Managing the Microsoft Security stack with **PowerShell**

Alex Verboon

Alex Verboon

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Session Objectives

- Provide an overview of the various Microsoft Security Solutions and how you can interact with them using PowerShell
  - Windows Defender
  - Microsoft Defender Advanced Threat Protection
  - Microsoft Defender Exploit Guard
  - Microsoft Cloud App Security
  - Microsoft Office 365 Advanced Threat Protection
  - AzureAD Multifactor Authentication
- References and examples of useful PowerShell scripts / modules

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Microsoft Threat Experts | Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt | MSSP | Cloud App Security | Azure Security Center | Microsoft Defender | Office 365 | Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Identity & Access

Azure Active Directory

- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Classification Labels

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score | Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene
Just in Time VM Access
Adaptive App Control

Extranet

NGFW
Edge DLP
SSL Proxy
IPS/IDS

Azure Firewall

Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs | Azure Stack | VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

Network protection
Credential protection
Exploit protection
Reputation analysis
Full Disk Encryption
Attack surface reduction

App control
Isolation
Antivirus
Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT | Azure IoT Security | Azure Sphere

IoT Security Maturity Model
IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

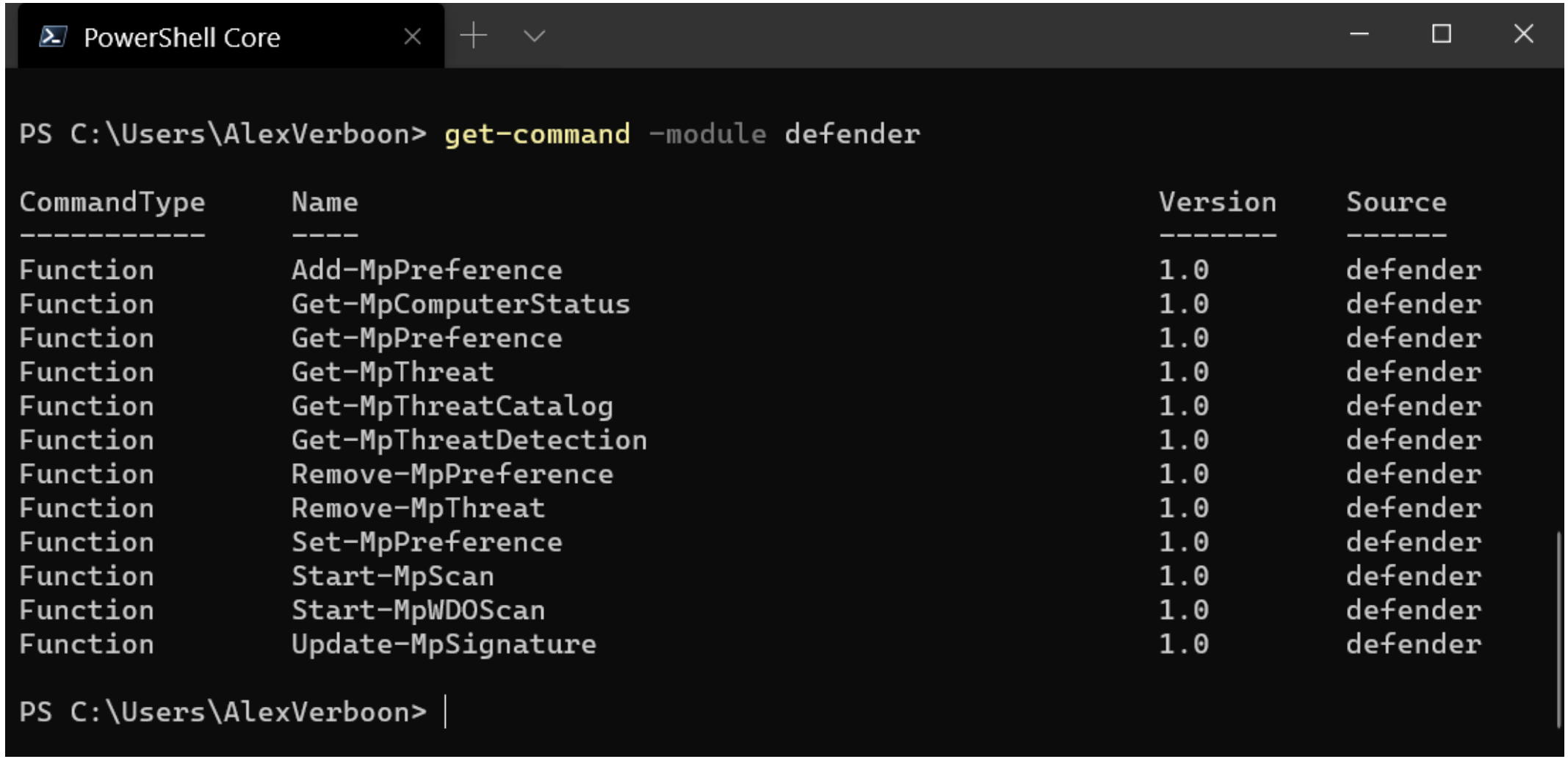
Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft

Windows Defender

Windows Defender is installed by default on Windows 10 / Server 2016/2019



Managing the Microsoft Security stack with PowerShell – Windows Defender

PowerShell Core

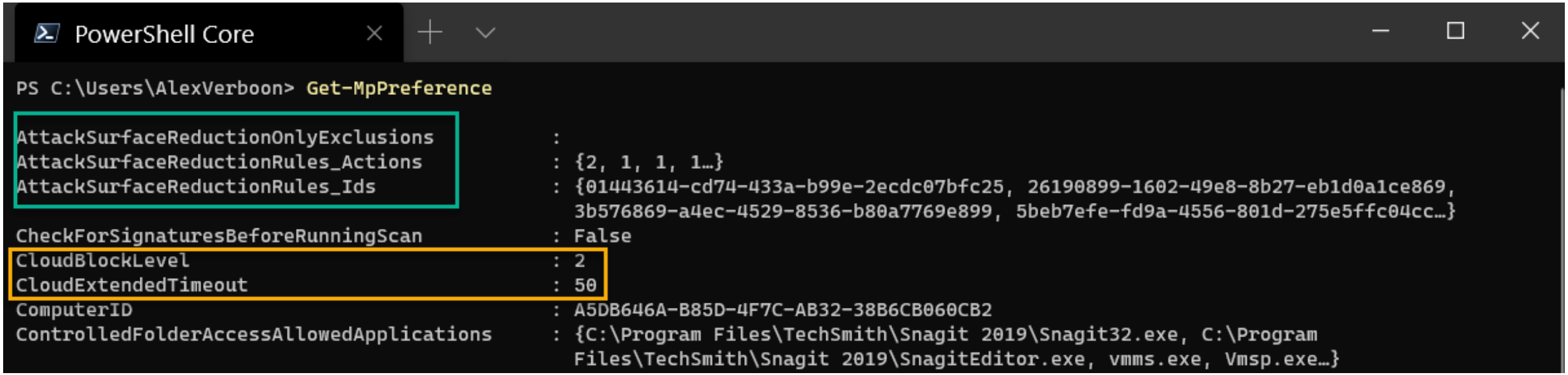
```
PS C:\Users\AlexVerboon> Get-MpComputerStatus

AMEngineVersion                 : 1.1.17300.4
AMProductVersion                : 4.18.2006.10
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2006.10
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 8/1/2020 8:18:36 AM
AntispywareSignatureVersion     : 1.321.346.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 8/1/2020 8:18:36 AM
AntivirusSignatureVersion       : 1.321.346.0
BehaviorMonitorEnabled          : True
ComputerID                      : A5DB646A-B85D-4F7C-AB32-38B6CB060CB2
ComputerState                   : 0
FullScanAge                     : 178
FullScanEndTime                 : 2/4/2020 3:26:33 PM
FullScanStartTime               : 2/4/2020 3:18:01 PM
IoavProtectionEnabled           : True
IsTamperProtected               : True
IsVirtualMachine                : False
LastFullScanSource              : 1
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 1.1.17300.4
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 8/1/2020 8:18:36 AM
NISSignatureVersion             : 1.321.346.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 9
QuickScanEndTime                : 7/23/2020 5:21:13 AM
QuickScanStartTime              : 7/23/2020 5:18:41 AM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
PSComputerName                  :
```

Use **Get-MpComputerStatus** to get an overview of installed versions and signature updates

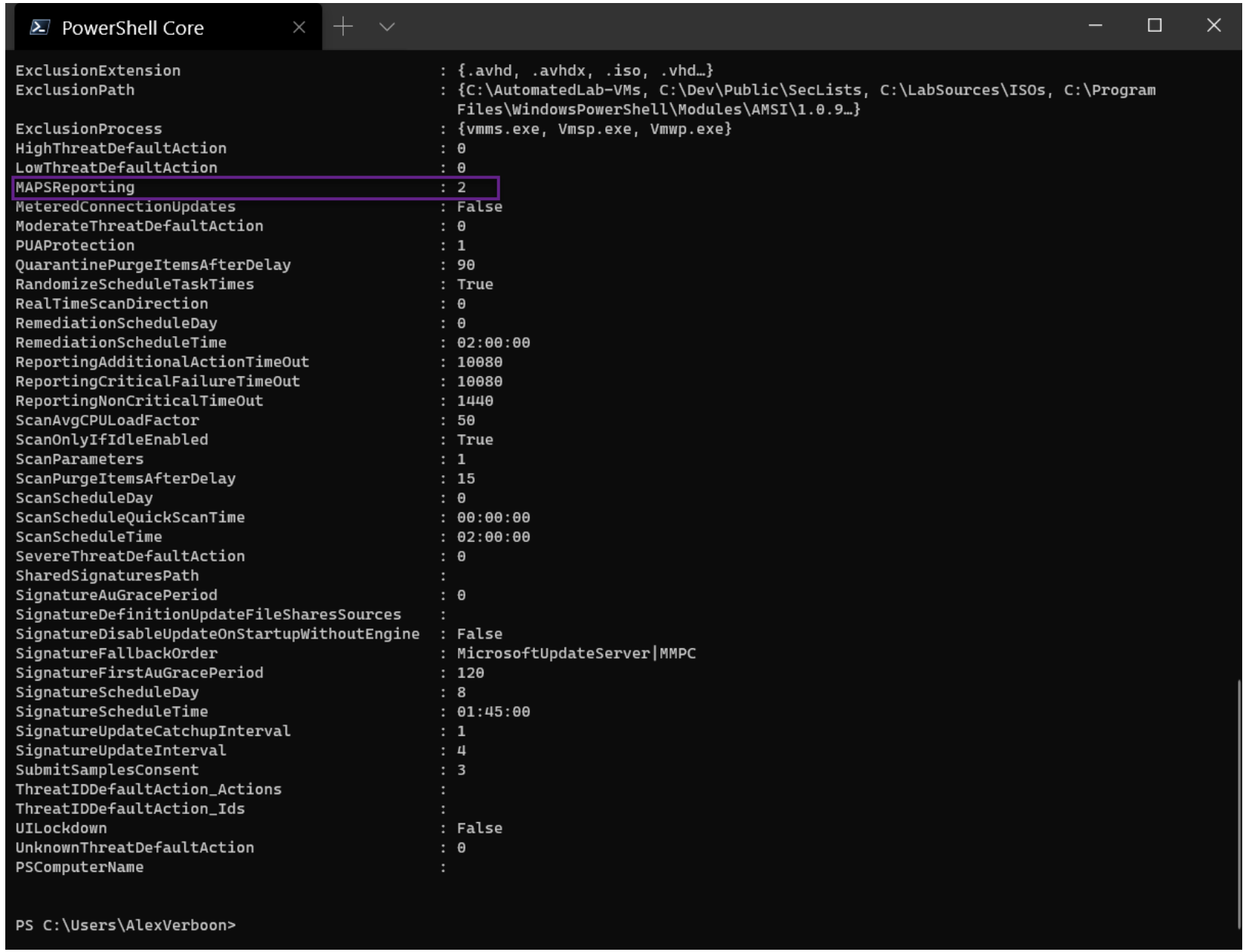
PowerShell Core

```
PS C:\Users\AlexVerboon> $LastFullScanSource = @{
>>   Name = 'LastFullScanSource'
>>   Expression = {
>>     # property is an array, so process all values
>>     $value = $_.LastFullScanSource
>>
>>     switch([int]$value)
>>       {
>>         0          {'Unknown'}
>>         1          {'User'}
>>         2          {'System'}
>>         3          {'Real-time'}
>>         4          {'IOAV'}
>>         default    {"$value"}
>>       }
>>
>>   }
>> }
PS C:\Users\AlexVerboon> Get-CimInstance -ClassName MSFT_MpComputerStatus -Namespac
e root/microsoft/windows/defender | Select-Object -Property Caption, $LastFullScanS
ource

Caption LastFullScanSource
------- ------------------
        User

PS C:\Users\AlexVerboon>
```

Use **Get-MpPreference** to look at Windows Defender configuration settings



Managing the Microsoft Security stack with PowerShell – Windows Defender



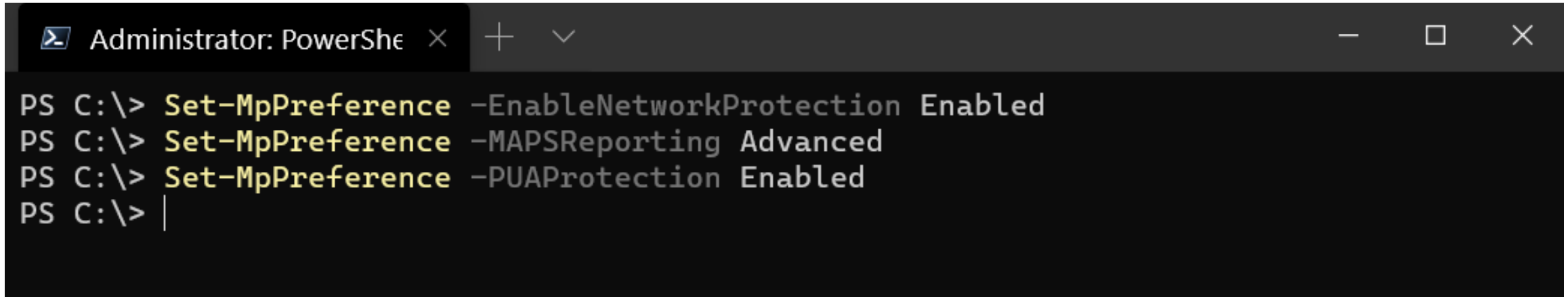
Get-MpComputerStatus uses MSF**T_MpComputerStatus**

```
PowerShell Core

PS C:\Users\AlexVerboon> Get-CimInstance -ClassName MSFT_MpComputerStatus -Namespace root/microsoft/windows/defender -Property *
```

https://powershell.one/wmi/root/microsoft/windows/defender/msft_mpcomputerstatus

```
#>

$RealTimeScanDirection = @{
  Name = 'RealTimeScanDirection'
  Expression = {
    # property is an array, so process all values
    $value = $_.RealTimeScanDirection

    switch([int]$value)
      {
        0          {'Both'}
        1          {'Incoming'}
        2          {'Outcoming'}
        default    {"$value"}
      }

  }
}
#endregion define calculated property

# retrieve all instances...
Get-CimInstance -ClassName MSFT_MpComputerStatus -Namespace root/microsoft/windows/defender |
  # ...and output properties "Caption" and "RealTimeScanDirection". The latter is defined
  # by the hashtable in $RealTimeScanDirection:
  Select-Object -Property Caption, $RealTimeScanDirection
```

Use **Set-MpPreference** to configure Windows Defender use **Add-MpPreference** to extend settings such as Exclusion paths



Mpcmdrun.exe provides an option to verify exclusions, **validate-Defenderexclusions** is a wrapper script I created for the use with PowerShell https://gist.github.com/alexverboon/b82348b4bce58092bef45c96d985a709

```
cmd

-CheckExclusion -path <path>
      Checks whether <path> is excluded. It can be either a path, or a file.
```

```
Administrator: PowerShe

PS C:\Dev\Alex\MSSecurityPowerShell\DefenderAV> . .\Validate-DefenderExclusoins.ps1
PS C:\Dev\Alex\MSSecurityPowerShell\DefenderAV> Validate-DefenderExclusion -Path C:\AutomatedLab-VMs\
C:\AutomatedLab-VMs\ [\Device\HarddiskVolume3\AutomatedLab-VMs] is excluded. Exit code is 0.

Path                 Excluded
----                 --------
C:\AutomatedLab-VMs\ True

PS C:\Dev\Alex\MSSecurityPowerShell\DefenderAV> Validate-DefenderExclusion -Path C:\temp\demo\
C:\temp\demo\ [\Device\HarddiskVolume3\temp\demo] is excluded. Exit code is 0.

Path          Excluded
----          --------
C:\temp\demo\ True

PS C:\Dev\Alex\MSSecurityPowerShell\DefenderAV> Validate-DefenderExclusion -Path C:\temp\
C:\temp\ [\Device\HarddiskVolume3\temp] is not excluded. Exit code is 1.

Path     Excluded
----     --------
C:\temp\ False

PS C:\Dev\Alex\MSSecurityPowerShell\DefenderAV>
```

Get a list of all possible Windows event IDs for Windows Defender

```
(Get-WinEvent -ListProvider "Microsoft-Windows-Windows Defender").Events | format-table id,Description -AutoSize
```

PowerShell Core

```
PS C:\> (Get-WinEvent -ListProvider "Microsoft-Windows-Windows Defender").events | Format-Table id, description -AutoSize

  Id Description
  -- -----------
 101 Windows Defender Antivirus state updated to %1.
1000 %1 scan has started.…
1001 %1 scan has finished.…
1002 %1 scan has been stopped before completion.…
1003 %1 scan has been paused.…
1004 %1 scan has resumed.…
1005 %1 scan has encountered an error and terminated.…
1006 %1 has detected malware or other potentially unwanted software.…
1007 %1 has taken action to protect this machine from malware or other potentially unwanted software.…
1008 %1 has encountered an error when taking action on malware or other potentially unwanted software.…
1009 %1 has restored an item from quarantine.…
1010 %1 has encountered an error trying to restore an item from quarantine.…
1011 %1 has deleted an item from quarantine.…
1012 %1 has encountered an error trying to delete an item from quarantine.…
1013 %1 has removed history of malware and other potentially unwanted software.…
1014 %1 has encountered an error trying to remove history of malware and other potentially unwanted software.…
1015 %1 has detected a suspicious behavior.…
1116 %1 has detected malware or other potentially unwanted software.…
1117 %1 has taken action to protect this machine from malware or other potentially unwanted software.…
1118 %1 has encountered a non-critical error when taking action on malware or other potentially unwanted software.…
1119 %1 has encountered a critical error when taking action on malware or other potentially unwanted software.…
```

Find specific Event IDs

PowerShell Core

```
PS C:\>
PS C:\> $EventFilter = @{
>>     ID = 1000,1001
>>     ProviderName = "Microsoft-Windows-Windows Defender"
>> }
PS C:\> Get-WinEvent -FilterHashtable $EventFilter | format-table -autosize


   ProviderName: Microsoft-Windows-Windows Defender

TimeCreated             Id LevelDisplayName Message
-----------             -- ---------------- -------
7/23/2020 5:21:13 AM 1001 Information      Windows Defender Antivirus scan has finished.…
7/23/2020 5:18:41 AM 1000 Information      Windows Defender Antivirus scan has started.…

PS C:\>
```

Windows Defender Exploit Guard Network Protection, Attack Surface Reduction and Controlled Folder Access events are written to the Windows Event log: Microsoft-Windows-Windows Defender

#Controlled Folder Access
1124 Audit
1123 Block

Network Protection
1125 Audit
1126 Block

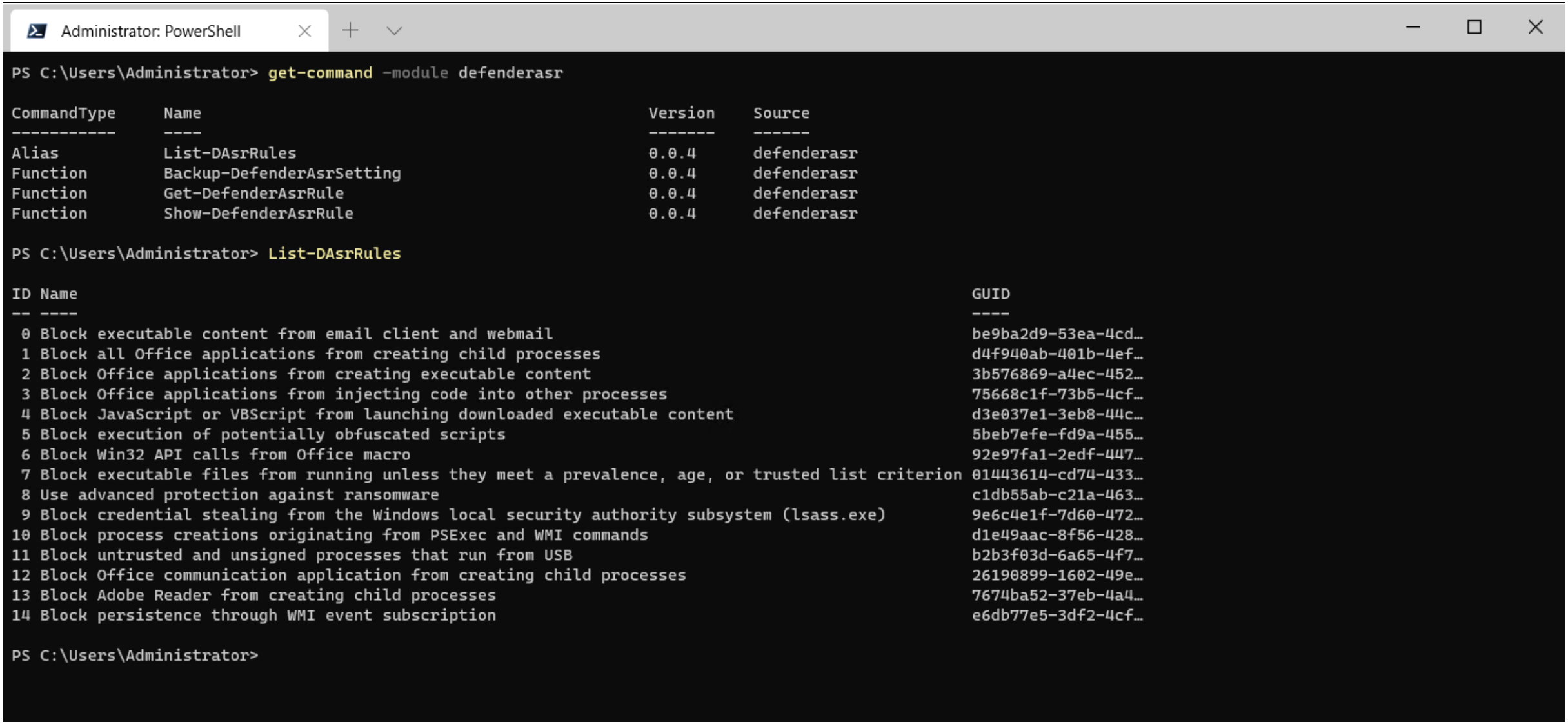
Attack Surface Rules
1121 Block
1122 Audit

The **Get-DefenderEGEvents** cmdlet allows you to quickly pull those events from the Windows Event log

https://www.verboon.info/2019/05/retrieving-windows-defender-exploit-guard-windows-event-logs-with-powershell/

