName                  : acrobat_dc
recommendationName           : Disable JavaScript on Adobe DC
weaknesses                   : 1
vendor                       : adobe
recommendedVersion           :
recommendedVendor            :
recommendedProgram           :
recommendationCategory       : Application
subCategory                  : Adobe Acrobat
severityScore                : 0.0
publicExploit                : False
activeAlert                  : False
associatedThreats            : {}
remediationType              : ConfigurationChange
status                       : Active
configScoreImpact            : 0.0
exposureImpact               : 0.0
totalMachineCount            : 0
exposedMachinesCount         : 1
nonProductivityImpactedAssets : 0
relatedComponent             : Acrobat Dc
hasUnpatchableCve            : False
tags                         : {}
exposedCriticalDevices       : 0
```

Get-M365DefenderSoftware

This command provides information about the software installed on devices. You can examine which software is installed and its security status.

```
# get all detected applications
Get-M365DefenderSoftware

# get just specific application
Get-M365DefenderSoftware -softwareId 'adobe-_-creative_cloud'
```



```
PS C:\Windows\system32> Get-M365DefenderSoftware -softwareId 'adobe-_-creative_cloud'


@odata.context    : https://api-eu.securitycenter.microsoft.com/api/$metadata#Software/$entity
id                : adobe-_-creative_cloud
name              : creative_cloud
vendor            : adobe
weaknesses        : 0
publicExploit     : False
activeAlert       : False
exposedMachines   : 0
installedMachines : 5
impactScore       : 0
isNormalized      : True
category          : Application
distributions     : {}



PS C:\Windows\system32>
```

Invoke-M365DefenderAdvancedQuery

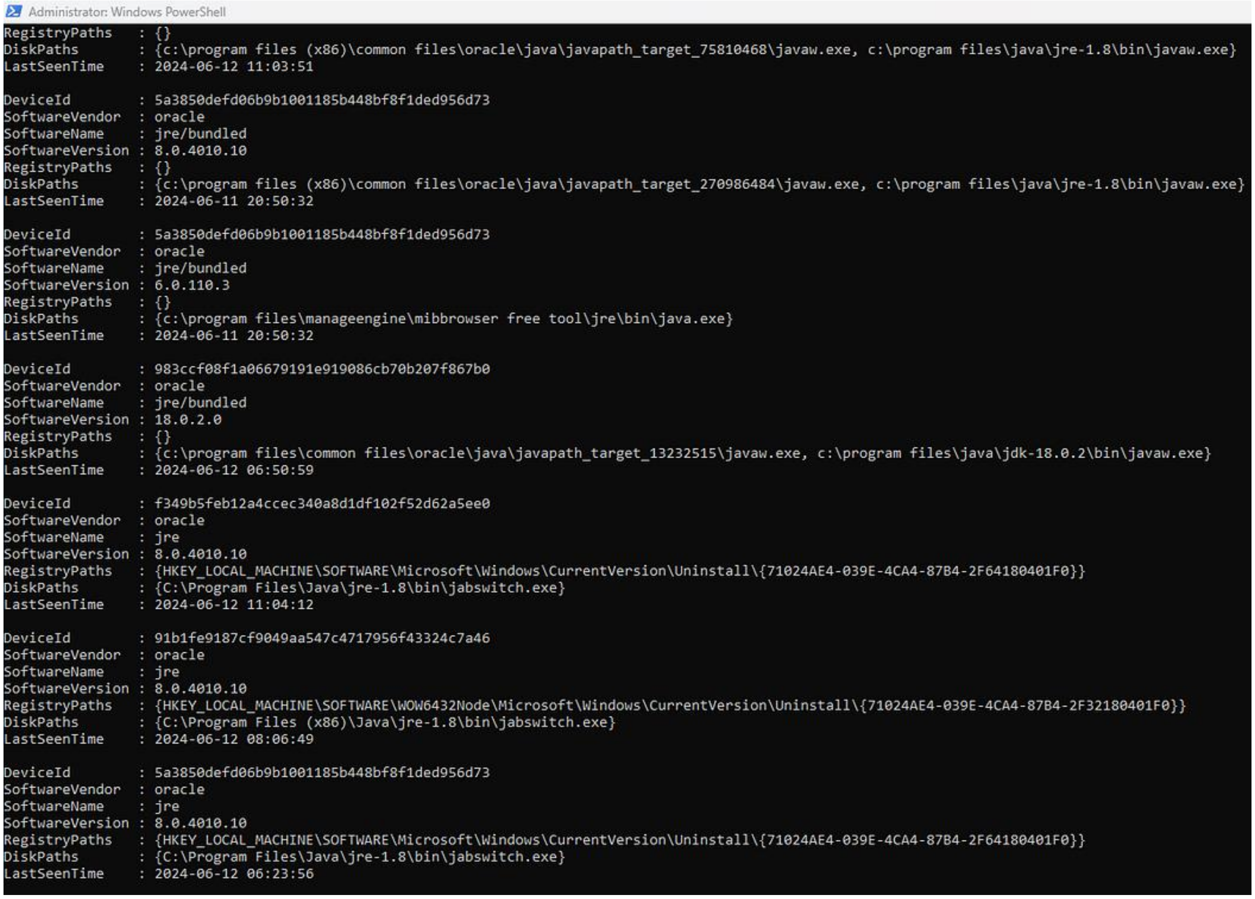
This command allows you to perform advanced queries in the Microsoft 365 Defender database. You can conduct detailed searches and analyses based on specific criteria.