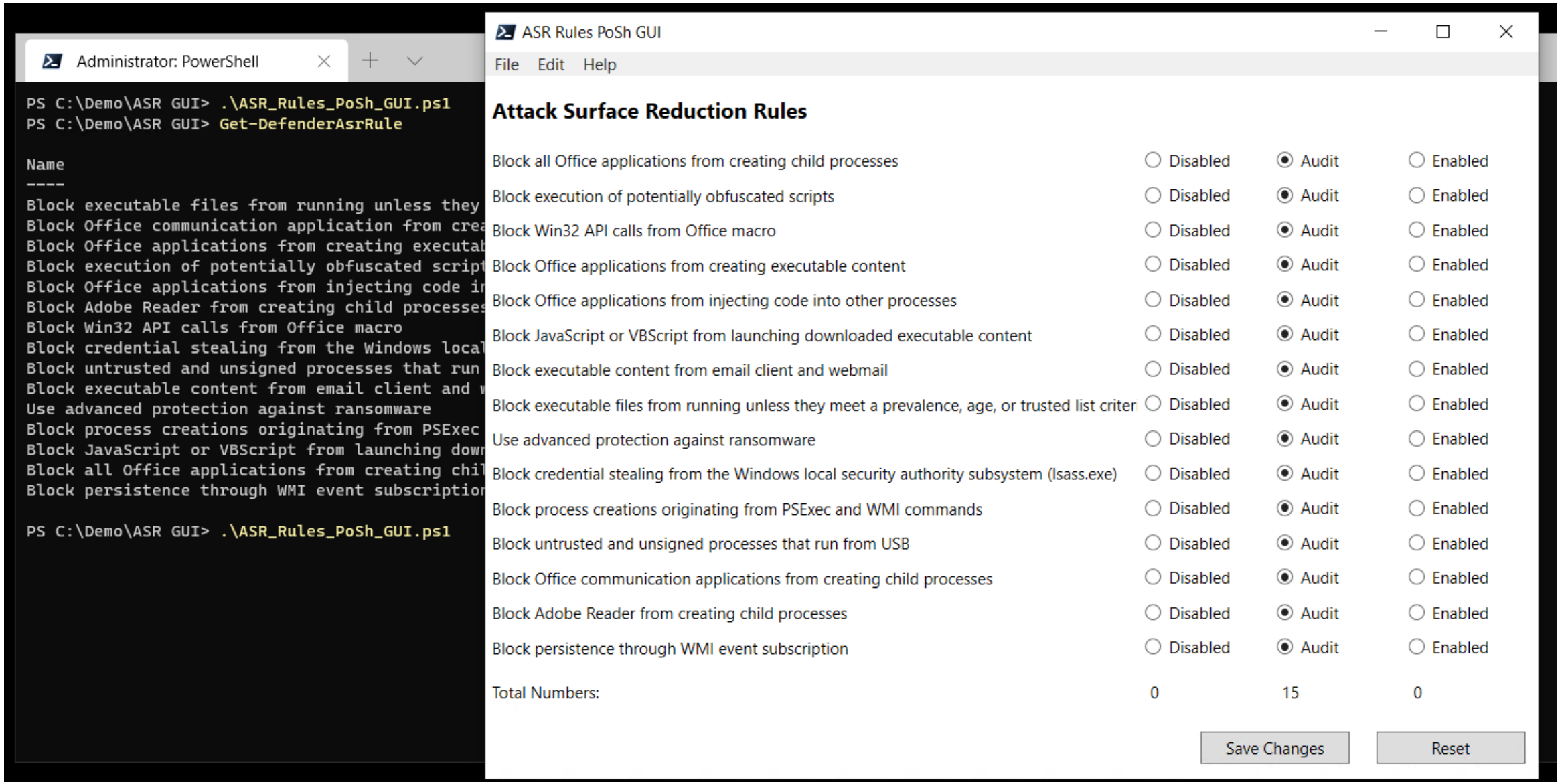
Managing the Microsoft Security stack with PowerShell – Windows Defender – Attack Surface Reduction

https://github.com/sassdawe/HardenWindows/tree/main/WindowsDefender/DefenderASR



Managing the Microsoft Security stack with PowerShell – Windows Defender – Attack Surface Reduction

https://github.com/anthonws/MDATP_PoSh_Scripts



Managing the Microsoft Security stack with PowerShell – Windows Defender – Network Protection Events

Windows PowerShell | PowerShell Core

```
PS C:\dev\alex\MSSecurityPowerShell\DefenderASR> Invoke-RestMethod -Uri "https://smartscreentestratings2.net"
Invoke-RestMethod : The request was aborted: Could not create SSL/TLS secure channel.
At line:1 char:1
+ Invoke-RestMethod -Uri "https://smartscreentestratings2.net"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [I
   eption
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.Inv

PS C:\dev\alex\MSSecurityPowerShell\DefenderASR>
```

Windows Security

This content is blocked

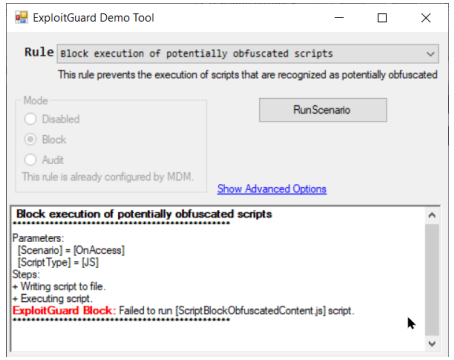
For your protection, your administrator is not allowing you to access content from smartscreentestratings2.net.

OK | Unblock

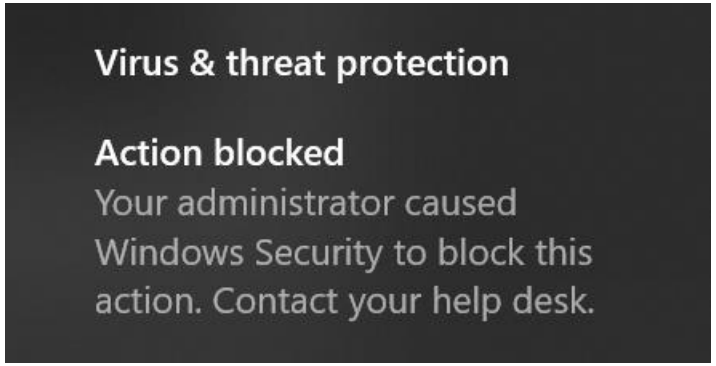
Windows PowerShell | PowerShell Core

```
PS C:\Dev\Alex\MSSecurityPowerShell\DefenderASR> Get-DefenderEGEvents -Component NP -EGMode Block | fl

TimeCreated  : 8/25/2020 4:05:49 PM
ProviderName : Microsoft-Windows-Windows Defender
Id           : 1126
Message      : Your IT administrator has caused Microsoft Defender Exploit Guard to block a potentially dangerous
               network connection.
                        Detection time: 2020-08-25T14:05:49.126Z
                        User: S-1-12-1-2321900437-1234520018-2326948268-2308314766
                        Destination: https://smartscreentestratings2.net
                        Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Managing the Microsoft Security stack with PowerShell – Windows Defender – Attack Surface Protection Events



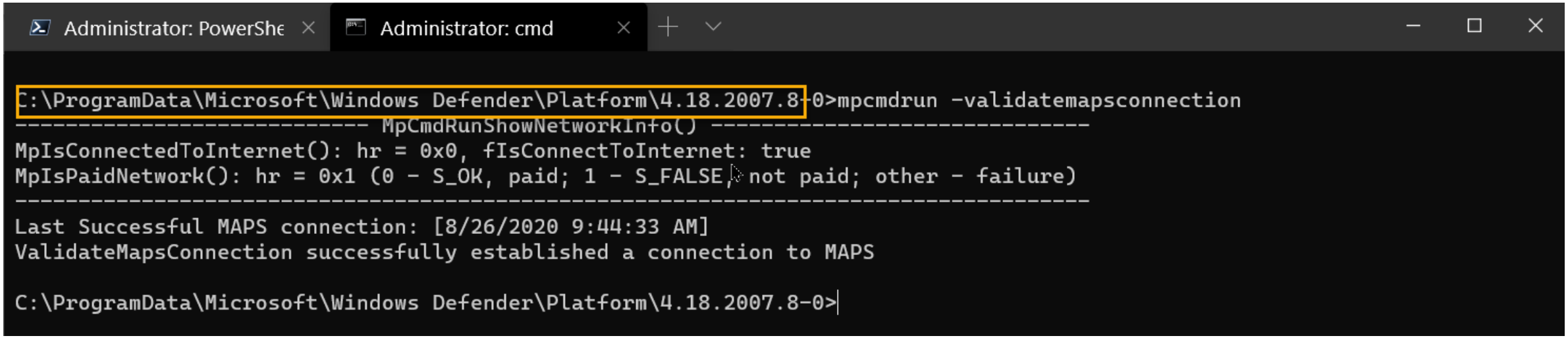
Executing obfuscated scripts

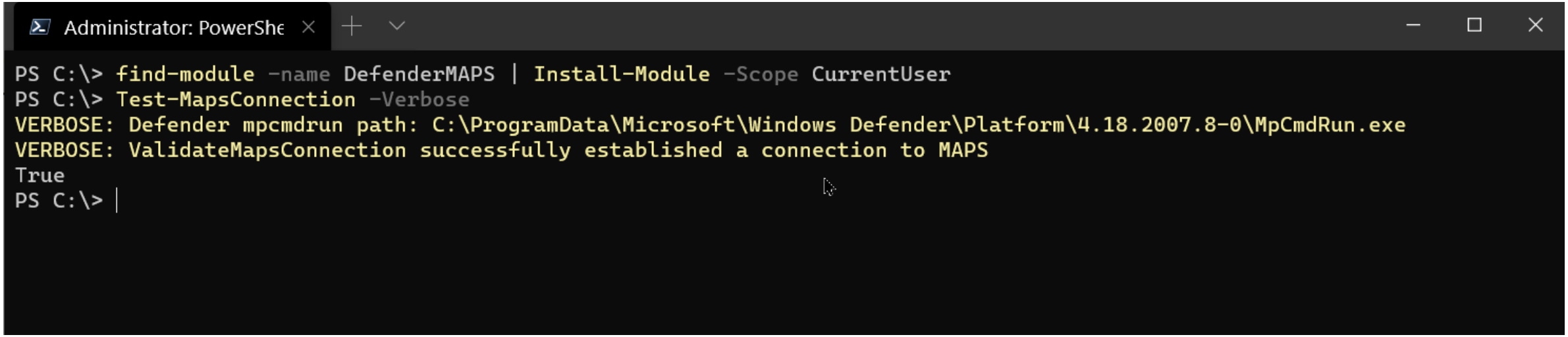


Windows PowerShell | PowerShell Core

```
PS C:\Dev\Alex\MSSecurityPowerShell\DefenderASR> Get-DefenderEGEvents -Component ASR -EGMode Block | fl

TimeCreated  : 8/25/2020 4:09:25 PM
ProviderName : Microsoft-Windows-Windows Defender
Id           : 1121
Message      : Microsoft Defender Exploit Guard has blocked an operation that is not allowed by your IT
               administrator.
                For more information please contact your IT administrator.
                       ID: 5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
                       Detection time: 2020-08-25T14:09:25.304Z
                       User: AzureAD\AlexVerboon
                       Path: C:\ProgramData\AntiMalwareTest\8_25_2020\846cadc1-dcf1-41e1-b409-519bf5d37d2c\Script
BlockO
             bfuscatedContent-{c89e36a0-5606-43ee-b30b-72e8214b35ee}.js
                       Process Name: C:\Windows\System32\wscript.exe
                       Security intelligence Version: 1.321.2158.0
                       Engine Version: 1.1.17300.4
                       Product Version: 4.18.2007.8
```

Test Windows Defender **MAPS** Connection





PSMDATP – PowerShell Module for Microsoft Defender Advanced Threat Protection
https://github.com/alexverboon/PSMDATP

Microsoft Defender Advanced Threat Protection

prevent, detect, investigate, and respond to advanced threats.

Threat & Vulnerability Management

Attack surface reduction

Next-generation protection

Endpoint detection and response

Automated investigation and remediation

Microsoft Threat Experts

Centralized configuration and administration, APIs

Microsoft Threat Protection

Managing the Microsoft Security stack with PowerShell – Defender ATP

Administrator: PowerShe

```
PS C:\> find-module -name PSMDATP

Version              Name                                Repository           Description
-------              ----                                ----------           -----------
1.0.0                PSMDATP                             PSGallery            "Manage Microsoft Defender ATP with Powe…

PS C:\> find-module -name PSMDATP | Install-Module -Scope CurrentUser
PS C:\>
```

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

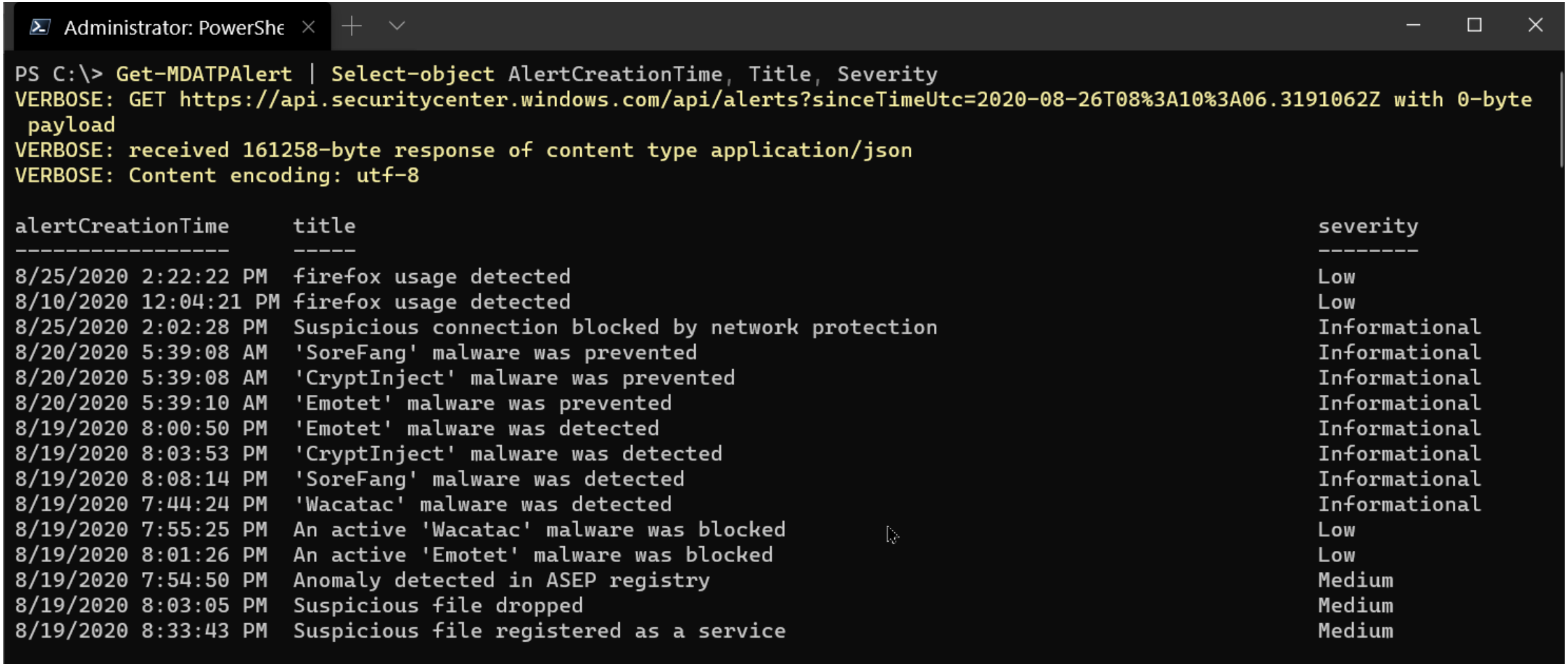
+ Add a permission | Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent req...	Status
Azure Active Directory Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	
WindowsDefenderATP (17)				
AdvancedQuery.Read.All	Application	Run advanced queries	Yes	
Alert.Read.All	Application	Read all alerts	Yes	
Alert.ReadWrite.All	Application	Read and write all alerts	Yes	
Machine.CollectForensics	Application	Collect forensics	Yes	
Machine.Isolate	Application	Isolate machine	Yes	
Machine.Offboard	Application	Offboard machine	Yes	
Machine.Read.All	Application	Read all machine profiles	Yes	
Machine.ReadWrite.All	Application	Read and write all machine information	Yes	
Machine.RestrictExecution	Application	Restrict code execution	Yes	
Machine.Scan	Application	Scan machine	Yes	
Score.Read.All	Application	Read Threat and Vulnerability Management score	Yes	
SecurityConfiguration.Read.All	Application	Read Threat and Vulnerability Management security co...	Yes	
SecurityRecommendation.Read	Application	Read Threat and Vulnerability Management security re...	Yes	
Software.Read.All	Application	Read Threat and Vulnerability Management software in...	Yes	
Ti.ReadWrite	Application	Read and write IOCs belonging to the app	Yes	
Ti.ReadWrite.All	Application	Read and write all IOCs	Yes	Granted for Contoso
Vulnerability.Read.All	Application	Read Threat and Vulnerability Management vulnerabilit...	Yes	Granted for Contoso

PoshMTPconfig.json - Notepad

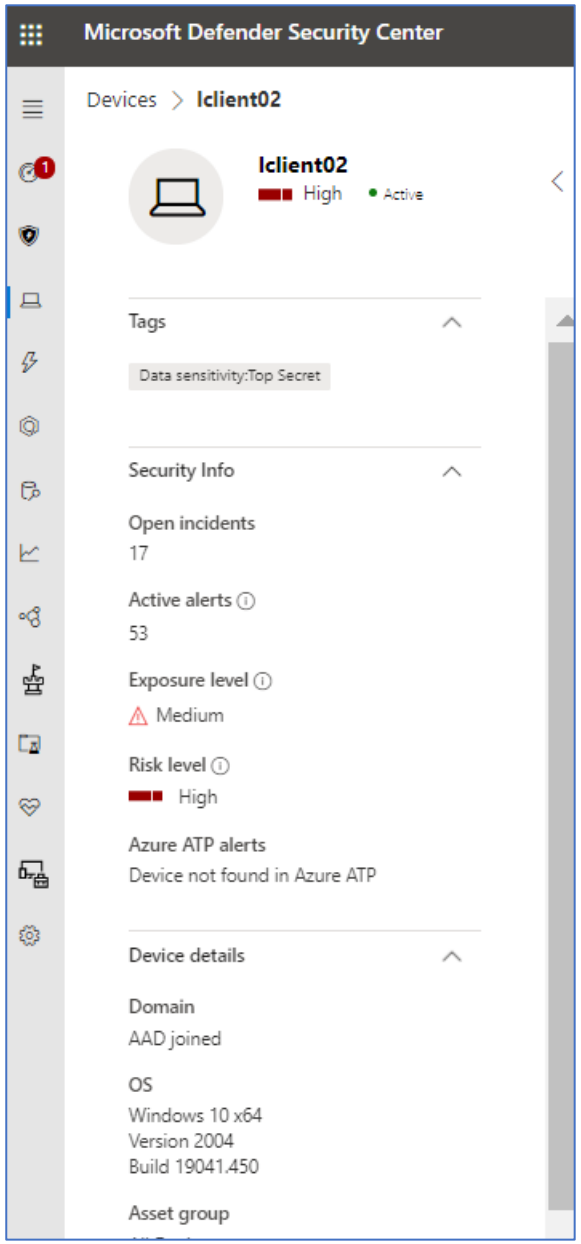
File Edit Format View Help

```
{
    "API_MDATP":  {
                      "AppName":  "MDATPOPS",
                      "OAuthUri":  "https://login.windows.net/[redacted]/oauth2/token",
                      "ClientID":  "[redacted]",
                      "ClientSecret":  "[redacted]"
                  },
    "API_MSGRAPH":  {
                        "AppName":  "xMSGraph",
                        "OAuthUri":  "https://login.windows.net/[redacted]/oauth2/token",
                        "ClientID":  "[redacted]",
                        "ClientSecret":  "[redacted]"
                    }
}
```

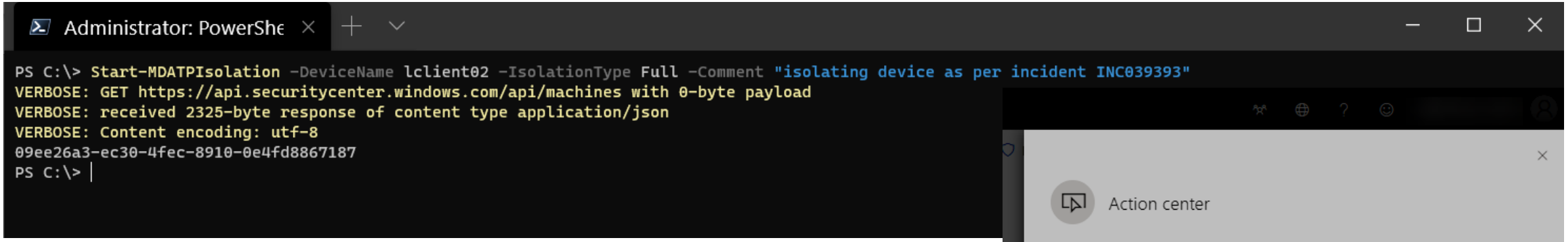

Administrator: PowerShe
PS C:\> Get-MDATPAlert | Select-object AlertCreationTime, Title, Severity
VERBOSE: GET https://api.securitycenter.windows.com/api/alerts?sinceTimeUtc=2020-08-26T08%3A10%3A06.3191062Z with 0-byte payload
VERBOSE: received 161258-byte response of content type application/json
VERBOSE: Content encoding: utf-8
alertCreationTime title severity
8/25/2020 2:22:22 PM firefox usage detected Low
8/10/2020 12:04:21 PM firefox usage detected Low
8/25/2020 2:02:28 PM Suspicious connection blocked by network protection Informational
8/20/2020 5:39:08 AM 'SoreFang' malware was prevented Informational
8/20/2020 5:39:08 AM 'CryptInject' malware was prevented Informational
8/20/2020 5:39:10 AM 'Emotet' malware was prevented Informational
8/19/2020 8:00:50 PM 'Emotet' malware was detected Informational
8/19/2020 8:03:53 PM 'CryptInject' malware was detected Informational
8/19/2020 8:08:14 PM 'SoreFang' malware was detected Informational
8/19/2020 7:44:24 PM 'Wacatac' malware was detected Informational
8/19/2020 7:55:25 PM An active 'Wacatac' malware was blocked Low
8/19/2020 8:01:26 PM An active 'Emotet' malware was blocked Low
8/19/2020 7:54:50 PM Anomaly detected in ASEP registry Medium
8/19/2020 8:03:05 PM Suspicious file dropped Medium
8/19/2020 8:33:43 PM Suspicious file registered as a service Medium

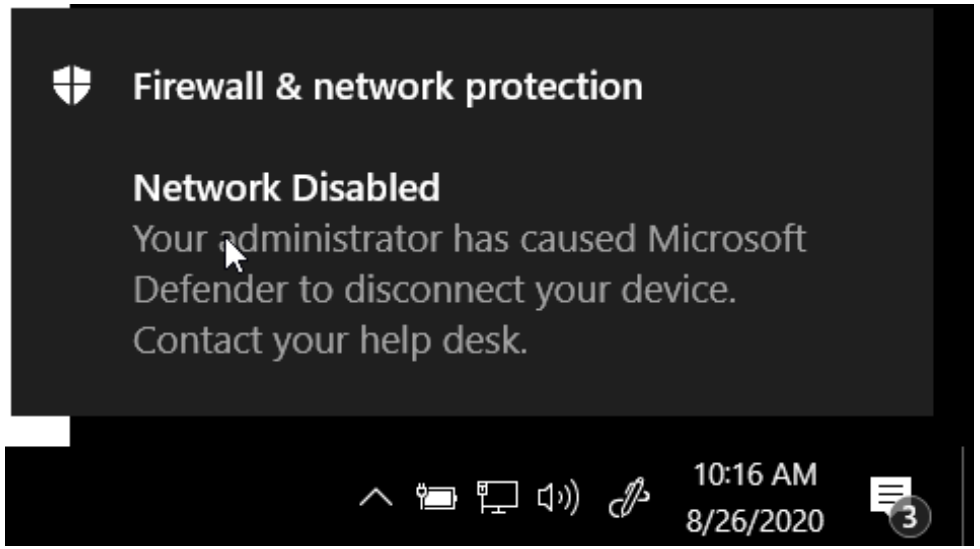
Managing the Microsoft Security stack with PowerShell – Defender ATP

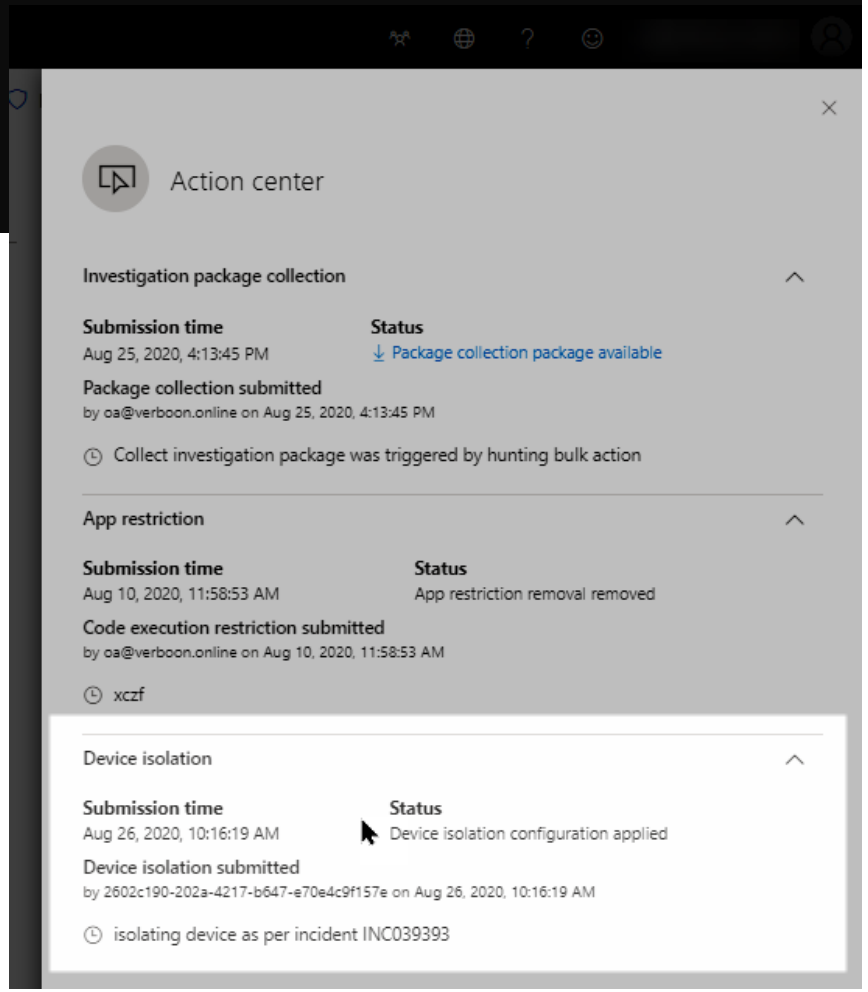
```
Administrator: PowerShe

PS C:\> Get-MDATPDevice -DeviceName lclient02
VERBOSE: GET https://api.securitycenter.windows.com/api/machines?$filter=ComputerDNSName eq 'lclient02' with 0-byte payload
VERBOSE: received 667-byte response of content type application/json
VERBOSE: Content encoding: utf-8

id                    : 57b63cb49223ce246f26d57a81287c9f17893bea
computerDnsName       : lclient02
firstSeen             : 7/10/2020 6:00:22 PM
lastSeen              : 8/26/2020 7:34:05 AM
osPlatform            : Windows10
osVersion             :
osProcessor           : x64
version               : 2004
lastIpAddress         : 172.18.192.1
lastExternalIpAddress : 77.56.162.123
agentVersion          : 10.7430.19041.423
osBuild               : 19041
healthStatus          : Active
deviceValue           : Normal
rbacGroupId           : 913
rbacGroupName         : All Devices
riskScore             : High
exposureLevel         : Medium
aadDeviceId           : 9eb5a403-e50a-435a-ae25-32cc8510ad6a
machineTags           : {}


PS C:\>
```



Isolating the device from the network







Managing the Microsoft Security stack with PowerShell – Defender ATP

Windows PowerShell | PowerShell Core

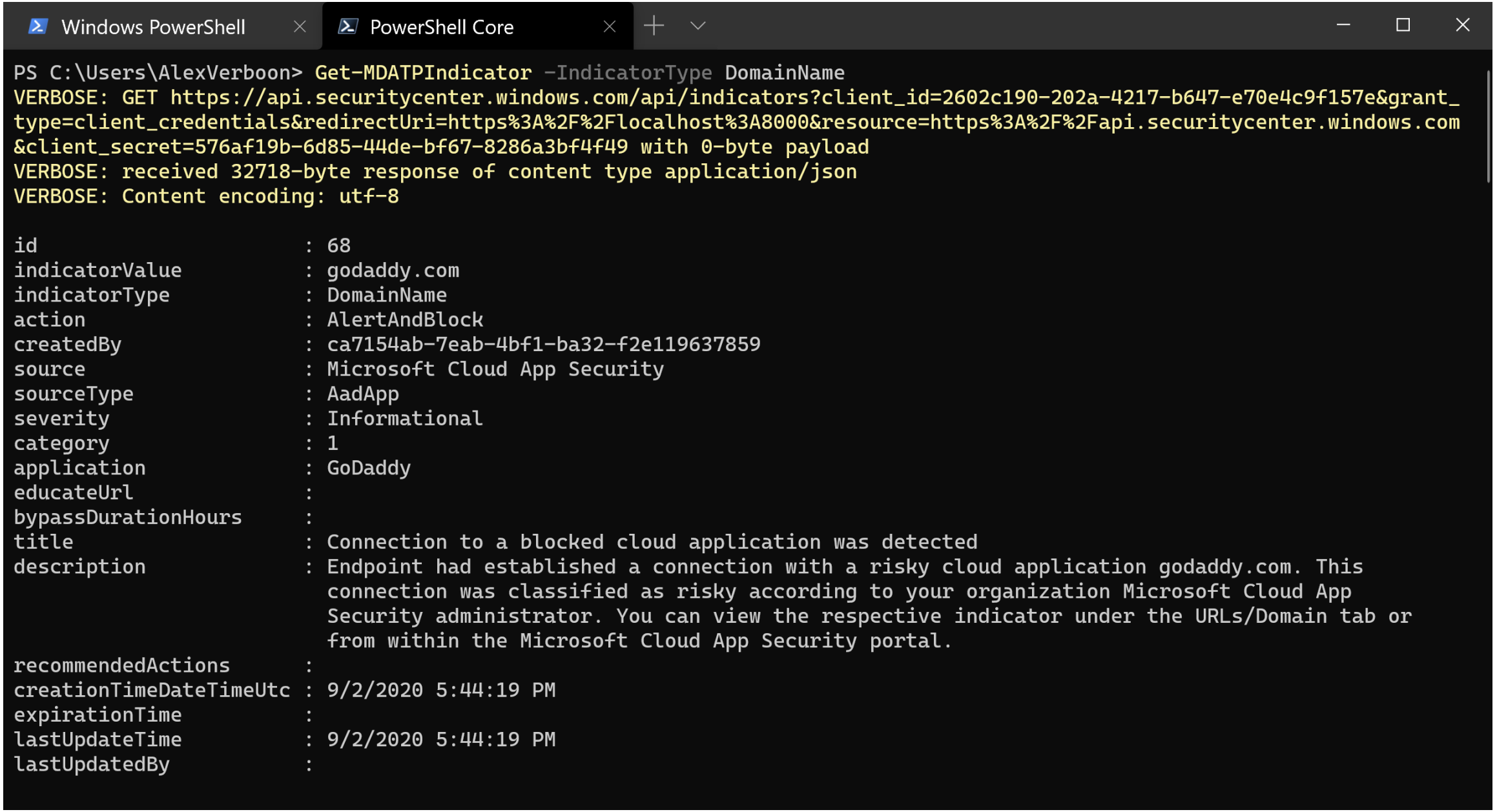
```
PS C:\Users\AlexVerboon> Get-MDATPAlert -Severity High
VERBOSE: GET https://api.securitycenter.windows.com/api/alerts?sinceTimeUtc=2020-09-09T18%3A41%3A45.6929104Z with 0-byte
 payload
VERBOSE: received 199002-byte response of content type application/json
VERBOSE: Content encoding: utf-8

id                  : da637329116998998878_-1447647443
incidentId          : 47
investigationId     :
assignedTo          :
severity            : High
status              : New
classification      :
determination       :
investigationState  : UnsupportedAlertType
detectionSource     : WindowsDefenderAtp
category            : CredentialAccess
threatFamilyName    :
title               : Sensitive credential memory read
description         : A process scanned or dumped memory from the Local Security Authority Subsystem Service
                      (lsass.exe).  Accessing this process memory allows the attacker to extract secrets such as
                      authentication hashes or passwords.  A copy of this memory may be written to the file system and
                      exfiltrated to extract these credentials offline.
alertCreationTime   : 8/13/2020 10:34:59 AM
firstEventTime      : 8/13/2020 10:11:34 AM
lastEventTime       : 8/13/2020 10:11:34 AM
lastUpdateTime      : 8/13/2020 10:35:01 AM
resolvedTime        :
machineId           : 57b63cb49223ce246f26d57a81287c9f17893bea
```

Managing the Microsoft Security stack with PowerShell – Defender ATP

Windows PowerShell | PowerShell Core

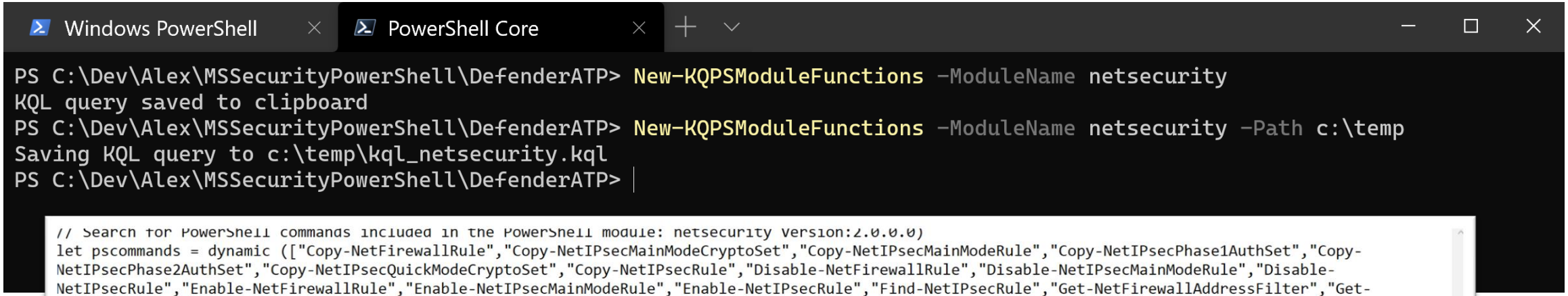
```
PS C:\Users\AlexVerboon> Start-MDATPAVScan -DeviceName lclient02 -ScanType Quick
VERBOSE: GET https://api.securitycenter.windows.com/api/machines with 0-byte payload
VERBOSE: received 4090-byte response of content type application/json
VERBOSE: Content encoding: utf-8
0be12ca5-fdf8-440d-a40e-77e7afe62d1c
PS C:\Users\AlexVerboon> Get-MDATPDeviceAction -DeviceName lclient02
VERBOSE: GET https://api.securitycenter.windows.com/api/machines?$filter=ComputerDNSName eq 'lclient02' with 0-byte payl
oad
VERBOSE: received 669-byte response of content type application/json
VERBOSE: Content encoding: utf-8
VERBOSE: GET https://api.securitycenter.windows.com/api/machines/57b63cb49223ce246f26d57a81287c9f17893bea with 0-byte pa
yload
VERBOSE: received 665-byte response of content type application/json
VERBOSE: Content encoding: utf-8
VERBOSE: GET https://api-us.securitycenter.windows.com/api/machineactions/?$filter=machineId+eq+'57b63cb49223ce246f26d57
a81287c9f17893bea' with 0-byte payload
VERBOSE: received 23970-byte response of content type application/json
VERBOSE: Content encoding: utf-8

id                      : 0be12ca5-fdf8-440d-a40e-77e7afe62d1c
type                    : RunAntiVirusScan
requestor               : 2602c190-202a-4217-b647-e70e4c9f157e
requestorComment        : submitted by automation
status                  : Pending
machineId               : 57b63cb49223ce246f26d57a81287c9f17893bea
computerDnsName         : lclient02
creationDateTimeUtc     : 9/9/2020 6:50:40 PM
lastUpdateDateTimeUtc   : 9/9/2020 6:50:40 PM
cancellationRequestor   :
```

Managing the Microsoft Security stack with PowerShell – Defender ATP



Managing the Microsoft Security stack with PowerShell – Defender ATP – Advanced Hunting

User PowerShell to generate a KQL query that looks for executed cmdlets included in a PowerShell Module




```
// Search for PowerShell commands included in the PowerShell module: netsecurity Version:2.0.0.0)
let pscommands = dynamic (["Copy-NetFirewallRule","Copy-NetIPsecMainModeCryptoSet","Copy-NetIPsecMainModeRule","Copy-NetIPsecPhase1AuthSet","Copy-
NetIPsecPhase2AuthSet","Copy-NetIPsecQuickModeCryptoSet","Copy-NetIPsecRule","Disable-NetFirewallRule","Disable-NetIPsecMainModeRule","Disable-
NetIPsecRule","Enable-NetFirewallRule","Enable-NetIPsecMainModeRule","Enable-NetIPsecRule","Find-NetIPsecRule","Get-NetFirewallAddressFilter","Get-
NetFirewallApplicationFilter","Get-NetFirewallInterfaceFilter","Get-NetFirewallInterfaceTypeFilter","Get-NetFirewallPortFilter","Get-
NetFirewallProfile","Get-NetFirewallRule","Get-NetFirewallSecurityFilter","Get-NetFirewallServiceFilter","Get-NetFirewallSetting","Get-
NetIPsecDospSetting","Get-NetIPsecMainModeCryptoSet","Get-NetIPsecMainModeRule","Get-NetIPsecMainModeSA","Get-NetIPsecPhase1AuthSet","Get-
NetIPsecPhase2AuthSet","Get-NetIPsecQuickModeCryptoSet","Get-NetIPsecQuickModeSA","Get-NetIPsecRule","New-NetFirewallRule","New-NetIPsecDospSetting","New-
NetIPsecMainModeCryptoSet","New-NetIPsecMainModeRule","New-NetIPsecPhase1AuthSet","New-NetIPsecPhase2AuthSet","New-NetIPsecQuickModeCryptoSet","New-
NetIPsecRule","Open-NetGPO","Remove-NetFirewallRule","Remove-NetIPsecDospSetting","Remove-NetIPsecMainModeCryptoSet","Remove-
NetIPsecMainModeRule","Remove-NetIPsecMainModeSA","Remove-NetIPsecPhase1AuthSet","Remove-NetIPsecPhase2AuthSet","Remove-
NetIPsecQuickModeCryptoSet","Remove-NetIPsecQuickModeSA","Remove-NetIPsecRule","Rename-NetFirewallRule","Rename-NetIPsecMainModeCryptoSet","Rename-
NetIPsecMainModeRule","Rename-NetIPsecPhase1AuthSet","Rename-NetIPsecPhase2AuthSet","Rename-NetIPsecQuickModeCryptoSet","Rename-NetIPsecRule","Save-
NetGPO","Set-NetFirewallAddressFilter","Set-NetFirewallApplicationFilter","Set-NetFirewallInterfaceFilter","Set-NetFirewallInterfaceTypeFilter","Set-
NetFirewallPortFilter","Set-NetFirewallProfile","Set-NetFirewallRule","Set-NetFirewallSecurityFilter","Set-NetFirewallServiceFilter","Set-
NetFirewallSetting","Set-NetIPsecDospSetting","Set-NetIPsecMainModeCryptoSet","Set-NetIPsecMainModeRule","Set-NetIPsecPhase1AuthSet","Set-
NetIPsecPhase2AuthSet","Set-NetIPsecQuickModeCryptoSet","Set-NetIPsecRule","Show-NetFirewallRule","Show-NetIPsecRule","Sync-NetIPsecRule","Update-
NetIPsecRule","Get-DAPolicyChange","New-NetIPsecAuthProposal","New-NetIPsecMainModeCryptoProposal","New-NetIPsecQuickModeCryptoProposal"]);
DeviceEvents
| where ActionType contains "PowerShellCommand"
| where AdditionalFields has_any (pscommands)
```

https://gist.github.com/alexverboon/9ccf8af7569103397da2b8ba4079529d

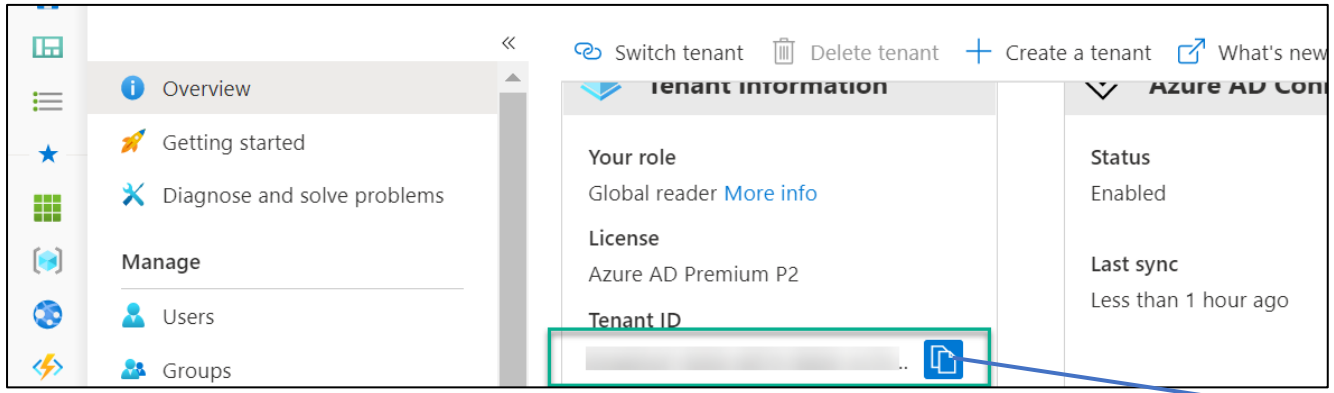
AzureAD

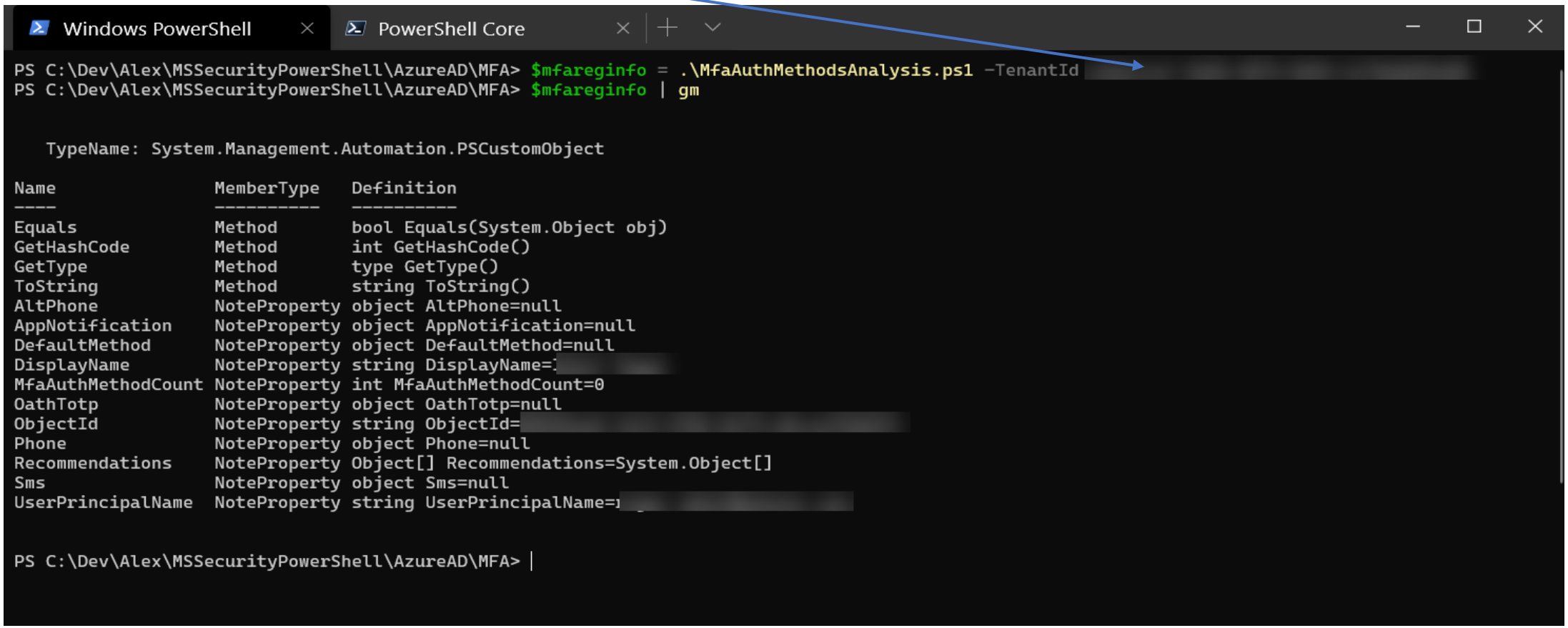
Multifactor Authentication

Who has registered for MFA and who hasn't?
What MFA methods are registered?

Script for Azure MFA authentication method analysis
https://github.com/Azure-Samples/azure-mfa-authentication-method-analysis/tree/master/

Managing the Microsoft Security stack with PowerShell – AzureAD Multifactor Authentication





Get an overview of the MFA registration status

Windows PowerShell | PowerShell Core

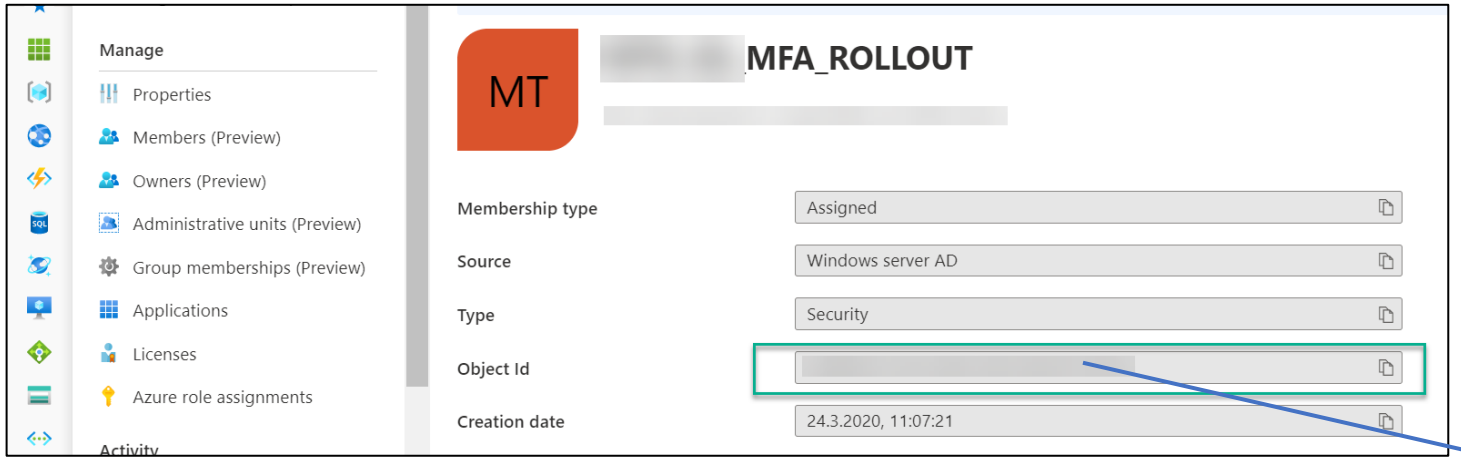
```
PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA> $no_mfa = $mfareginfo | where MfaAuthMethodCount -eq 0
PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA> $no_mfa.count
2599
PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA> $mfa = $mfareginfo | where MfaAuthMethodCount -gt 0
PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA> $mfa.count
131
PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA>
```

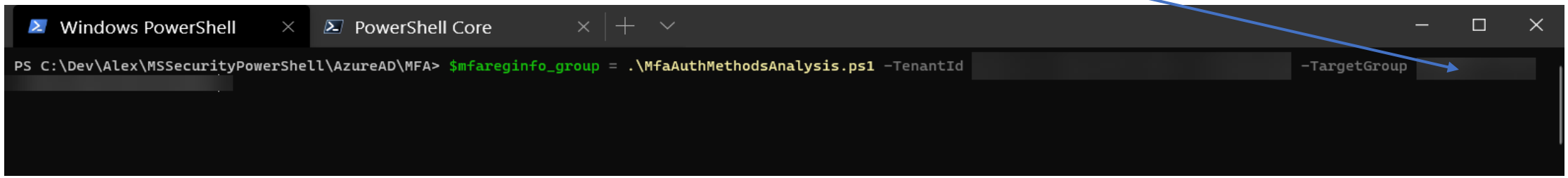
User details

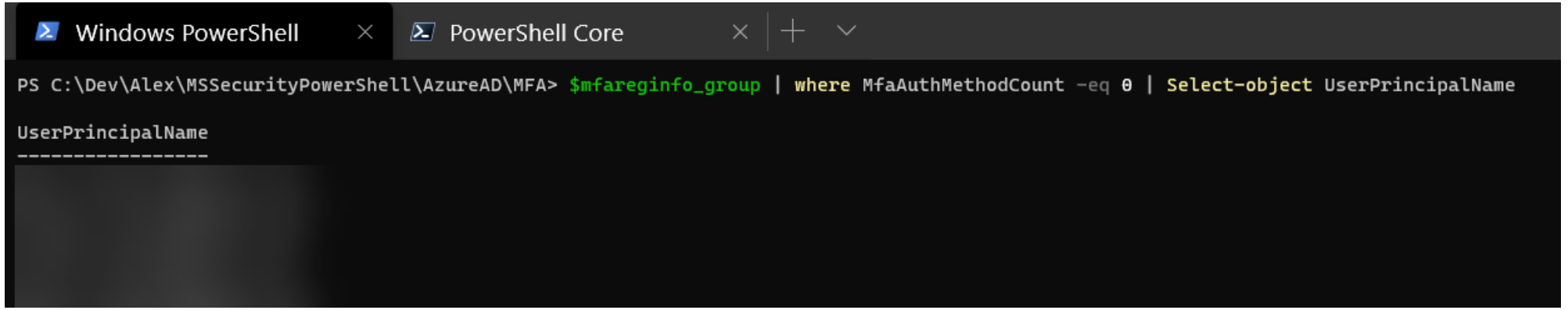
Windows PowerShell | PowerShell Core