```
Invoke-M365DefenderAdvancedQuery -Query "DeviceEvents | where Timestamp >
ago(7d)"
```

Invoke-M365DefenderSoftwareEvidenceQuery

This command allows you to query evidence and details related to specific software. You can evaluate the security status and potential threats of the software.

```
Invoke-M365DefenderSoftwareEvidenceQuery -appName JRE
```



```
RegistryPaths   : {}
DiskPaths       : {c:\program files (x86)\common files\oracle\java\javapath_target_75810468\javaw.exe, c:\program files\java\jre-1.8\bin\javaw.exe}
LastSeenTime    : 2024-06-12 11:03:51

DeviceId        : 5a3850defd06b9b1001185b448bf8f1ded956d73
SoftwareVendor  : oracle
SoftwareName    : jre/bundled
SoftwareVersion : 8.0.4010.10
RegistryPaths   : {}
DiskPaths       : {c:\program files (x86)\common files\oracle\java\javapath_target_270986484\javaw.exe, c:\program files\java\jre-1.8\bin\javaw.exe}
LastSeenTime    : 2024-06-11 20:50:32

DeviceId        : 5a3850defd06b9b1001185b448bf8f1ded956d73
SoftwareVendor  : oracle
SoftwareName    : jre/bundled
SoftwareVersion : 6.0.110.3
RegistryPaths   : {}
DiskPaths       : {c:\program files\manageengine\mibbrowser free tool\jre\bin\java.exe}
LastSeenTime    : 2024-06-11 20:50:32

DeviceId        : 983ccf08f1a06679191e919086cb70b207f867b0
SoftwareVendor  : oracle
SoftwareName    : jre/bundled
SoftwareVersion : 18.0.2.0
RegistryPaths   : {}
DiskPaths       : {c:\program files\common files\oracle\java\javapath_target_13232515\javaw.exe, c:\program files\java\jdk-18.0.2\bin\javaw.exe}
LastSeenTime    : 2024-06-12 06:50:59

DeviceId        : f349b5feb12a4ccec340a8d1df102f52d62a5ee0
SoftwareVendor  : oracle
SoftwareName    : jre
SoftwareVersion : 8.0.4010.10
RegistryPaths   : {HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{71024AE4-039E-4CA4-87B4-2F64180401F0}}
DiskPaths       : {C:\Program Files\Java\jre-1.8\bin\jabswitch.exe}
LastSeenTime    : 2024-06-12 11:04:12

DeviceId        : 91b1fe9187cf9049aa547c4717956f43324c7a46
SoftwareVendor  : oracle
SoftwareName    : jre
SoftwareVersion : 8.0.4010.10
RegistryPaths   : {HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{71024AE4-039E-4CA4-87B4-2F32180401F0}}
DiskPaths       : {C:\Program Files (x86)\Java\jre-1.8\bin\jabswitch.exe}
LastSeenTime    : 2024-06-12 08:06:49

DeviceId        : 5a3850defd06b9b1001185b448bf8f1ded956d73
SoftwareVendor  : oracle
SoftwareName    : jre
SoftwareVersion : 8.0.4010.10
RegistryPaths   : {HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{71024AE4-039E-4CA4-87B4-2F64180401F0}}
DiskPaths       : {C:\Program Files\Java\jre-1.8\bin\jabswitch.exe}
LastSeenTime    : 2024-06-12 06:23:56
```

New-M365DefenderAuthHeader

This command creates the necessary authentication headers for communicating with Microsoft 365 Defender APIs. It ensures authentication in your API calls.

```
New-M365DefenderAuthHeader -ClientId "YourClientId" -ClientSecret
"YourClientSecret" -TenantId "YourTenantId"
```

Outputs of the M365DefenderStuff Module

The M365DefenderStuff module generates various outputs that help improve your security operations:

1. **Threat Reports:** Detailed reports on security incidents, providing information on the type, source, affected systems, and actions taken.
2. **Security Dashboard:** Real-time security dashboards displaying all security threats and incidents on a single screen.
3. **Automated Alerts:** The module sends immediate alerts when specific threats or anomalies are detected. These alerts can be delivered via email, SMS, or other communication channels.
4. **Analysis Reports:** Advanced analysis reports providing in-depth information on attack vectors, vulnerabilities, and preventive measures.
5. **Incident Response Reports:** Detailed reports on all actions taken during the incident response process and the outcomes of those actions.

Conclusion

The M365DefenderStuff module extends the capabilities of Microsoft 365 Defender, helping organizations protect more effectively against cyber threats. With advanced reporting, automated security operations, and detailed analyses, IT and security teams can adopt a more proactive approach. By using this module, you can enhance your organization’s security posture and respond more quickly and effectively to potential threats.

thanks to Doitpshway