```
PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA> $mfareginfo | where UserPrincipalName -like '*verale*'


UserPrincipalName  : 1
DisplayName        : Alex Verboon
ObjectId           : a
MfaAuthMethodCount : 4
DefaultMethod      : PhoneAppNotification
AppNotification    : Yes
OathTotp           : Yes
Sms                : Yes
Phone              : Yes
AltPhone           :
Recommendations    : {'Consider adding an alternative phone number for additional resilience.'}



PS C:\Dev\Alex\MSSecurityPowerShell\AzureAD\MFA>
```

Managing the Microsoft Security stack with PowerShell – AzureAD Multifactor Authentication



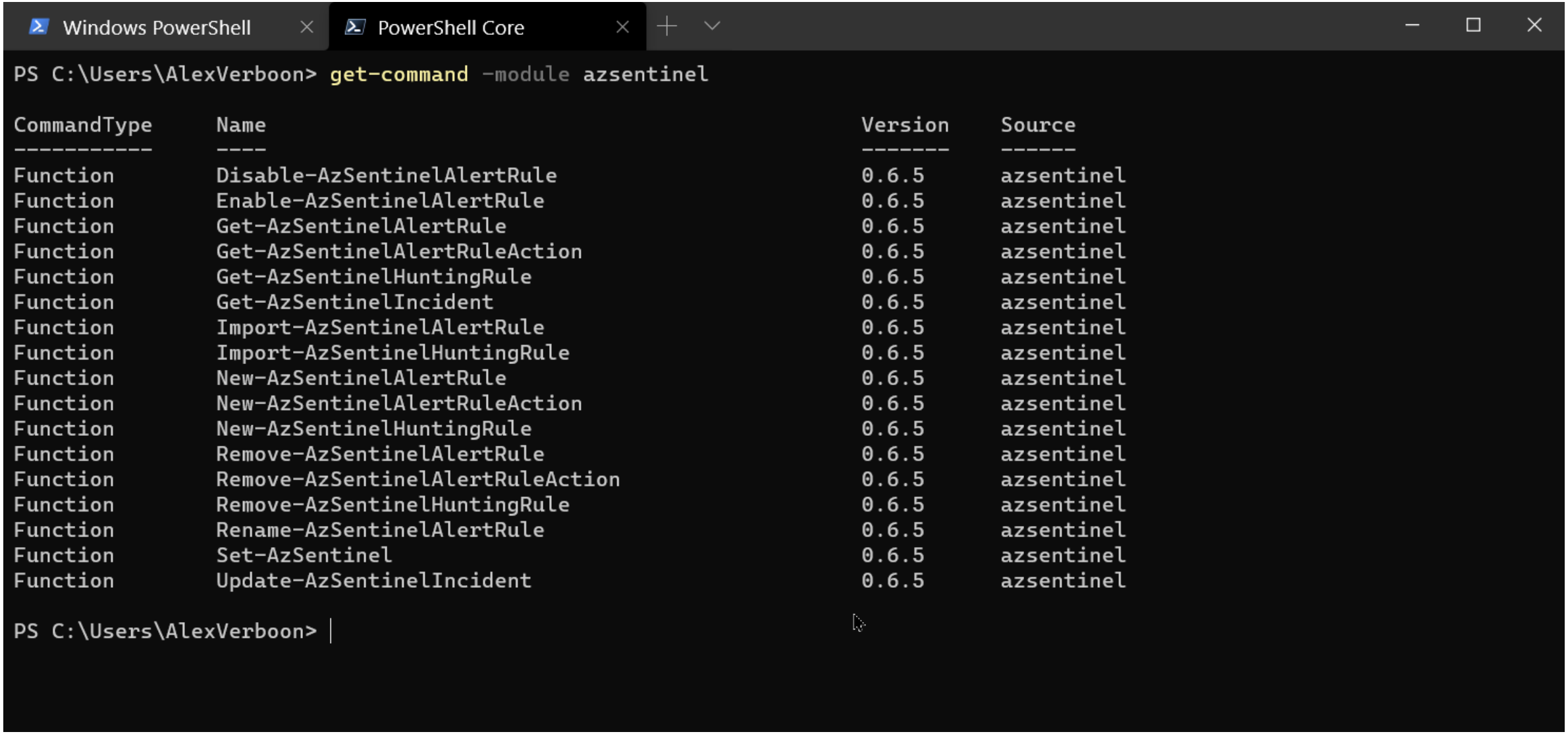




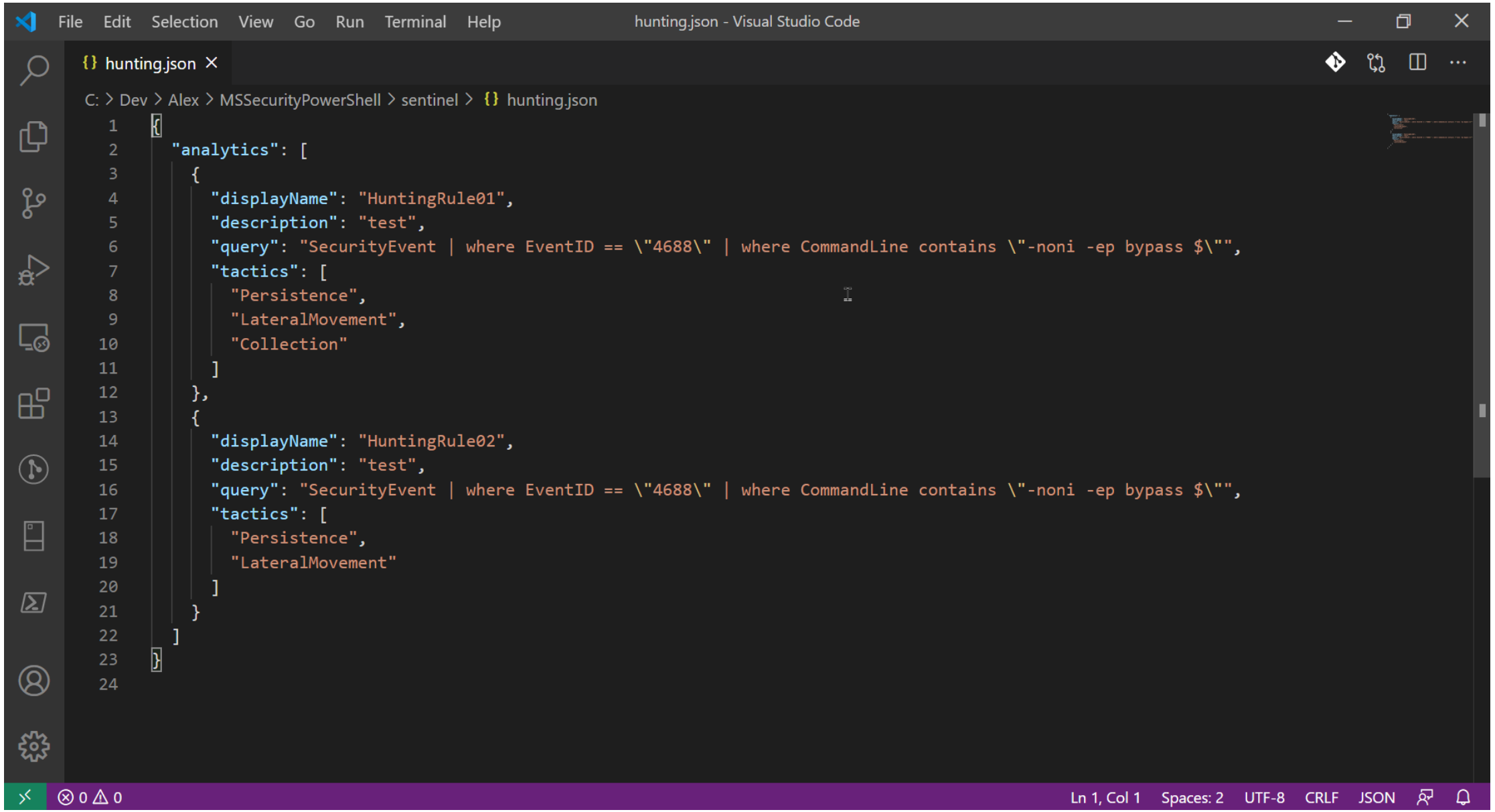
Azure Sentinel

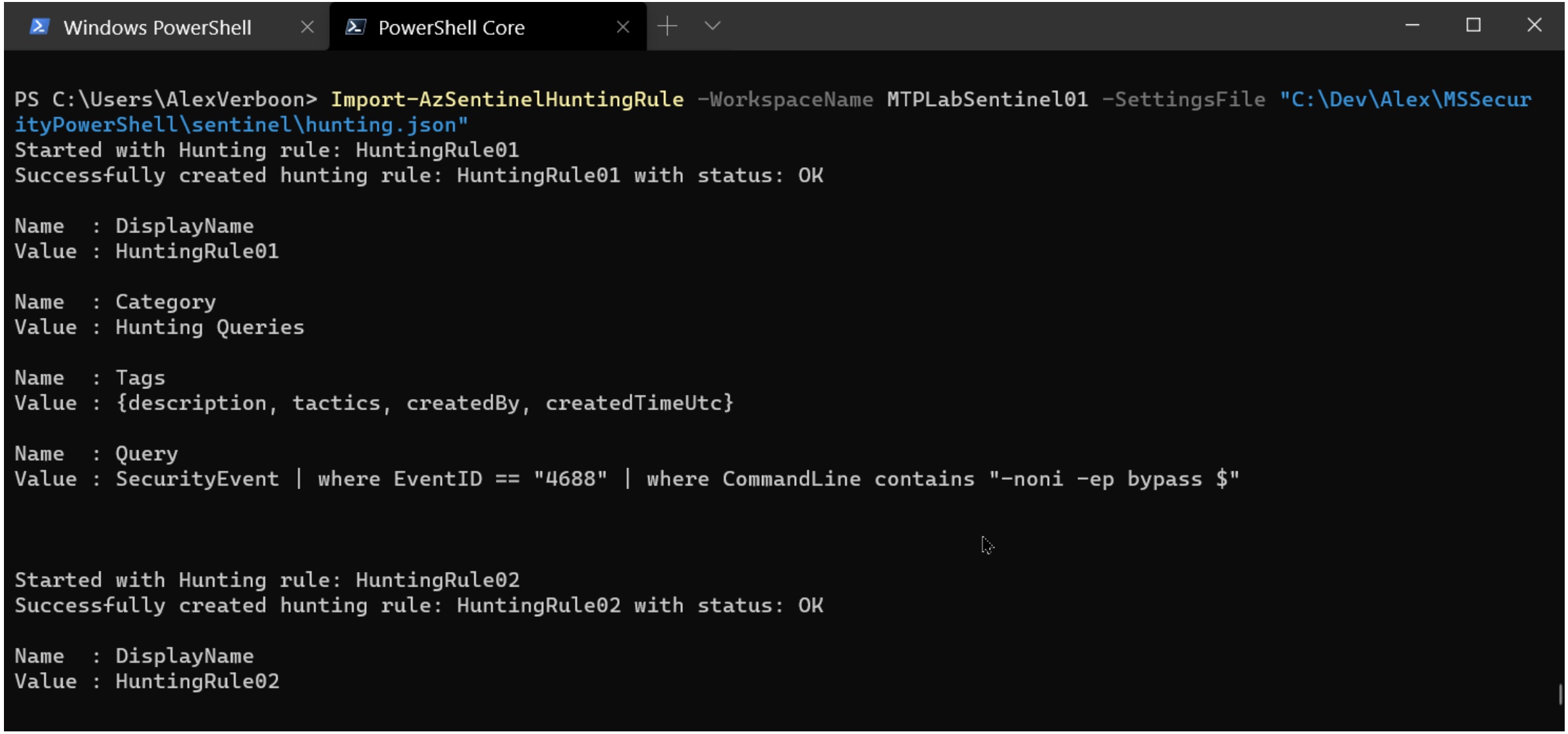
Managing the Microsoft Security stack with PowerShell – Azure Sentinel

https://github.com/wortell/AZSentinel

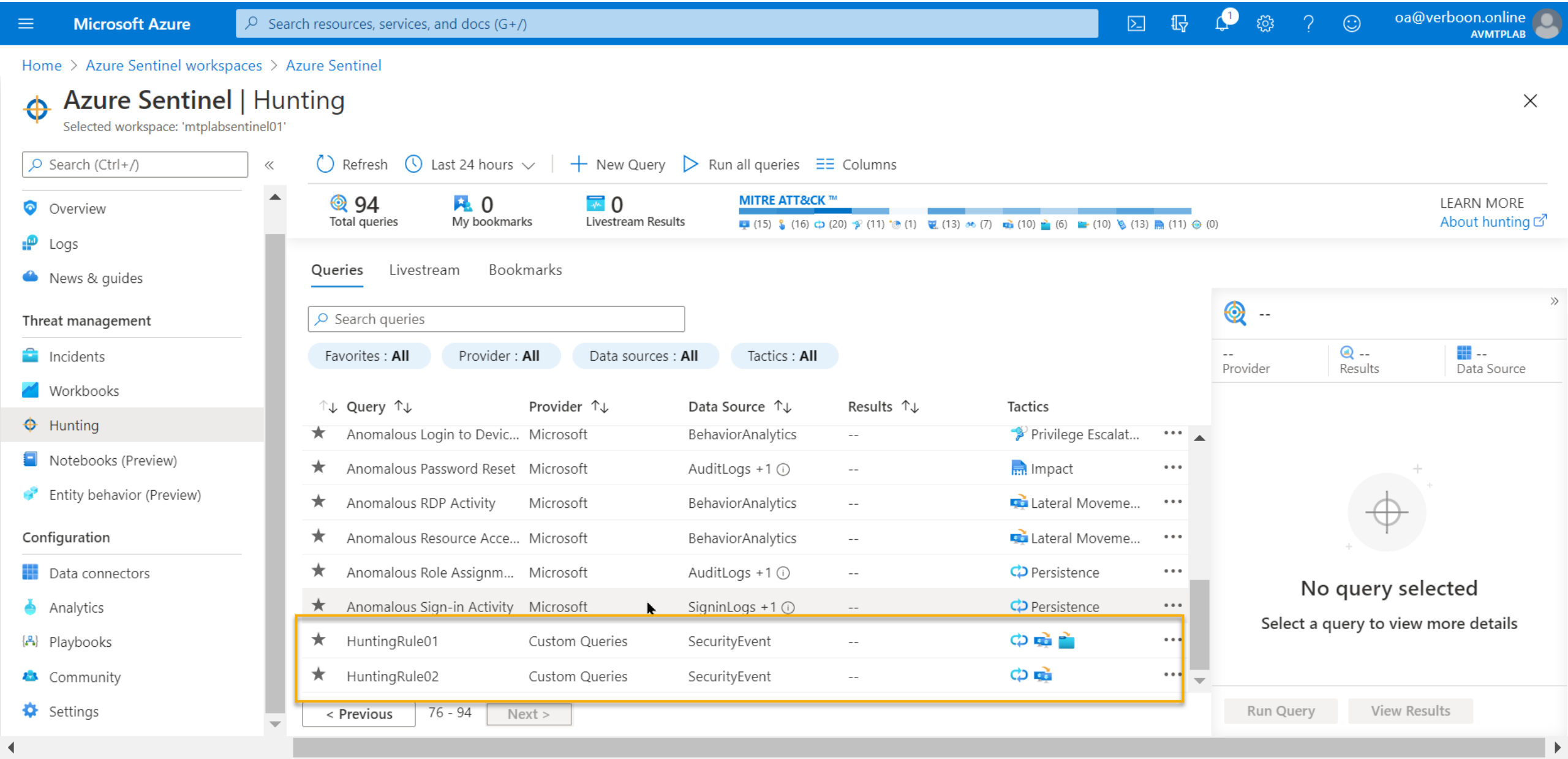


Managing the Microsoft Security stack with PowerShell – Azure Sentinel



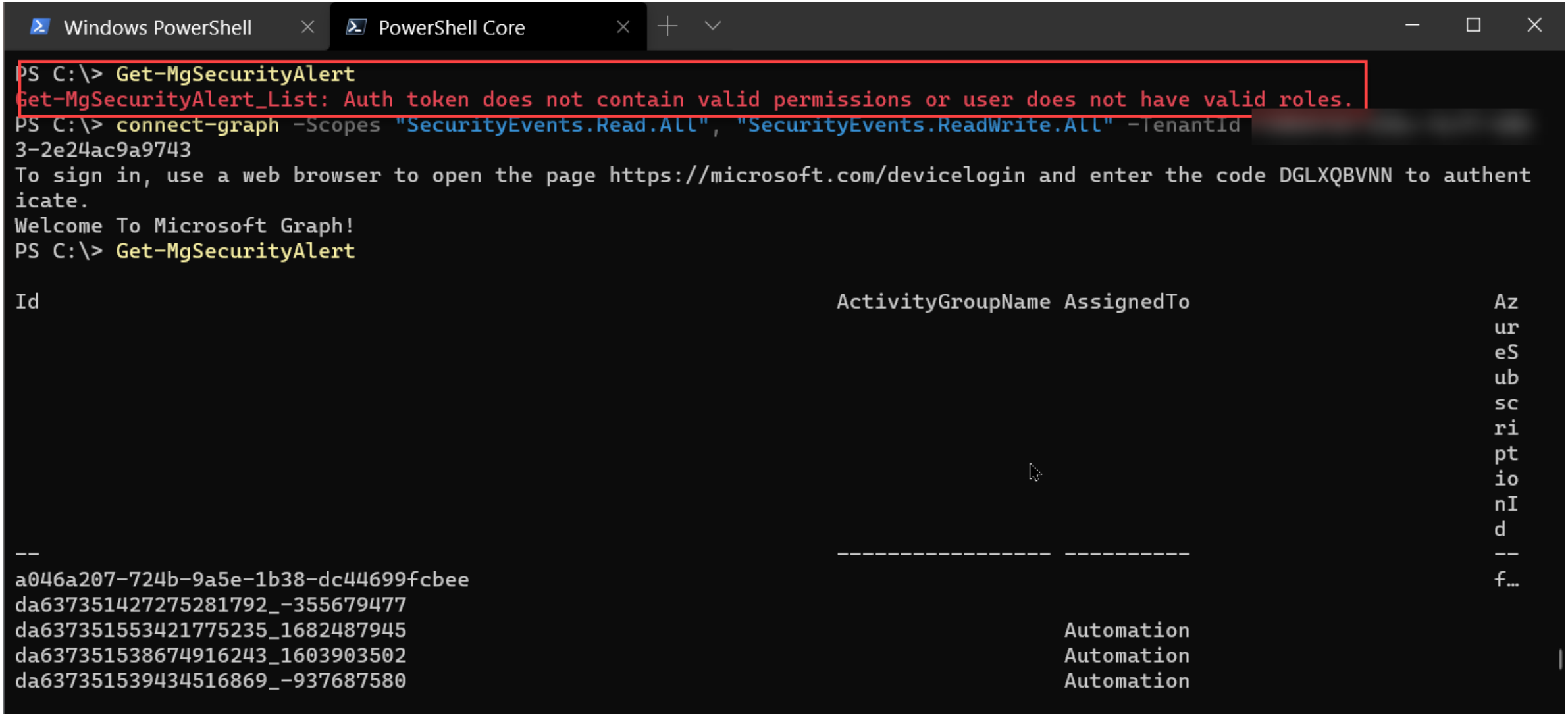

Windows PowerShell
PowerShell Core
PS C:\Users\AlexVerboon> Import-AzSentinelHuntingRule -WorkspaceName MTPLabSentinel01 -SettingsFile "C:\Dev\Alex\MSSecurityPowerShell\sentinel\hunting.json"
Started with Hunting rule: HuntingRule01
Successfully created hunting rule: HuntingRule01 with status: OK
Name : DisplayName
Value : HuntingRule01
Name : Category
Value : Hunting Queries
Name : Tags
Value : {description, tactics, createdBy, createdTimeUtc}
Name : Query
Value : SecurityEvent | where EventID == "4688" | where CommandLine contains "-noni -ep bypass $"
Started with Hunting rule: HuntingRule02
Successfully created hunting rule: HuntingRule02 with status: OK
Name : DisplayName
Value : HuntingRule02

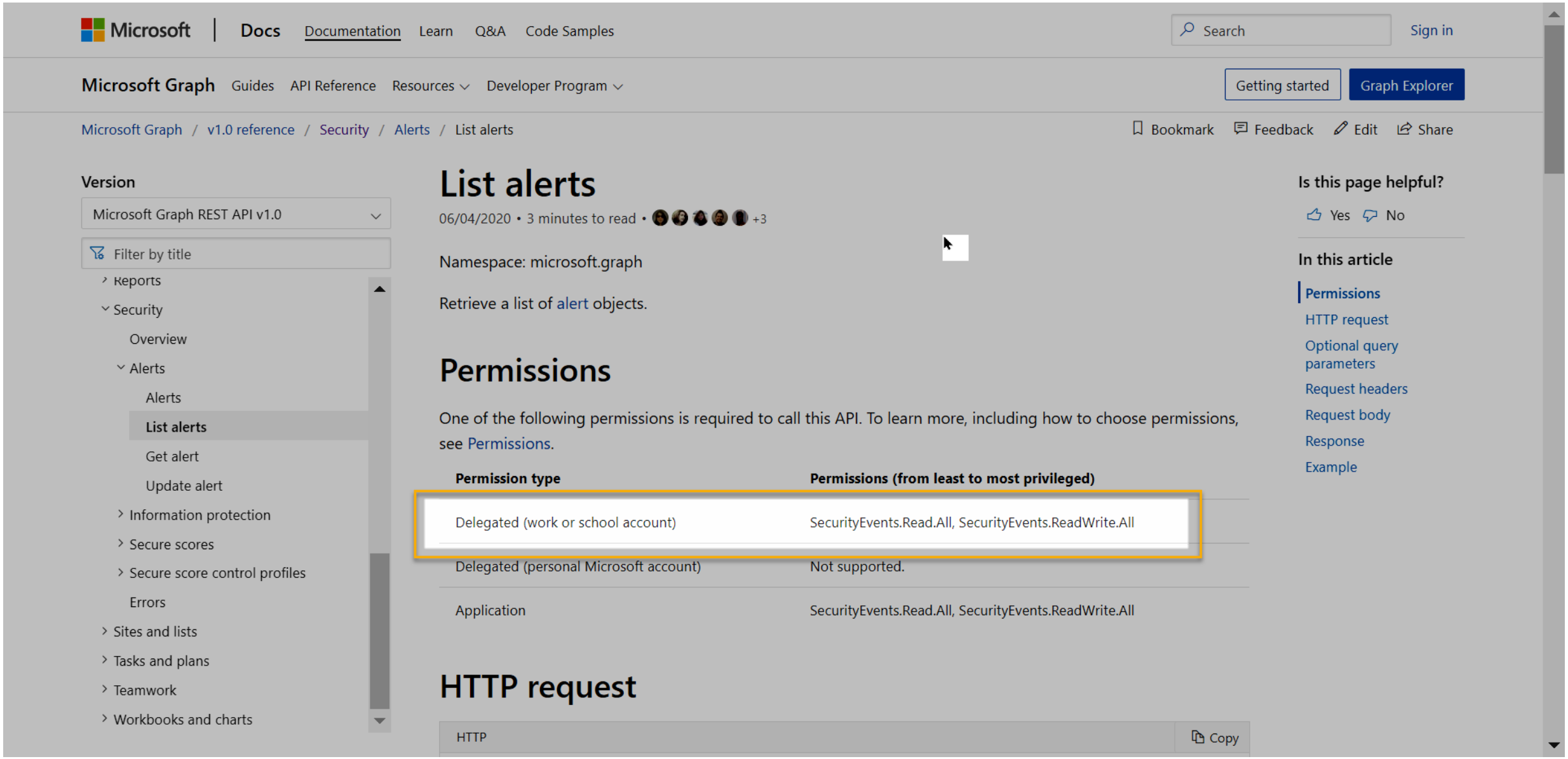
Managing the Microsoft Security stack with PowerShell – Azure Sentinel



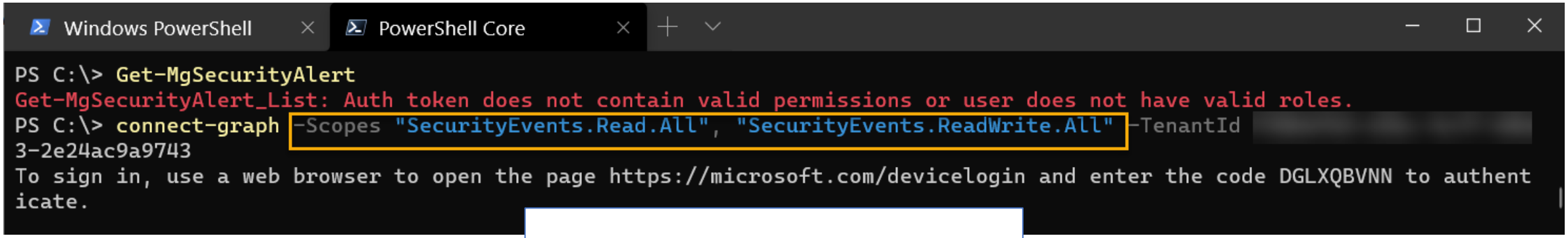
Microsoft Graph

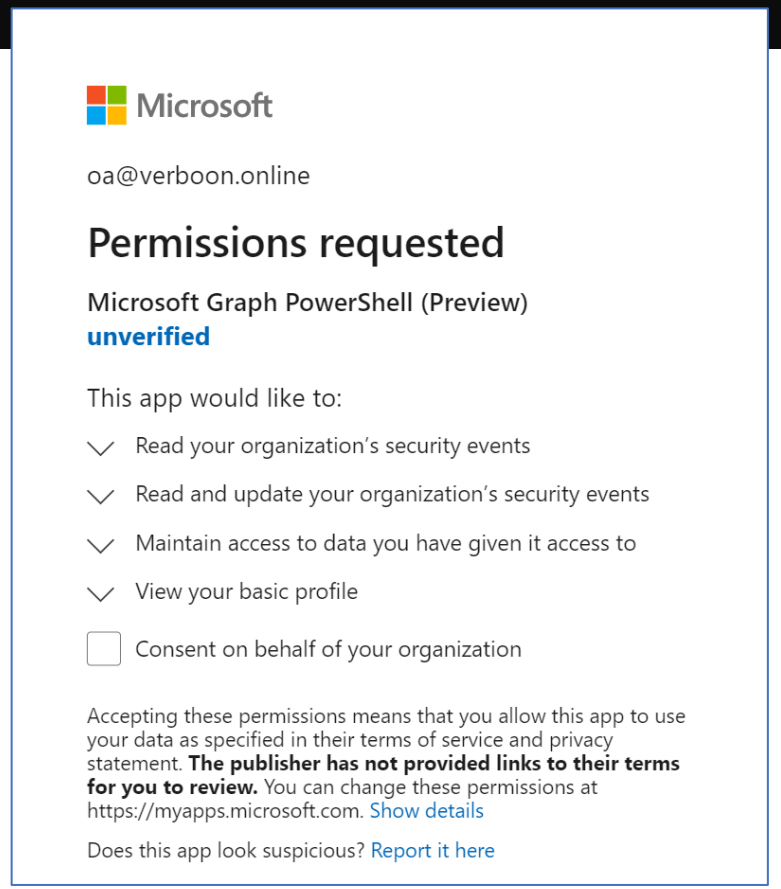
Managing the Microsoft Security stack with PowerShell – Microsoft Graph




Microsoft | Docs
Documentation
Learn
Q&A
Code Samples
Search
Sign in
Microsoft Graph
Guides
API Reference
Resources
Developer Program
Getting started
Graph Explorer
Microsoft Graph / v1.0 reference / Security / Alerts / List alerts
Bookmark
Feedback
Edit
Share
Version
Microsoft Graph REST API v1.0
Filter by title
Reports
Security
Overview
Alerts
Alerts
List alerts
Get alert
Update alert
Information protection
Secure scores
Secure score control profiles
Errors
Sites and lists
Tasks and plans
Teamwork
Workbooks and charts
List alerts
06/04/2020 • 3 minutes to read • +3
Namespace: microsoft.graph
Retrieve a list of alert objects.
Permissions
One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.
Permission type
Permissions (from least to most privileged)
Delegated (work or school account)
SecurityEvents.Read.All, SecurityEvents.ReadWrite.All
Delegated (personal Microsoft account)
Not supported.
Application
SecurityEvents.Read.All, SecurityEvents.ReadWrite.All
HTTP request
HTTP
Copy
Is this page helpful?
Yes
No
In this article
Permissions
HTTP request
Optional query parameters
Request headers
Request body
Response
Example

Managing the Microsoft Security stack with PowerShell – Microsoft Graph



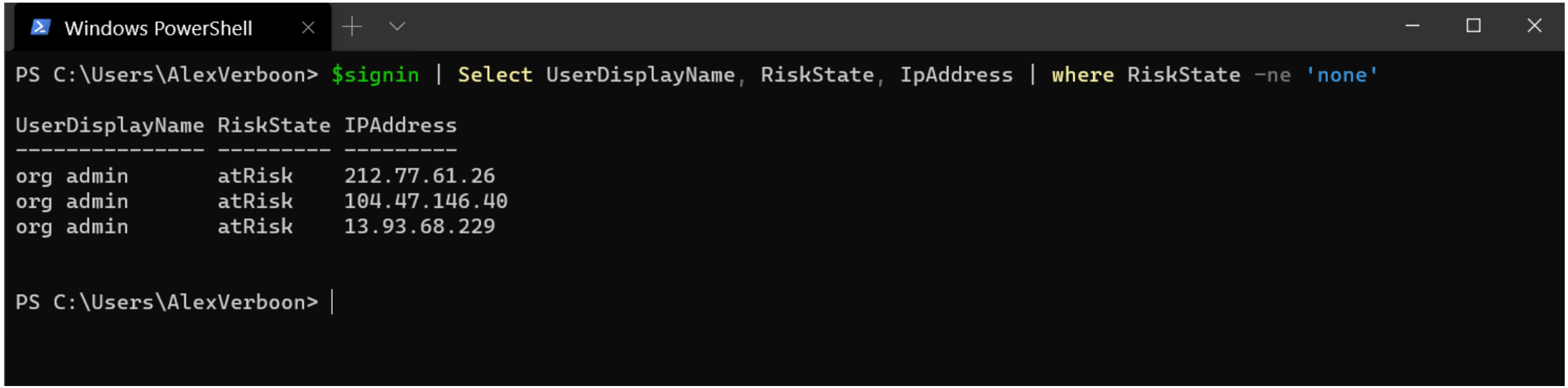


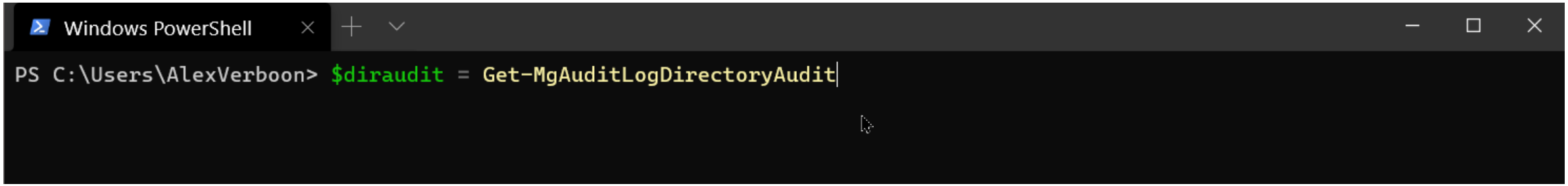
Managing the Microsoft Security stack with PowerShell – Microsoft Graph

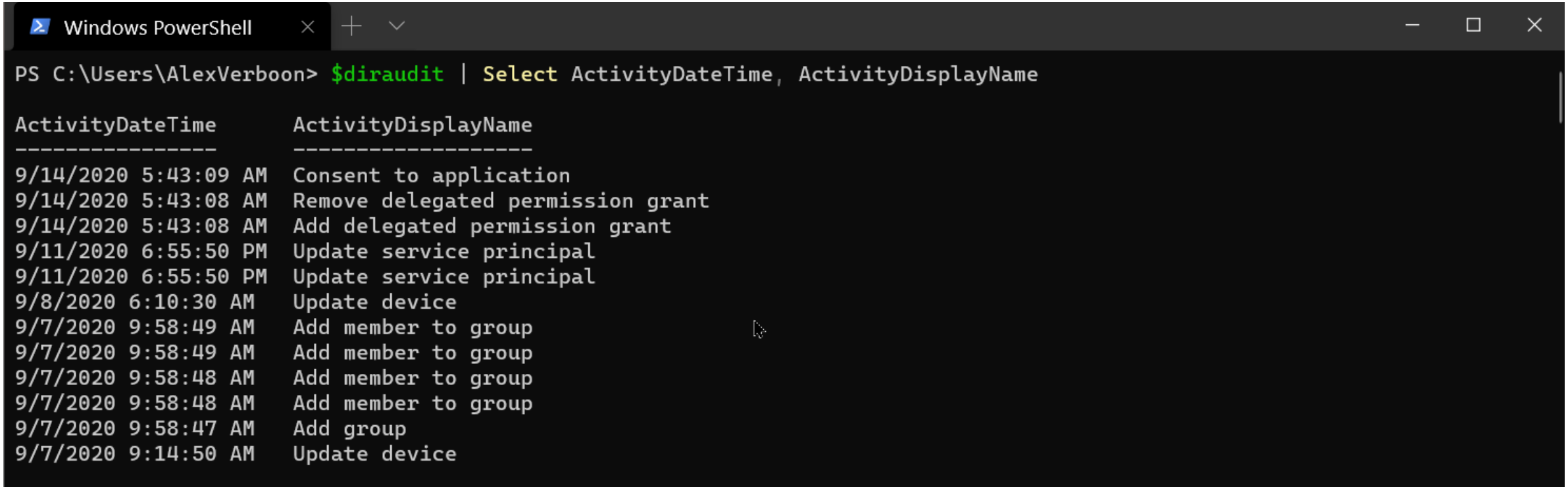
Windows PowerShell | PowerShell Core

```
PS C:\> Get-MgSecurityAlert | Select-object EventDateTime, Category, Title

EventDateTime         Category                                                                Title
-------------         --------                                                                -----
8/18/2020 5:28:23 PM  c46c4e10-5d81-409a-9fbb-3857dc9db495_d8270f6f-9dc0-4e28-a035-c65bd31b6e76 SharePointFileOperatio…
9/8/2020 6:14:07 AM   Malware                                                                 'PowerView' hacktool w…
9/8/2020 9:21:32 AM   UnwantedSoftware                                                        'EICAR_Test_File' unwa…
9/8/2020 9:21:32 AM   UnwantedSoftware                                                        'EICAR_Test_File' unwa…
9/8/2020 9:22:19 AM   Malware                                                                 'Wacatac' malware was …
9/8/2020 7:53:18 AM   Execution                                                               [Test Alert] Suspiciou…
9/8/2020 6:16:48 AM   Malware                                                                 'Sehyioa' malware was …
9/8/2020 6:16:48 AM   Malware                                                                 'Wacatac' malware was …
9/8/2020 6:13:28 AM   DefenseEvasion                                                          A process was injected…
9/7/2020 8:57:46 AM   Execution                                                               [Test Alert] Suspiciou…
9/6/2020 12:26:40 PM  Malware                                                                 'Meterpreter' malware …
9/6/2020 12:27:57 PM  Malware                                                                 'Meterpreter' hacktool…
9/6/2020 12:38:16 PM  Malware                                                                 'Ploty' malware was pr…
9/6/2020 12:38:16 PM  DefenseEvasion                                                          A process was injected…
9/2/2020 5:25:31 PM   InitialAccess                                                           Connection to a custom…
9/2/2020 5:25:31 PM   InitialAccess                                                           Connection to a custom…
9/2/2020 5:27:30 PM   InitialAccess                                                           Connection to a custom…
9/2/2020 5:28:23 PM   InitialAccess                                                           Connection to a custom…
9/2/2020 5:24:57 PM   Persistence                                                             local account created
9/1/2020 2:57:31 PM   Execution                                                               firefox usage detected
8/27/2020 9:57:33 AM  LateralMovement                                                         Suspicious remote Powe…
8/27/2020 9:57:33 AM  LateralMovement                                                         Suspicious remote acti…
8/27/2020 9:57:37 AM  Malware                                                                 'Injector' malware was…
8/27/2020 9:57:33 AM  Execution                                                               Suspicious PowerShell …
```

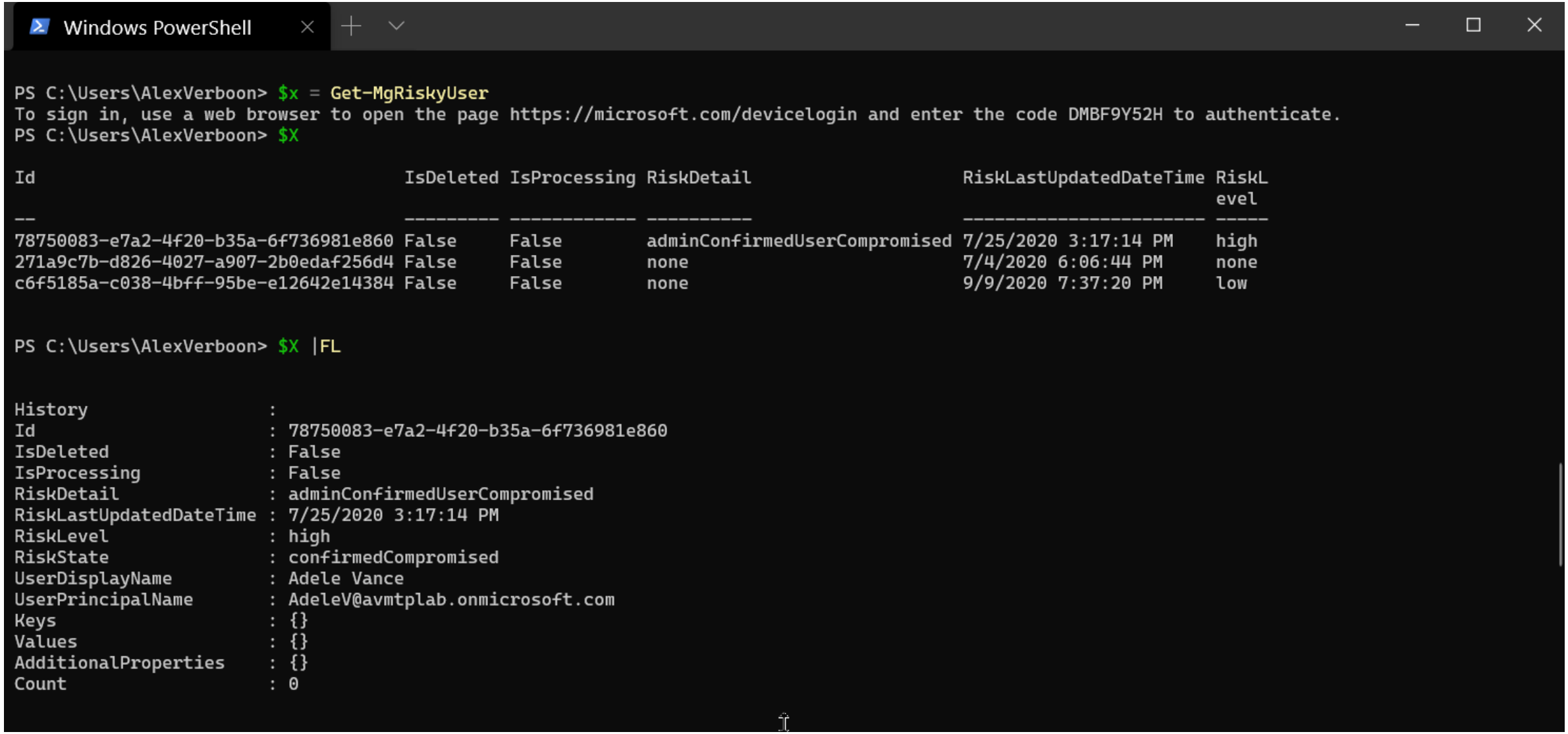

Windows PowerShell
PS C:\Users\AlexVerboon> $signin = Get-MgAuditLogSignIn

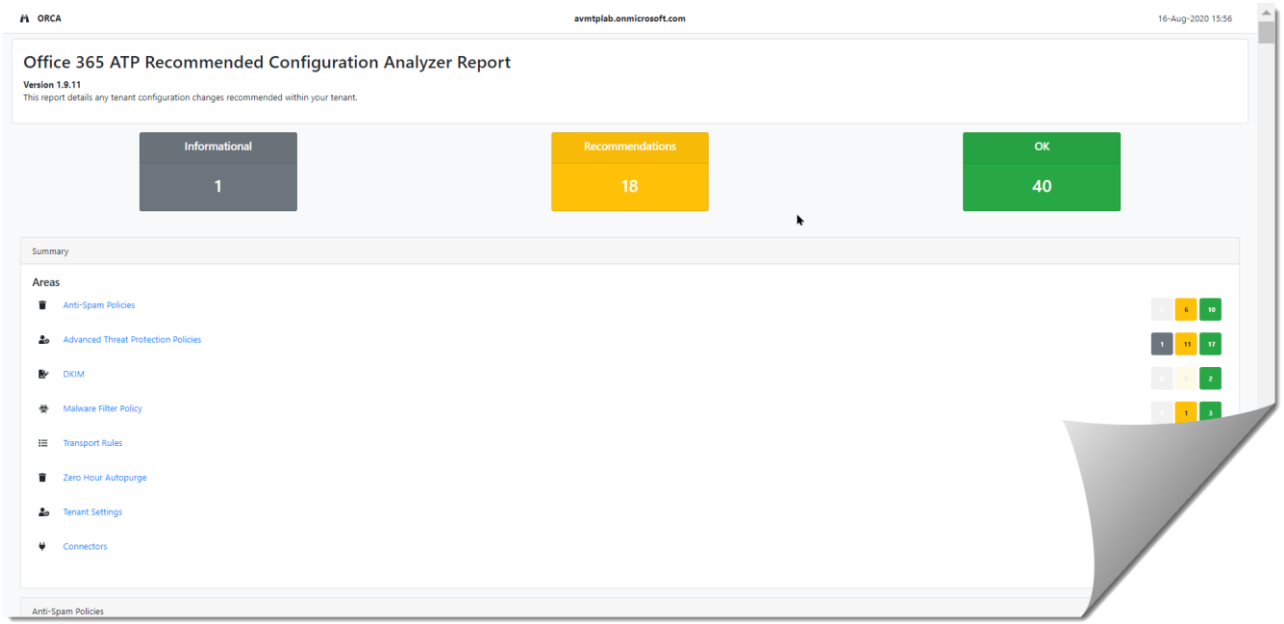

Windows PowerShell
PS C:\Users\AlexVerboon> $signin | Select UserDisplayName, RiskState, IpAddress | where RiskState -ne 'none'
UserDisplayName RiskState IPAddress
org admin atRisk 212.77.61.26
org admin atRisk 104.47.146.40
org admin atRisk 13.93.68.229
PS C:\Users\AlexVerboon>


Windows PowerShell
PS C:\Users\AlexVerboon> $diraudit = Get-MgAuditLogDirectoryAudit


Windows PowerShell
PS C:\Users\AlexVerboon> $diraudit | Select ActivityDateTime, ActivityDisplayName
ActivityDateTime ActivityDisplayName
9/14/2020 5:43:09 AM Consent to application
9/14/2020 5:43:08 AM Remove delegated permission grant
9/14/2020 5:43:08 AM Add delegated permission grant
9/11/2020 6:55:50 PM Update service principal
9/11/2020 6:55:50 PM Update service principal
9/8/2020 6:10:30 AM Update device
9/7/2020 9:58:49 AM Add member to group
9/7/2020 9:58:49 AM Add member to group
9/7/2020 9:58:48 AM Add member to group
9/7/2020 9:58:48 AM Add member to group
9/7/2020 9:58:47 AM Add group
9/7/2020 9:14:50 AM Update device

Managing the Microsoft Security stack with PowerShell – Microsoft Graph





The Office 365 ATP Recommended Configuration Analyzer (ORCA)
https://github.com/cammurray/orca

Managing the Microsoft Security stack with PowerShell – Office 365 ATP Recommended Configuration Analyzer

Windows PowerShell | PowerShell Core

```
PS C:\> find-module -name Orca

Version              Name                                Repository           Description
-------              ----                                ----------           -----------
1.9.11               ORCA                                PSGallery            Office 365 Advanced Threat Prote...

PS C:\> find-module -name Orca | install-module -Scope CurrentUser
```

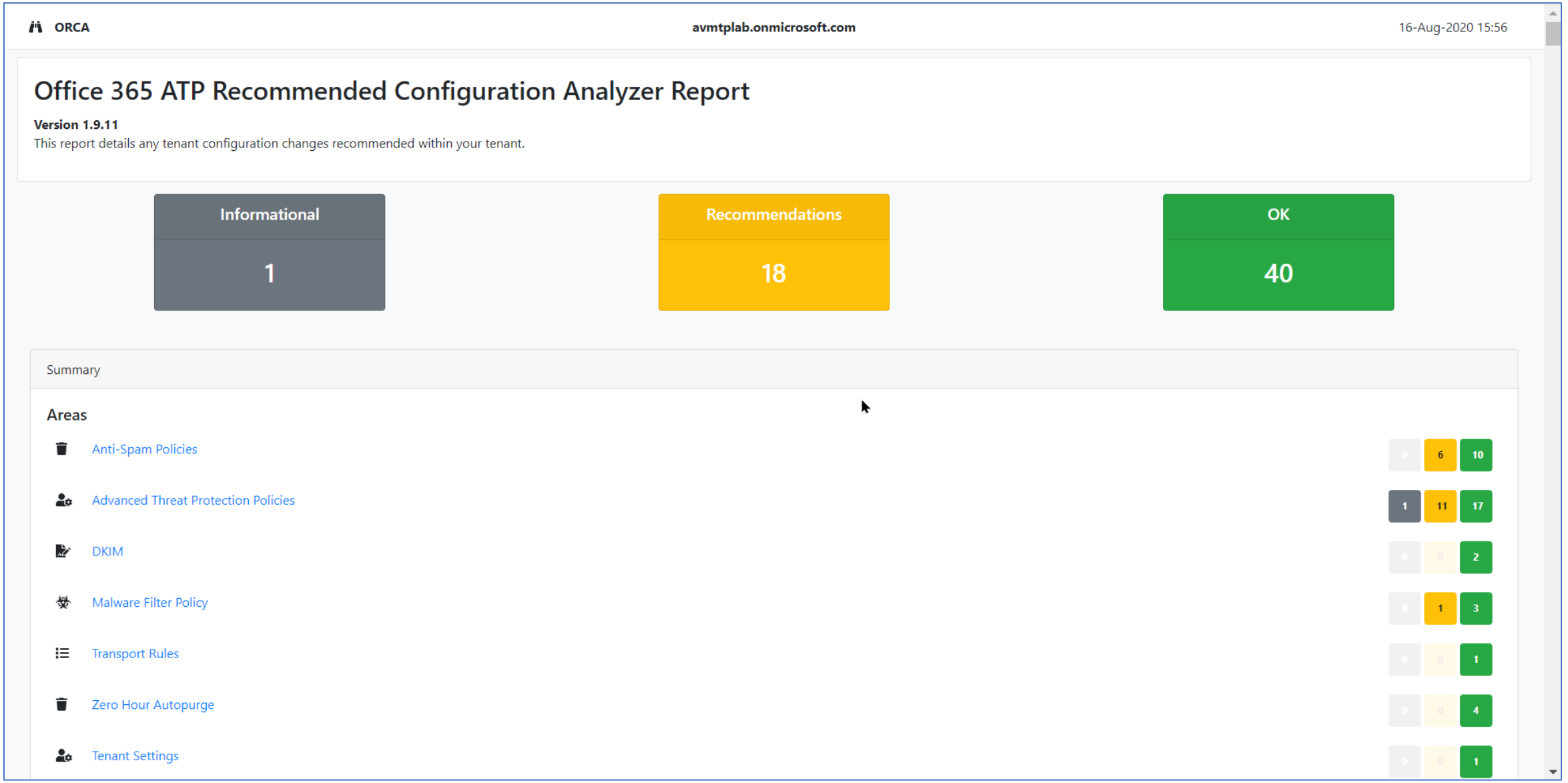
Windows PowerShell | PowerShell Core

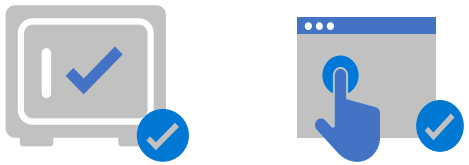
```
PS C:\> Get-ORCAReport
```

Windows PowerShell | PowerShell Core

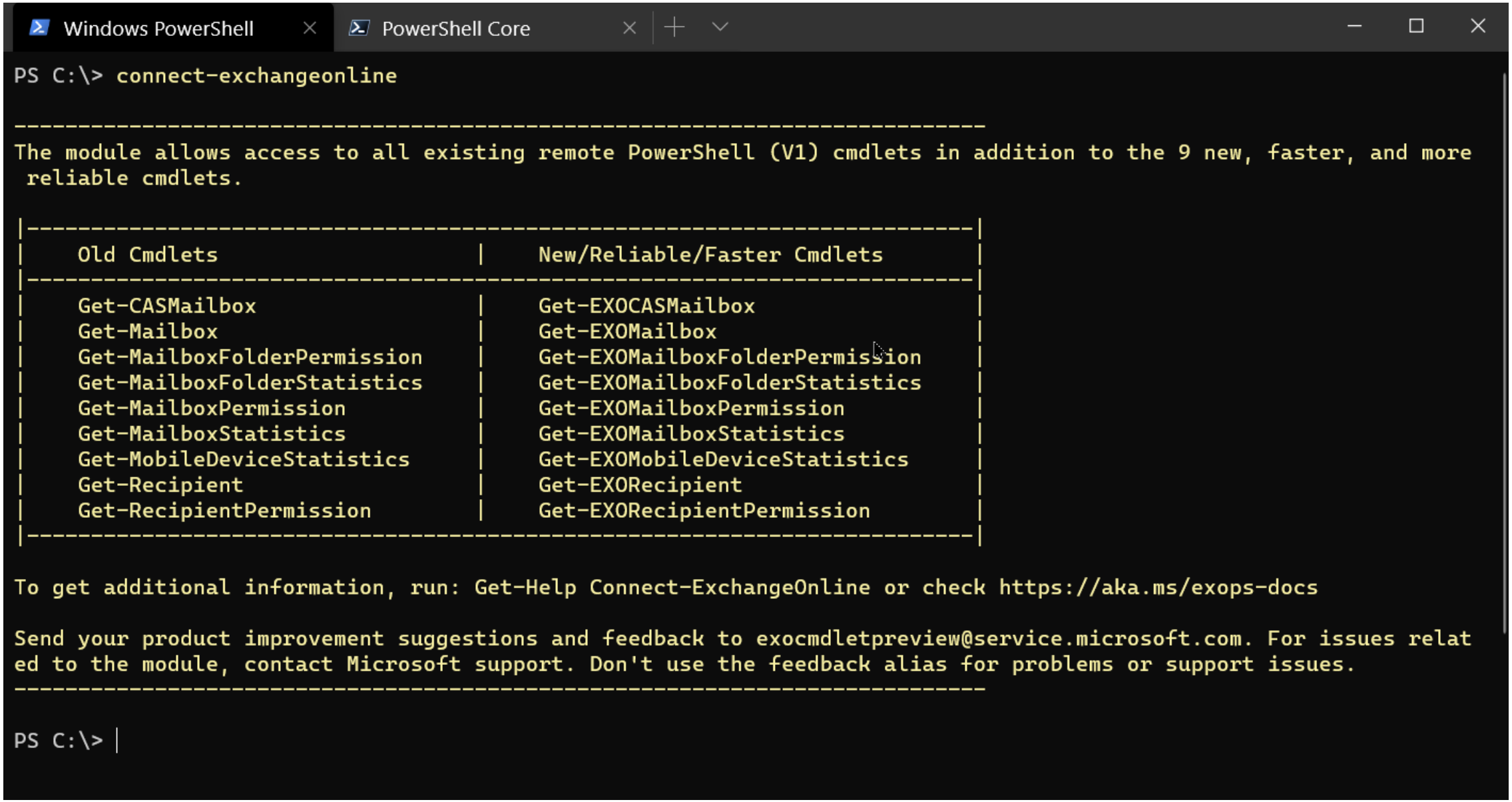
```
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - IP Allow Lists
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - Advanced Spam Filter (ASF)
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - Outbound spam filter policy settings
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - End-user Spam notifications
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - Quarantine retention period
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - High Confidence Phish Action
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - Allowed Senders
08/16/2020 15:56:04 Analysis - Anti-Spam Policies - High Confidence Spam Action
08/16/2020 15:56:05 Analysis - Anti-Spam Policies - Bulk Complaint Level
08/16/2020 15:56:05 Analysis - Anti-Spam Policies - Spam Action
08/16/2020 15:56:05 Analysis - Anti-Spam Policies - Mark Bulk as Spam
08/16/2020 15:56:05 Analysis - Connectors - Domains
08/16/2020 15:56:05 Analysis - Connectors - Enhanced Filtering Configuration
08/16/2020 15:56:05 Analysis - DKIM - Signing Configuration
08/16/2020 15:56:05 Analysis - DKIM - DNS Records
08/16/2020 15:56:08 Analysis - Malware Filter Policy - External Sender Notifications
08/16/2020 15:56:08 Analysis - Malware Filter Policy - Malware Filter Policy Policy Rules
08/16/2020 15:56:08 Analysis - Malware Filter Policy - Common Attachment Type Filter
08/16/2020 15:56:09 Analysis - Malware Filter Policy - Internal Sender Notifications
08/16/2020 15:56:09 Analysis - Tenant Settings - Unified Audit Log
08/16/2020 15:56:09 Analysis - Transport Rules - Domain Whitelisting
08/16/2020 15:56:09 Analysis - Zero Hour Autopurge - Supported filter policy action
08/16/2020 15:56:09 Analysis - Zero Hour Autopurge - Zero Hour Autopurge Enabled for Malwa
re
08/16/2020 15:56:09 Analysis - Zero Hour Autopurge - Zero Hour Autopurge Enabled for Phish
08/16/2020 15:56:09 Analysis - Zero Hour Autopurge - Zero Hour Autopurge Enabled for Spam
08/16/2020 15:56:09 Generating Output
08/16/2020 15:56:09 Output - HTML
08/16/2020 15:56:11 Complete! Output is in C:\Users\AlexVerboon\AppData\Local\Microsoft\OR
CA\ORCA-avmtplab-202008161556.html
PS C:\>
```

Managing the Microsoft Security stack with PowerShell – Office 365 ATP Recommended Configuration Analyzer





Office 365 Advanced Threat Protection


Windows PowerShell
PowerShell Core
PS C:\> connect-exchangeonline
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more reliable cmdlets.
Old Cmdlets | New/Reliable/Faster Cmdlets
Get-CASMailbox | Get-EXOCASMailbox
Get-Mailbox | Get-EXOMailbox
Get-MailboxFolderPermission | Get-EXOMailboxFolderPermission
Get-MailboxFolderStatistics | Get-EXOMailboxFolderStatistics
Get-MailboxPermission | Get-EXOMailboxPermission
Get-MailboxStatistics | Get-EXOMailboxStatistics
Get-MobileDeviceStatistics | Get-EXOMobileDeviceStatistics
Get-Recipient | Get-EXORecipient
Get-RecipientPermission | Get-EXORecipientPermission
To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs
Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.
PS C:\>

Managing the Microsoft Security stack with PowerShell – Office ATP - Safe Attachments

```
Windows PowerShell

PS C:\> Get-SafeAttachmentPolicy | where Name -eq "Global - Safe Attachments" |fl


RunspaceId                    : 54f67ea9-29e3-42e7-a599-a6583c4f96f5
RedirectAddress               : mvpadmin@avmtplab.onmicrosoft.com
Redirect                      : True
Action                        : DynamicDelivery
ScanTimeout                   : 30
ConfidenceLevelThreshold      : 80
OperationMode                 : Delay
Enable                        : True
ActionOnError                 : True
RecommendedPolicyType         : Custom
IsDefault                     : False
AdminDisplayName              : Safe Attachments policy for all users
EnableOrganizationBranding    : False
ExchangeVersion               : 0.20 (15.0.0.0)
Name                          : Global - Safe Attachments
DistinguishedName             : CN=Global - Safe Attachments,CN=Safe A
                                oft.com,CN=ConfigurationUnits,DC=CHEP2
Identity                      : Global - Safe Attachments
ObjectCategory                : CHEP278A003.PROD.OUTLOOK.COM/Configura
ObjectClass                   : {top, msExchSafeAttachmentProtectionCo
WhenChanged                   : 6/29/2020 8:43:57 AM
WhenCreated                   : 6/29/2020 8:43:45 AM
WhenChangedUTC                : 6/29/2020 6:43:57 AM
WhenCreatedUTC                : 6/29/2020 6:43:45 AM
ExchangeObjectId              : 35477c0e-b2ab-411d-b5f4-8352a2af18f5
OrganizationId                : CHEP278A003.PROD.OUTLOOK.COM/Microsoft
                                CHEP278A003.PROD.OUTLOOK.COM/Configura
Id                            : Global - Safe Attachments
Guid                          : 35477c0e-b2ab-411d-b5f4-8352a2af18f5
OriginatingServer             : DB6P278A03DC002.CHEP278A003.PROD.OUTLO
IsValid                       : True
ObjectState                   : Unchanged
```

Global - Safe Attachments

Editing Settings

Monitor, Replace and Block actions may cause significant delay to email delivery. Learn more
Dynamic Delivery is only available for recipients with hosted mailboxes. Learn more
If you choose the Block, Replace or Dynamic Delivery options and malware is detected in attachment, the message containing the attachment will be quarantined and can be released only by an admin.

- ○ Off - Attachment will not be scanned for malware.
- ○ Monitor - Continue delivering the message after malware is detected; track scan results.
- ○ Block - Block the current and future email and attachments with detected malware.
- ○ Replace - Block the attachments with detected malware, continue to deliver the message.
- ◉ Dynamic Delivery (Preview Feature)- Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection

Send the blocked, monitored, or replaced attachment to an email address.

☑ Enable redirect ⓘ

Send the attachment to the following email address *

mvpadmin@avmtplab.onmicrosoft.com

Managing the Microsoft Security stack with PowerShell – Office ATP – Safe Attachments

Windows PowerShell

```
PS C:\> $rule = Get-SafeAttachmentPolicy | where Name -eq "Global - Safe Attachments" | Get-SafeAttachmentRule
PS C:\> $rule | fl


RunspaceId                : 084db004-fe56-4b8f-9698-067a1af0eb57
SafeAttachmentPolicy      : Global - Safe Attachments
State                     : Enabled
Priority                  : 0
Comments                  :
Description               : If the message:
                                recipients's address domain portion belo
                            'avmtplab.onmicrosoft.com'
                            Take the following actions:
                                Apply safe attachment policy "Global - S

RuleVersion               : 15.0.5.2
SentTo                    :
SentToMemberOf            :
RecipientDomainIs         : {verboon.online, avmtplab.onmicrosoft.com}
ExceptIfSentTo            :
ExceptIfSentToMemberOf    :
ExceptIfRecipientDomainIs :
Conditions                : {Microsoft.Exchange.MessagingPolicies.Rules.
Exceptions                :
Identity                  : Global - Safe Attachments
DistinguishedName         : CN=Global - Safe Attachments,CN=SafeAttachme
                            vmtplab.onmicrosoft.com,CN=ConfigurationUnit
Guid                      : c0f4dadb-9dfe-40fc-a897-ed5ccd69ceea
ImmutableId               : c0f4dadb-9dfe-40fc-a897-ed5ccd69ceea
OrganizationId            : CHEP278A003.PROD.OUTLOOK.COM/Microsoft Excha
                            CHEP278A003.PROD.OUTLOOK.COM/ConfigurationUn
Name                      : Global - Safe Attachments
IsValid                   : True
WhenChanged               : 6/29/2020 8:43:57 AM
ExchangeVersion           : 0.1 (8.0.535.0)
ObjectState               : Unchanged
```

Global - Safe Attachments

Editing Applied to

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

The recipient domain is

Any of these

verboon.online,avmtplab.onmicrosoft.com

Choose

(2 selected)

Add a condition

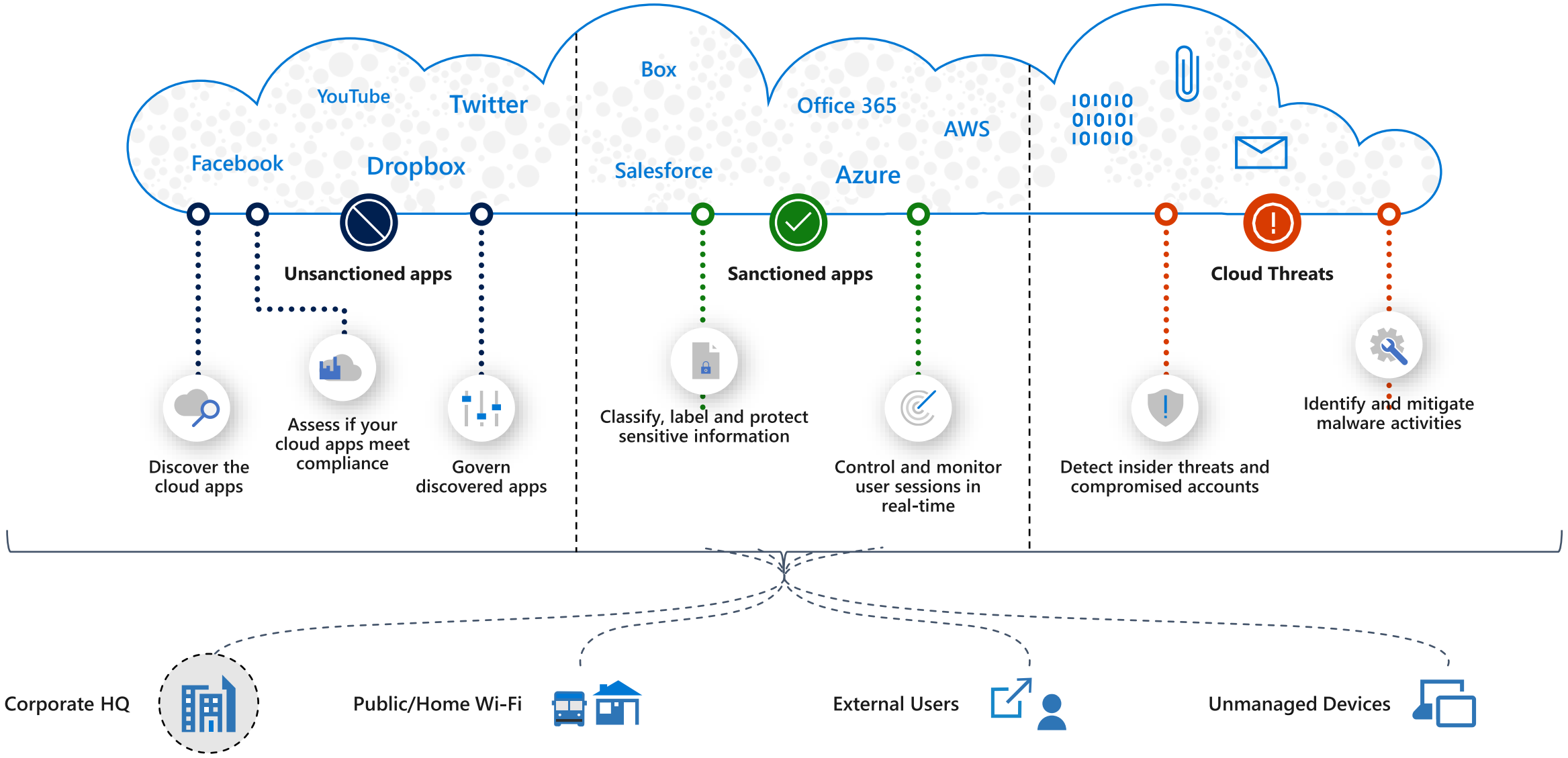
Save

Cancel

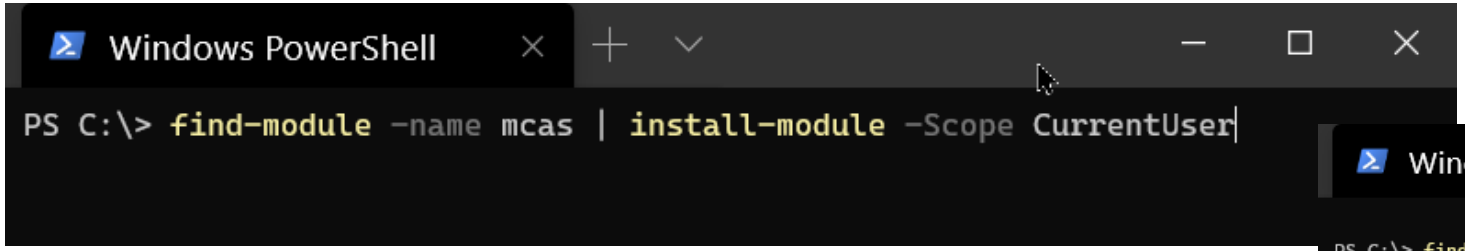
Managing the Microsoft Security stack with PowerShell – **Office ATP – DKIM**

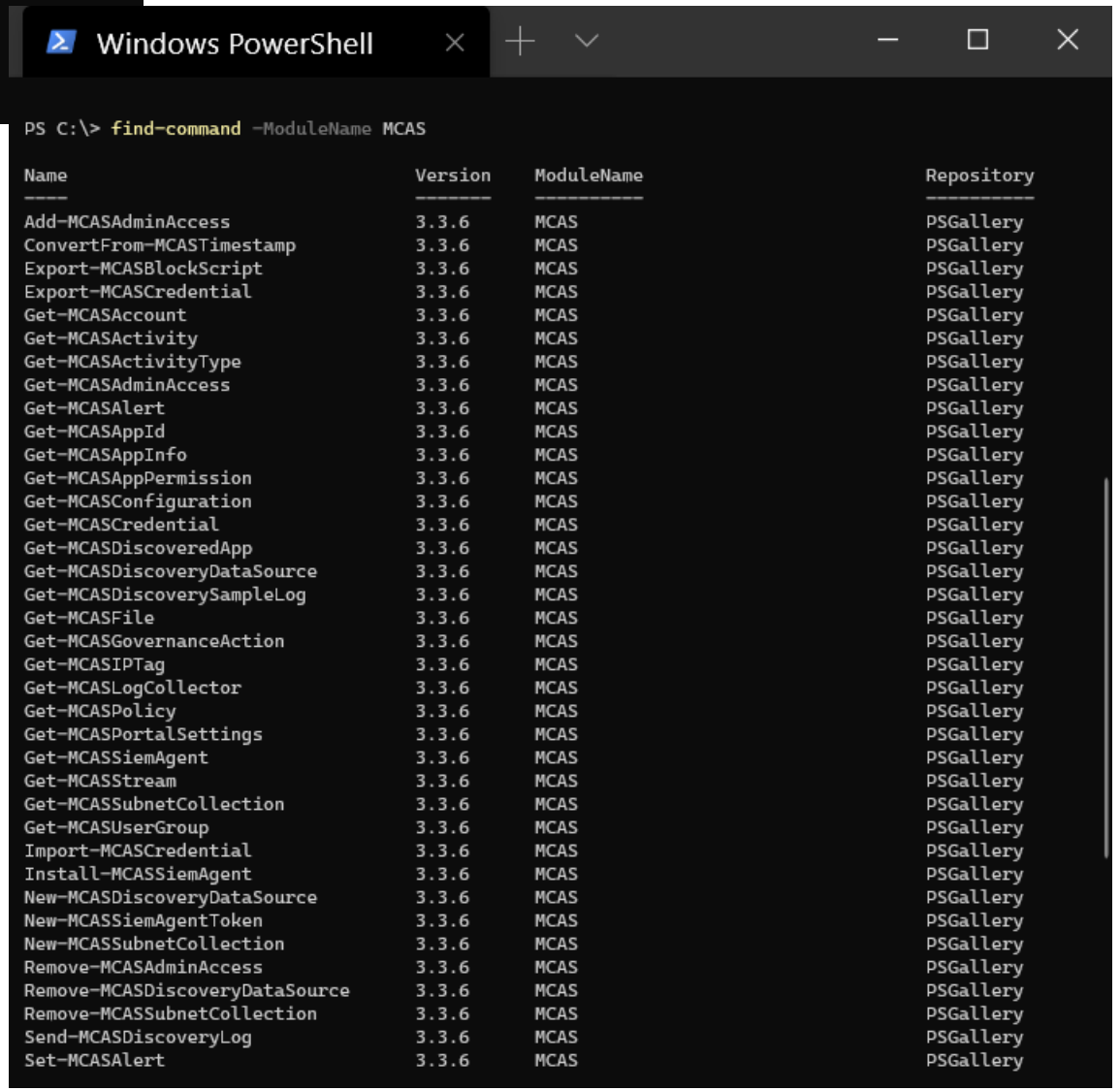
Unofficial Microsoft Cloud App Security PowerShell Module
https://github.com/Microsoft/MCAS

Managing the Microsoft Security stack with PowerShell – Microsoft Cloud App Security



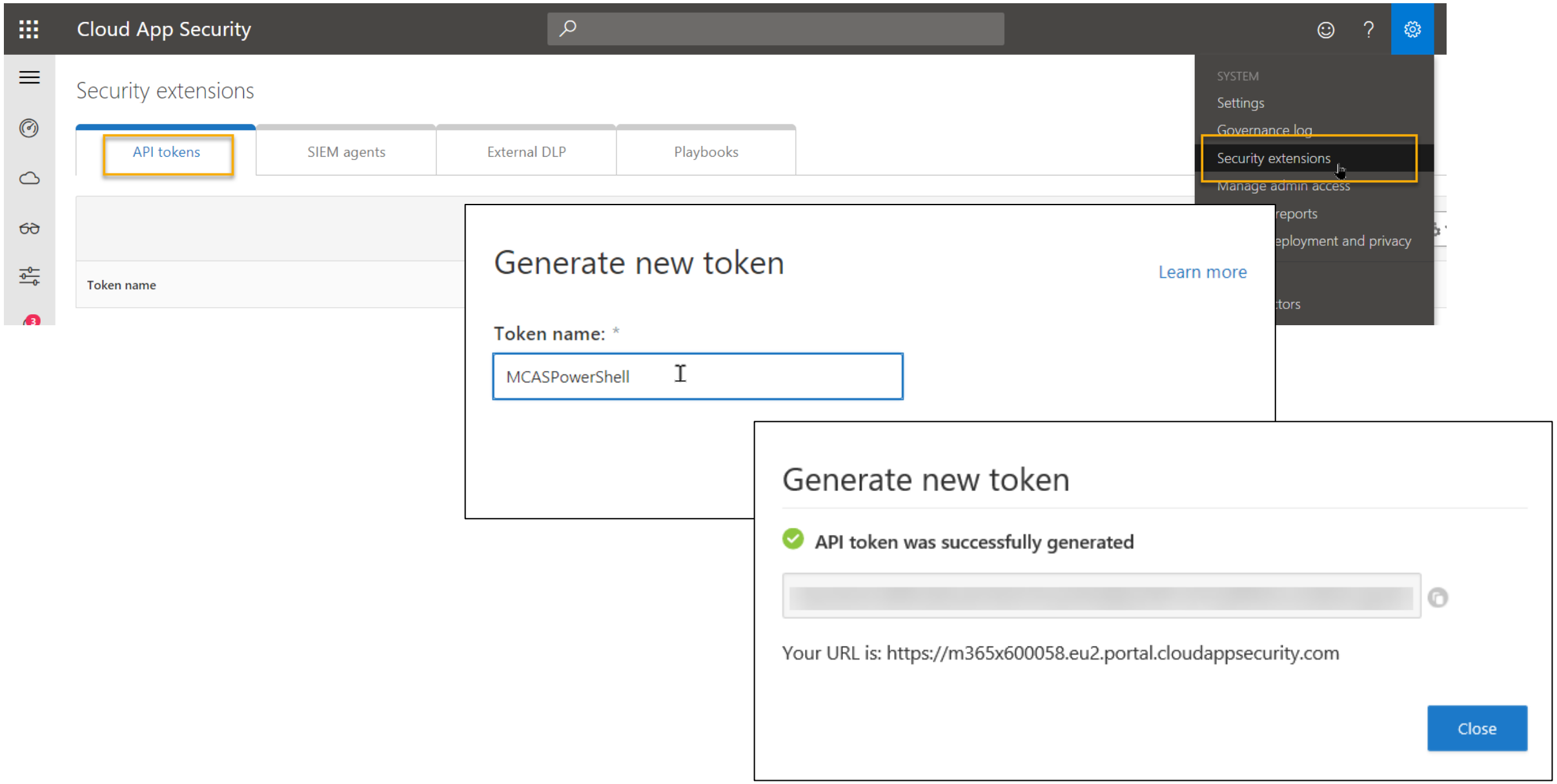
Managing the Microsoft Security stack with PowerShell – Microsoft Cloud App Security





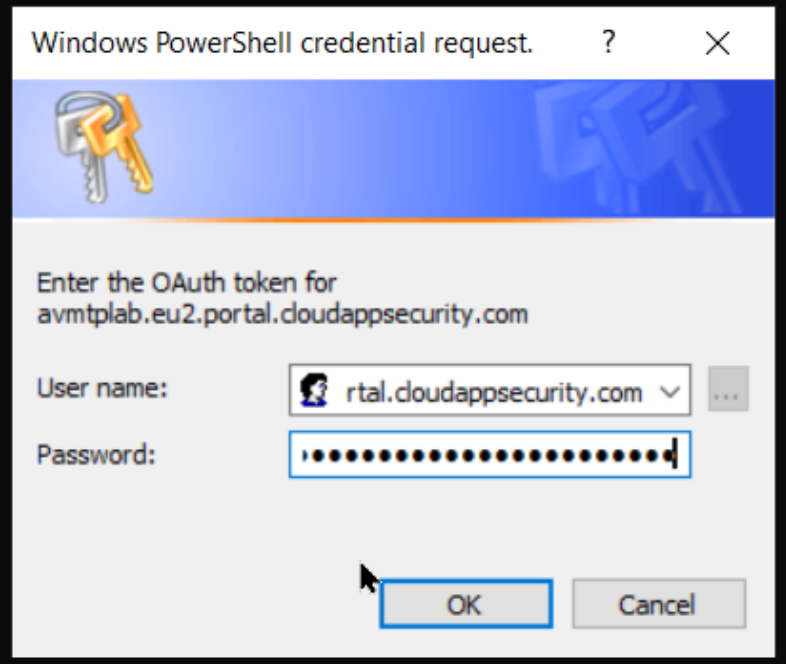
Name	Version	ModuleName	Repository
Add-MCASAdminAccess	3.3.6	MCAS	PSGallery
ConvertFrom-MCASTimestamp	3.3.6	MCAS	PSGallery
Export-MCASBlockScript	3.3.6	MCAS	PSGallery
Export-MCASCredential	3.3.6	MCAS	PSGallery
Get-MCASAccount	3.3.6	MCAS	PSGallery
Get-MCASActivity	3.3.6	MCAS	PSGallery
Get-MCASActivityType	3.3.6	MCAS	PSGallery
Get-MCASAdminAccess	3.3.6	MCAS	PSGallery
Get-MCASAlert	3.3.6	MCAS	PSGallery
Get-MCASAppId	3.3.6	MCAS	PSGallery
Get-MCASAppInfo	3.3.6	MCAS	PSGallery
Get-MCASAppPermission	3.3.6	MCAS	PSGallery
Get-MCASConfiguration	3.3.6	MCAS	PSGallery
Get-MCASCredential	3.3.6	MCAS	PSGallery
Get-MCASDiscoveredApp	3.3.6	MCAS	PSGallery
Get-MCASDiscoveryDataSource	3.3.6	MCAS	PSGallery
Get-MCASDiscoverySampleLog	3.3.6	MCAS	PSGallery
Get-MCASFile	3.3.6	MCAS	PSGallery
Get-MCASGovernanceAction	3.3.6	MCAS	PSGallery
Get-MCASIPTag	3.3.6	MCAS	PSGallery
Get-MCASLogCollector	3.3.6	MCAS	PSGallery
Get-MCASPolicy	3.3.6	MCAS	PSGallery
Get-MCASPortalSettings	3.3.6	MCAS	PSGallery
Get-MCASSiemAgent	3.3.6	MCAS	PSGallery
Get-MCASStream	3.3.6	MCAS	PSGallery
Get-MCASSubnetCollection	3.3.6	MCAS	PSGallery
Get-MCASUserGroup	3.3.6	MCAS	PSGallery
Import-MCASCredential	3.3.6	MCAS	PSGallery
Install-MCASSiemAgent	3.3.6	MCAS	PSGallery
New-MCASDiscoveryDataSource	3.3.6	MCAS	PSGallery
New-MCASSiemAgentToken	3.3.6	MCAS	PSGallery
New-MCASSubnetCollection	3.3.6	MCAS	PSGallery
Remove-MCASAdminAccess	3.3.6	MCAS	PSGallery
Remove-MCASDiscoveryDataSource	3.3.6	MCAS	PSGallery
Remove-MCASSubnetCollection	3.3.6	MCAS	PSGallery
Send-MCASDiscoveryLog	3.3.6	MCAS	PSGallery
Set-MCASAlert	3.3.6	MCAS	PSGallery

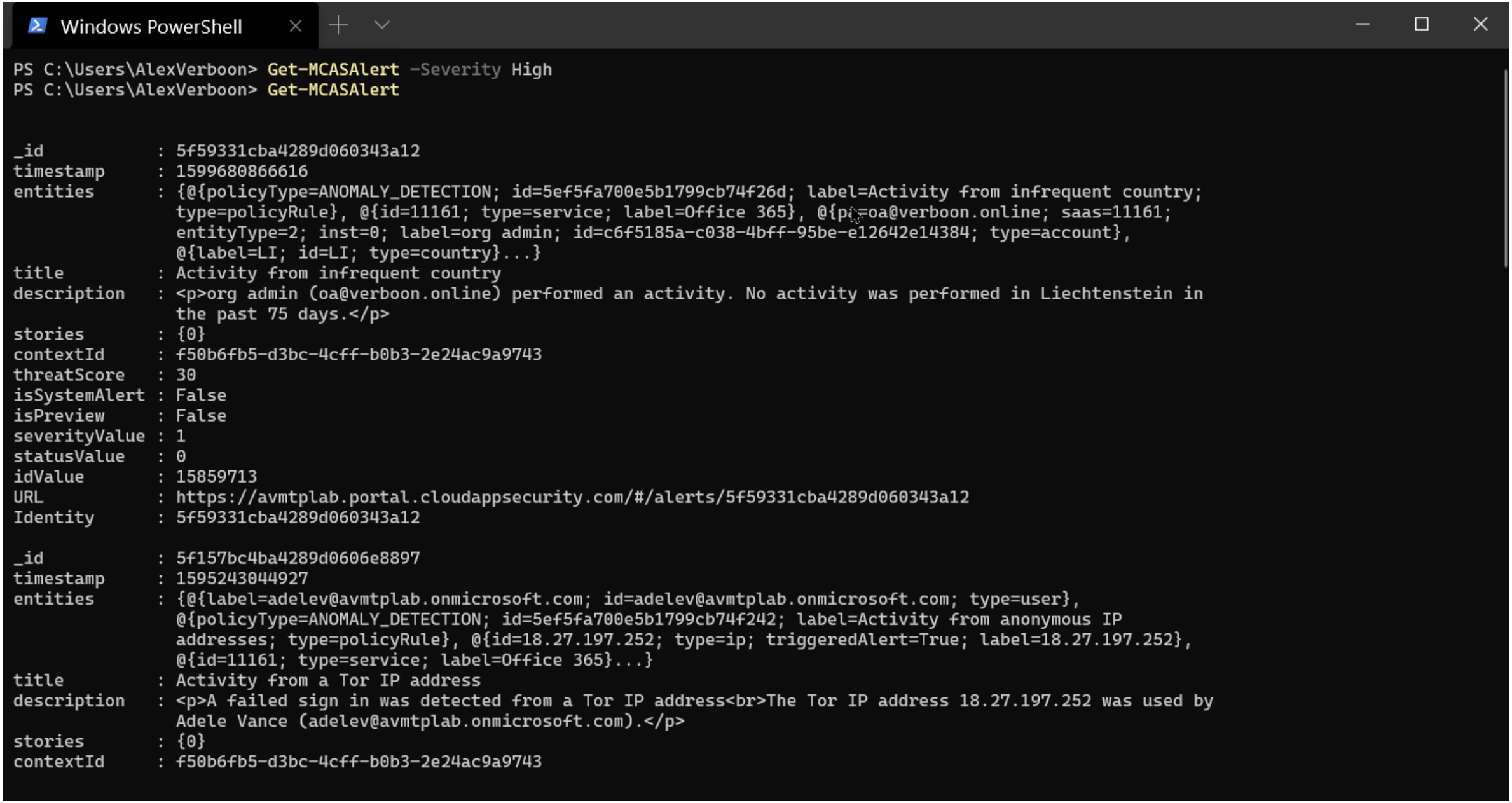
Managing the Microsoft Security stack with PowerShell – Microsoft Cloud App Security



Windows PowerShell

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\AlexVerboon>
PS C:\Users\AlexVerboon> Get-MCASCredential -TenantUri "avmtplab.eu2.portal.cloudappsecurity.com"
```



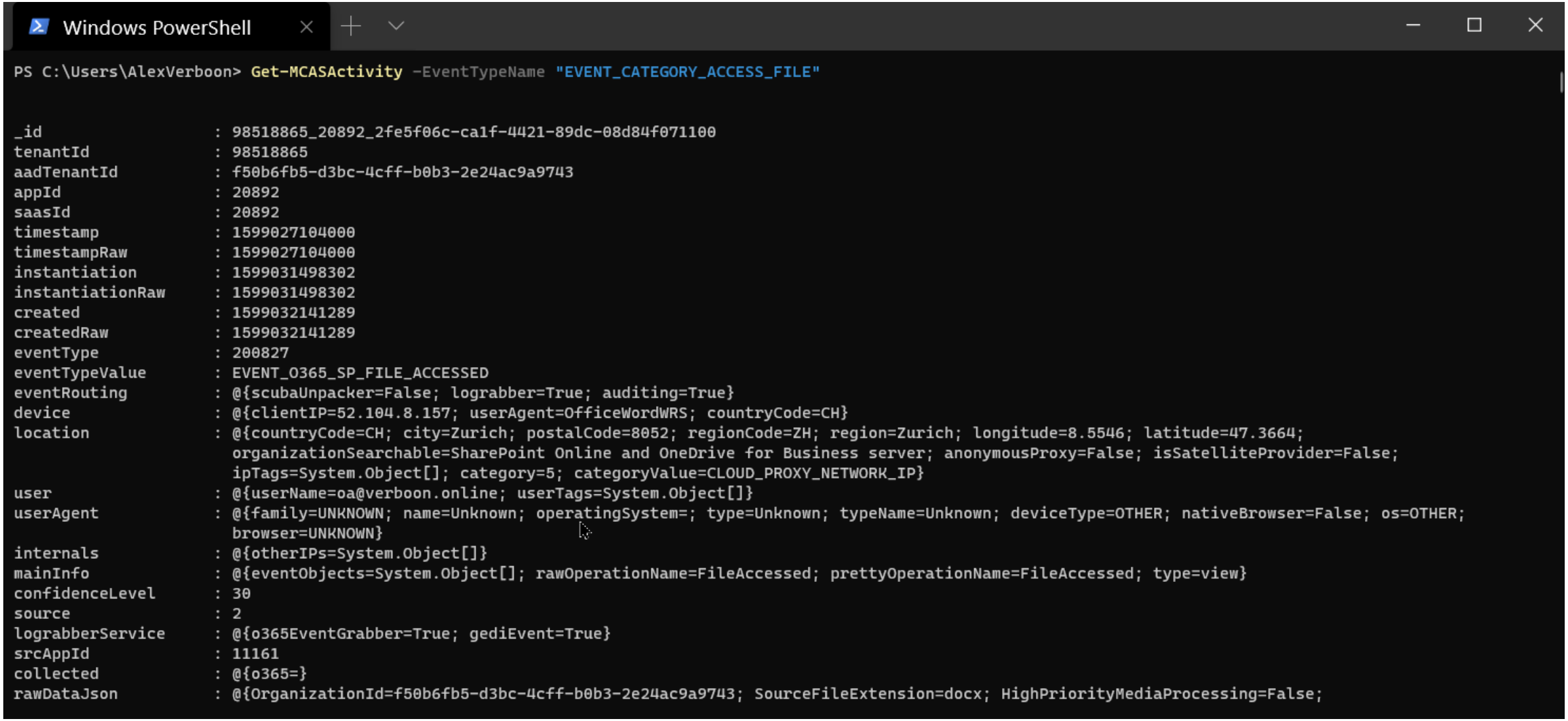

Windows PowerShell
PS C:\Users\AlexVerboon> Get-MCASAlert -Severity High
PS C:\Users\AlexVerboon> Get-MCASAlert
_id : 5f59331cba4289d060343a12
timestamp : 1599680866616
entities : {@{policyType=ANOMALY_DETECTION; id=5ef5fa700e5b1799cb74f26d; label=Activity from infrequent country; type=policyRule}, @{id=11161; type=service; label=Office 365}, @{p=oa@verboon.online; saas=11161; entityType=2; inst=0; label=org admin; id=c6f5185a-c038-4bff-95be-e12642e14384; type=account}, @{label=LI; id=LI; type=country}...}
title : Activity from infrequent country
description : org admin (oa@verboon.online) performed an activity. No activity was performed in Liechtenstein in the past 75 days.
stories : {0}
contextId : f50b6fb5-d3bc-4cff-b0b3-2e24ac9a9743
threatScore : 30
isSystemAlert : False
isPreview : False
severityValue : 1
statusValue : 0
idValue : 15859713
URL : https://avmtplab.portal.cloudappsecurity.com/#/alerts/5f59331cba4289d060343a12
Identity : 5f59331cba4289d060343a12
_id : 5f157bc4ba4289d0606e8897
timestamp : 1595243044927
entities : {@{label=adelev@avmtplab.onmicrosoft.com; id=adelev@avmtplab.onmicrosoft.com; type=user}, @{policyType=ANOMALY_DETECTION; id=5ef5fa700e5b1799cb74f242; label=Activity from anonymous IP addresses; type=policyRule}, @{id=18.27.197.252; type=ip; triggeredAlert=True; label=18.27.197.252}, @{id=11161; type=service; label=Office 365}...}
title : Activity from a Tor IP address
description : A failed sign in was detected from a Tor IP address
The Tor IP address 18.27.197.252 was used by Adele Vance (adelev@avmtplab.onmicrosoft.com).
stories : {0}
contextId : f50b6fb5-d3bc-4cff-b0b3-2e24ac9a9743

Managing the Microsoft Security stack with PowerShell – Microsoft Cloud App Security

Windows PowerShell

```
PS C:\Users\AlexVerboon> Get-MCASPolicy | Select Name,Description | format-table -AutoSize -Wrap

name                                                                description
----                                                                -----------
Suspicious OAuth app file download activities                       This policy scans the OAuth apps connected to your
                                                                    environment and triggers an alert when an app
                                                                    downloads multiple files from Microsoft SharePoint
                                                                    or Microsoft OneDrive in a manner that is uncommon
                                                                    for the user.
Preview: Suspicious change of CloudTrail logging service            This policy profiles your environment and triggers
                                                                    alerts when users perform suspicious changes to the
                                                                    CloudTrail logging service, which could indicate an
                                                                    attempted breach.
Suspicious email deletion activity (by user)                        This policy profiles your environment and triggers
                                                                    alerts when a user performs suspicious email
                                                                    deletion activities in a single session, which
                                                                    could indicate an attempted breach.
Preview: Suspicious Power BI report sharing                         This policy profiles your environment and triggers
                                                                    alerts when a user shared a Power BI report that
                                                                    may include sensitive information and may indicate
                                                                    a compromised account. The report was either shared
                                                                    with an external email address, published to the
                                                                    web, or a snapshot was delivered to an externally
                                                                    subscribed email address.
Multiple VM creation activities                                     This policy profiles your environment and triggers
                                                                    alerts when users perform multiple create VM
                                                                    activities in a single session with respect to the
                                                                    baseline learned, which could indicate an attempted
                                                                    breach.
Preview: Multiple Power BI report sharing activities                This policy profiles your environment and triggers
                                                                    alerts when users perform multiple share report in
                                                                    PowerBI activities in a single session with respect
                                                                    to the baseline learned, which could indicate an
                                                                    attempted breach.
Multiple storage deletion activities                                This policy profiles your environment and triggers
```

Managing the Microsoft Security stack with PowerShell – Microsoft Cloud App Security

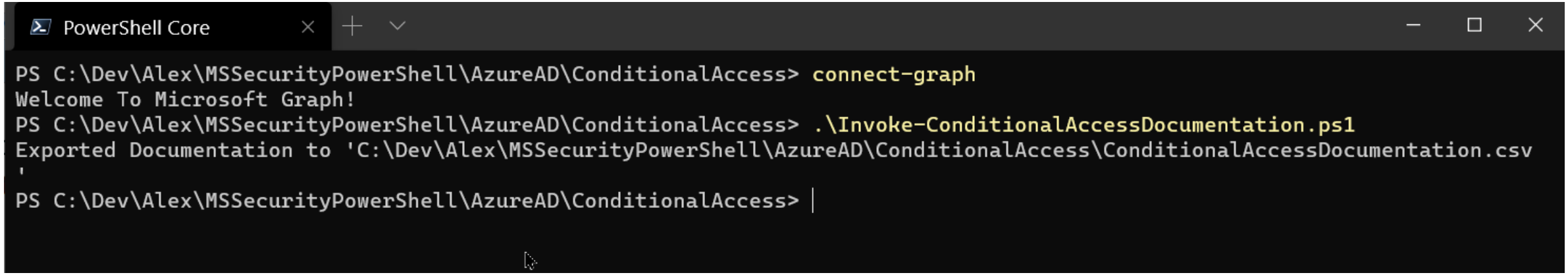


Managing the Microsoft Security stack with PowerShell – **Microsoft Cloud App Security**

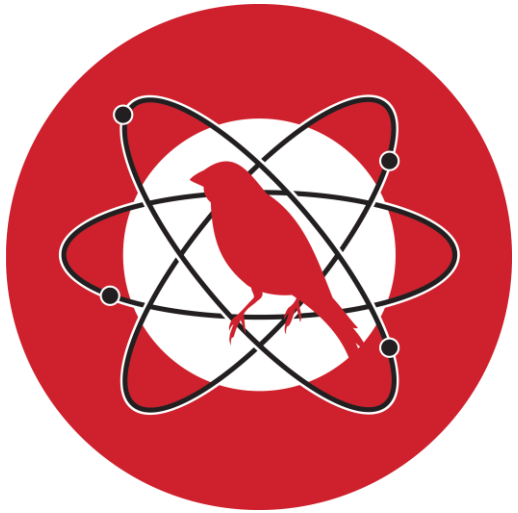
AzureAD Conditional Access

Document Conditional Access with PowerShell @nicolonsky, Nicolas Suter

https://github.com/nicolonsky/ConditionalAccessDocumentation



	TEST - Admin protection - All apps: Require MFA For M365 admins	TEST - Admin protection - All apps: Require trusted device For M365 admins	TEST - Base protection - All apps: Require MFA or trusted device or trusted location	TEST - Base protection - Register security information: Require trusted device or location	TEST - Attack surface reduction - All apps: Block legacy protocols	TEST - Attack surface reduction - All apps: Block access When using unknown or unsupported device platforms	TEST - Data protection - All apps: No persistent browser session When on untrusted device	TEST - Data protection - O365: Require app protection policy When using modern authentication clients on iOS or Android	TEST - Data protection - O365: Require trusted device When using modern authentication clients on Windows and macOS	TEST - Data protection - O365: Use app enforced restrictions When using a browser on untrusted devices
State	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled	enabled
Assignments										
IncludeUsers			All	All	All	All	All	All	All	All
IncludeGroups										
IncludeRoles	All (56)	All (56)								
ExcludeUsers				GuestsOrExternalUsers						
ExcludeGroups	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions	conditional-access-exclusions
ExcludeRoles										
Conditions										
IncludeApps	All	All	All		All	All	All	Office365	Office365	Office365
ExcludeApps										
IncludeUserActions				urn:user:registersecurityinfo						
ClientAppTypes					other easSupported easUnsupported			modern	modern	browser
IncludePlatforms						all		android iOS	windows macOS	
ExcludePlatforms						android iOS windows macOS				
IncludeLocations			All	All						
ExcludeLocations			AllTrusted	AllTrusted						
IncludeDeviceStates							All			All
ExcludeDeviceStates							Compliant DomainJoined			Compliant DomainJoined
Controls										
GrantControls	mfa	compliantDevice domainJoinedDevice	mfa compliantDevice domainJoinedDevice	compliantDevice domainJoinedDevice	block	block		compliantApplication approvedApplication	compliantDevice domainJoinedDevice	
GrantControlsOperator	OR	OR	OR	OR	OR	OR		AND	OR	
ApplicationEnforcedRestrictions										TRUE
CloudAppSecurity										
PersistentBrowser							never			
SignInFrequency							1 hours			

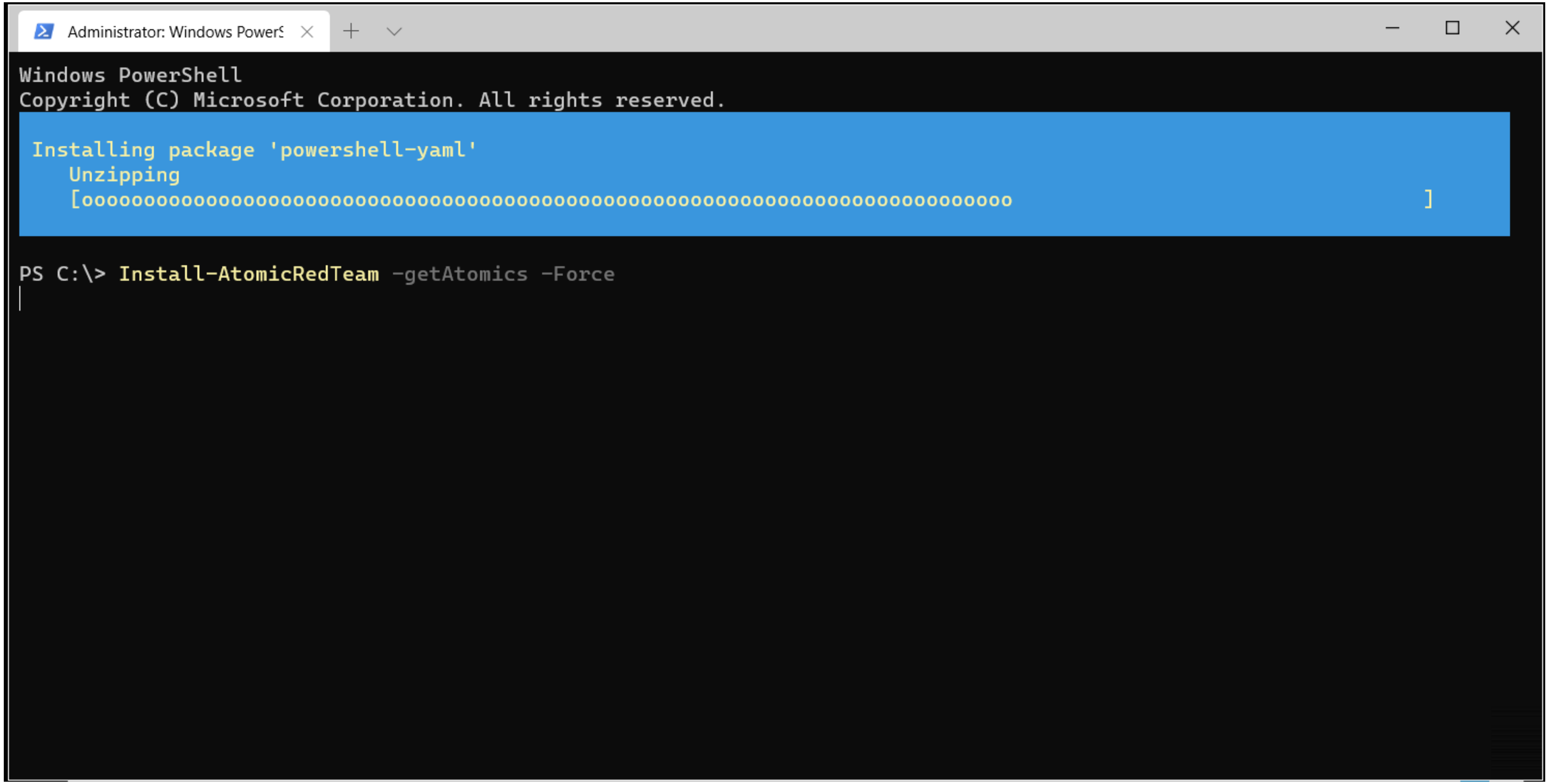


Attack Simulation with PowerShell

https://github.com/redcanaryco/invoke-atomicredteam/wiki

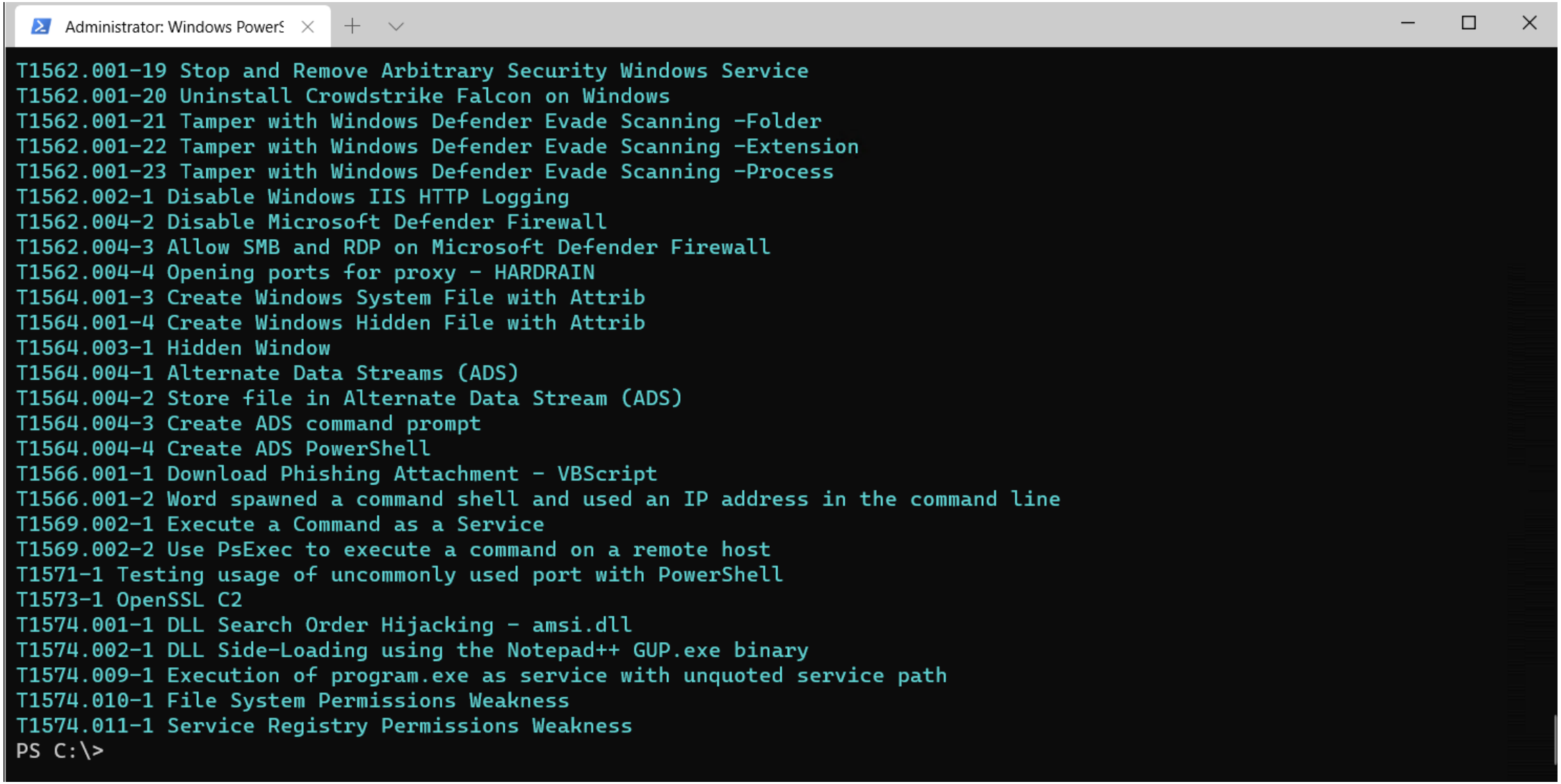
Managing the Microsoft Security stack with PowerShell – Atomic execution framework

```
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1');
Install-AtomicRedTeam -getAtomics -Force
```



Managing the Microsoft Security stack with PowerShell – **Atomic execution framework**

```
Invoke-AtomicTest All -ShowDetailsBrief
```



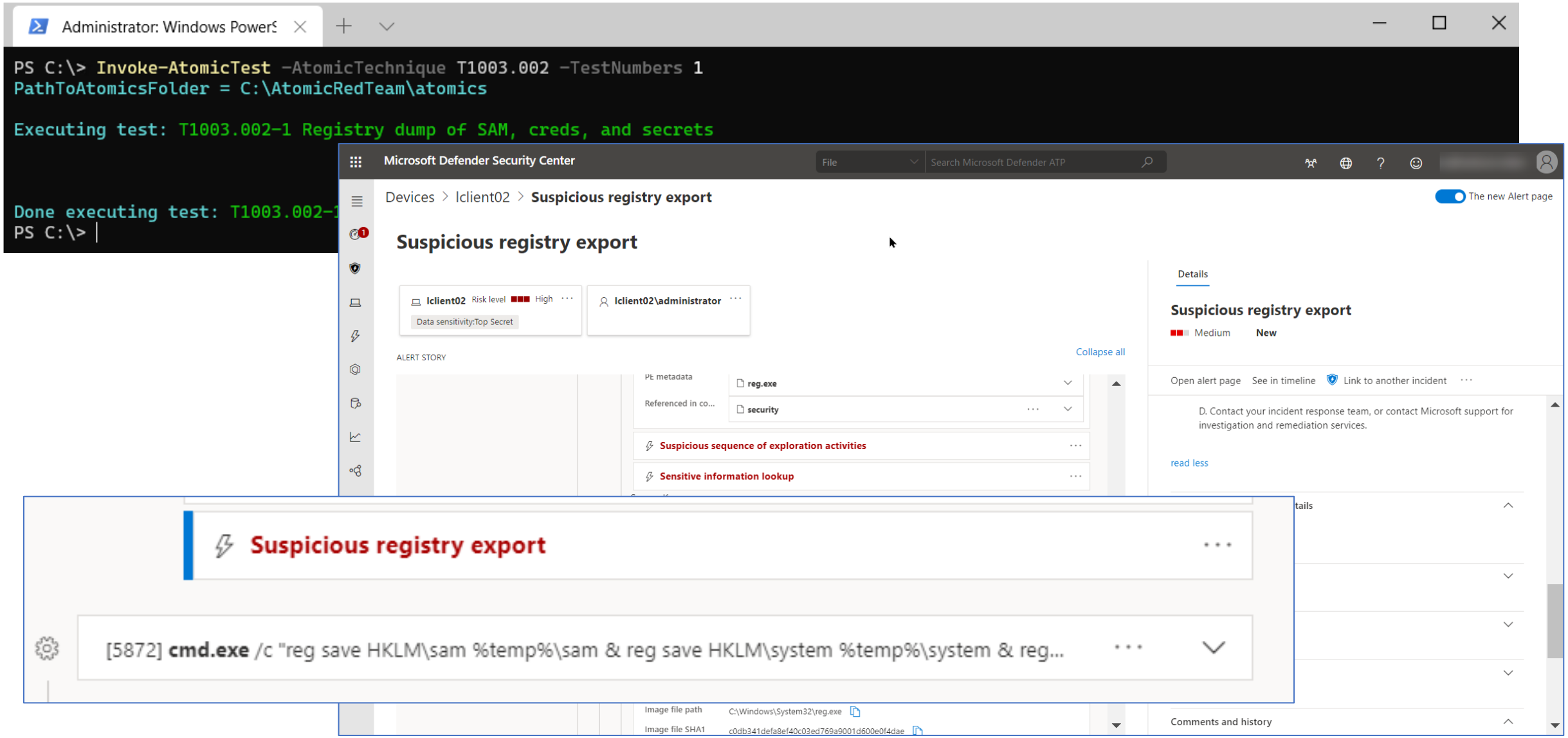
Managing the Microsoft Security stack with PowerShell – Atomic execution framework

```
Administrator: Windows PowerS
PS C:\> Invoke-AtomicTest All -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Powershell Mimikatz
T1003-2 Gsecdump
T1003-3 Credential Dumping with NPPSpy
T1003.001-1 Windows Credential Editor
T1003.001-2 Dump LSASS.exe Memory using ProcDump
T1003.001-3 Dump LSASS.exe Memory using comsvcs.dll
T1003.001-4 Dump LSASS.exe Memory using direct system calls and API unhooking
T1003.001-6 Offline Credential Theft With Mimikatz
T1003.001-7 LSASS read with pypykatz
T1003.002-1 Registry dump of SAM, creds, and secrets
T1003.002-2 Registry parse with pypykatz
T1003.002-3 esentutl.exe SAM copy
T1003.003-1 Create Volume Shadow Copy
T1003.003-2 Copy NTDS.dit from Volume
T1003.003-3 Dump Active Directory Data
T1003.003-4 Create Volume Shadow Copy
T1003.003-5 Create Volume Shadow Copy
T1003.003-6 Create Symlink to Volume S
T1003.004-1 Dumping LSA Secrets
T1007-1 System Service Discovery
T1007-2 System Service Discovery - net
```

```
Administrator: Windows PowerS
PS C:\> Invoke-AtomicTest -AtomicTechnique T1003.002 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
                                                                                [********BEGIN TEST*****
**]                                                                  Technique: OS Credential Dumping: Security Accou
nt Manager T1003.002                                    Atomic Test Name: Registry dump of SAM, creds, and secrets
                                          Atomic Test Number: 1
                        Atomic Test GUID: 5c2571d0-1572-416d-9676-812e64ca9f44
Description: Local SAM (SAM & System), cached credentials (System & Security) and LSA secrets (System & Security) can be enumerated via three re
gistry keys. Then processed locally using https://github.com/Neohapsis/creddump7              Upon successful execution of this test, you will
 find three files named, sam, system and security in the %temp% directory.

                        Attack Commands:
Executor: command_prompt
ElevationRequired: True
Command:
reg save HKLM\sam %temp%\sam
reg save HKLM\system %temp%\system
reg save HKLM\security %temp%\security

Cleanup Commands:
Command:
del %temp%\sam >nul 2> nul
del %temp%\system >nul 2> nul
del %temp%\security >nul 2> nul
[!!!!!!!!END TEST!!!!!!!]


PS C:\>
```

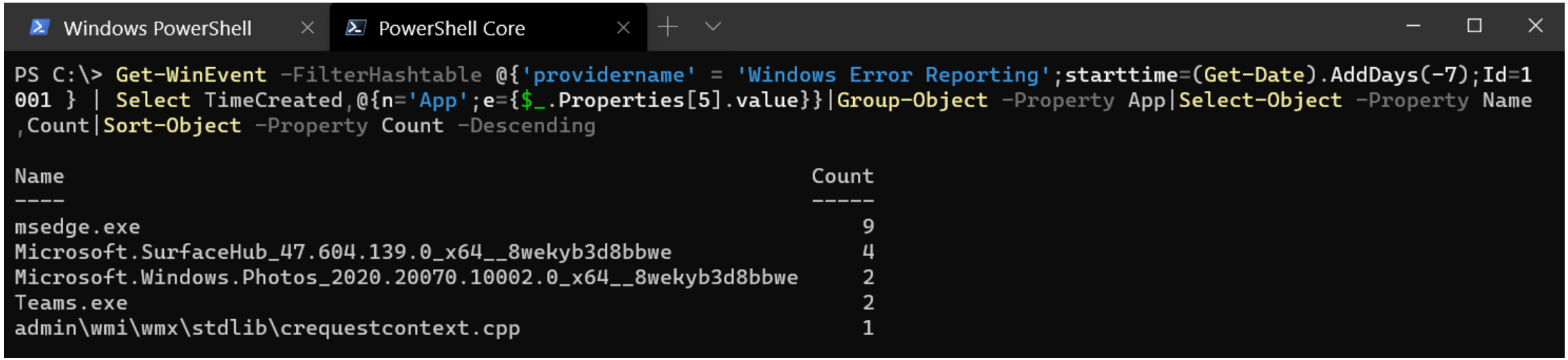
Managing the Microsoft Security stack with PowerShell – Atomic execution framework

Execute the simulation



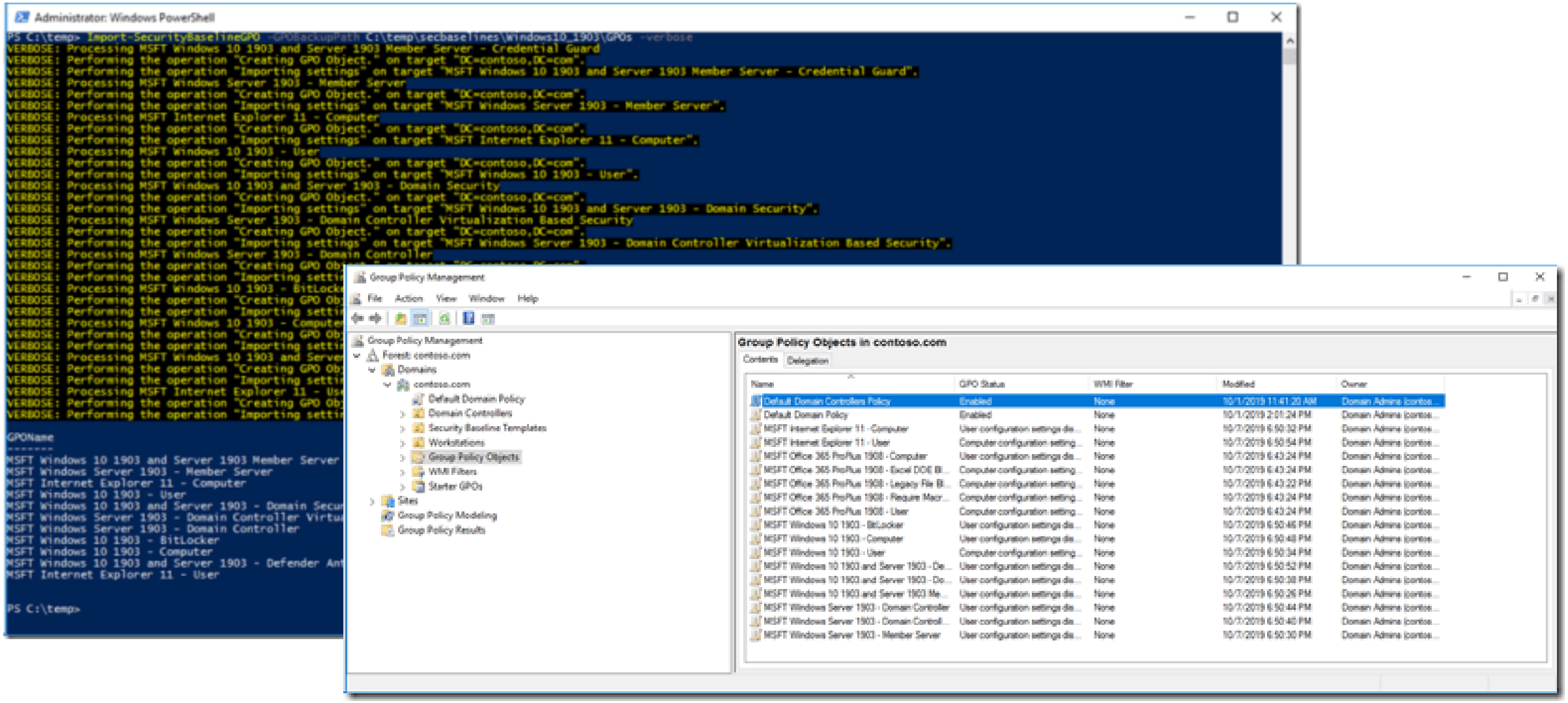
Random snippets I found on the internet or created myself

```
Get-WinEvent -FilterHashtable @{'providername' = 'Windows Error Reporting';starttime=(Get-Date).AddDays(-7);Id=1001 } | Select TimeCreated,@{n='App';e={$_.Properties[5].value}}|Group-Object -Property App|Select-Object -Property Name,Count|Sort-Object -Property Count -Descending
```



Managing the Microsoft Security stack with PowerShell – **Importing Microsoft Security Baselines**

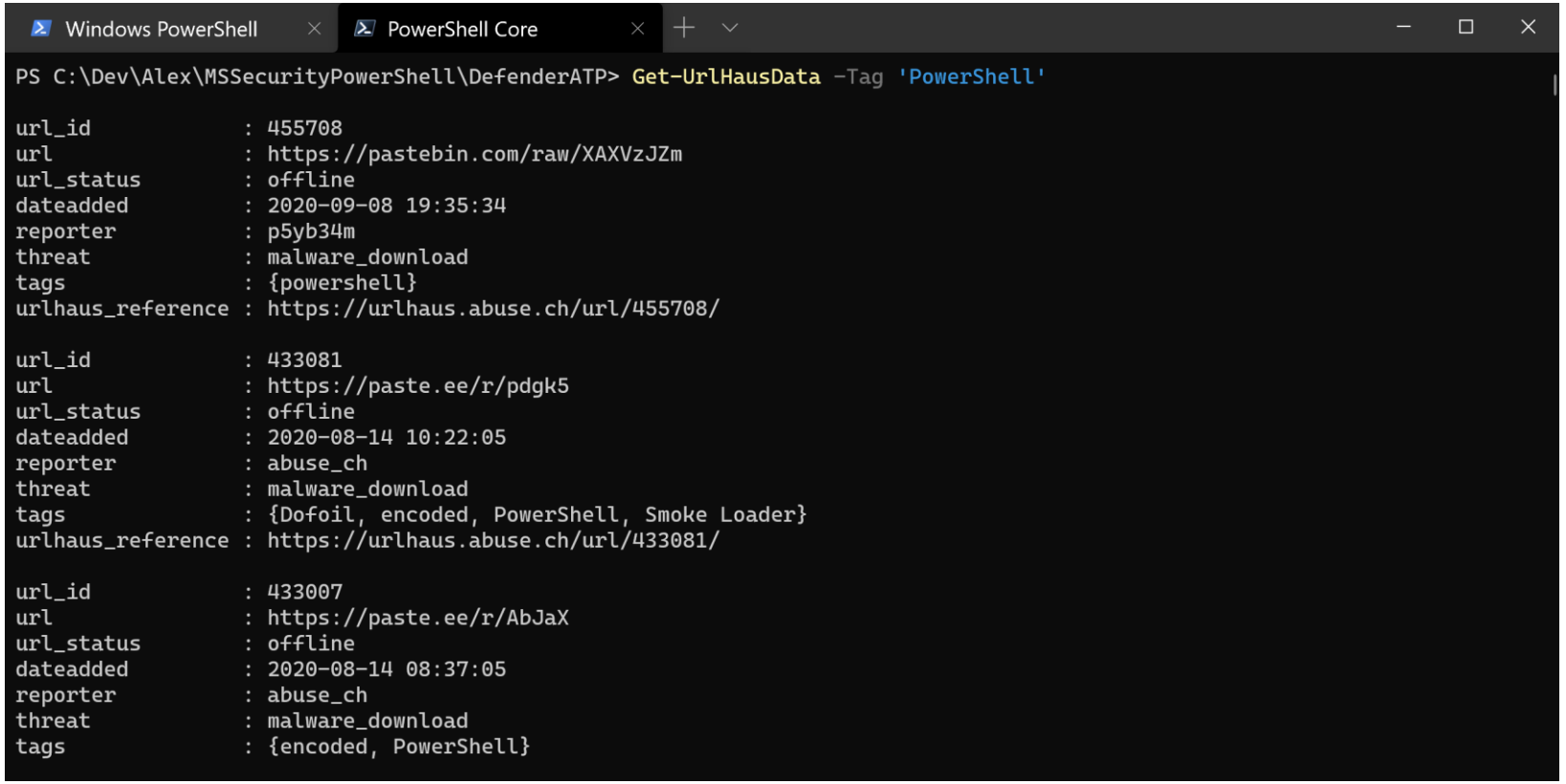
https://www.verboon.info/2019/10/importing-gpo-security-baselines-with-powershell/



Managing the Microsoft Security stack with PowerShell – **PSURLHAUS**

This module provides you with easy-to-use cmdlets to make it easy to interface with the URLhaus API a project operated by abuse.ch with the purpose of collecting, tracking and sharing malware URLs to support security analysts to protect their network and customers from cyber threats. https://github.com/alexverboon/PSURLhaus

Find URLs with PowerShell payload



Managing the Microsoft Security stack with PowerShell – PSURLHAUS

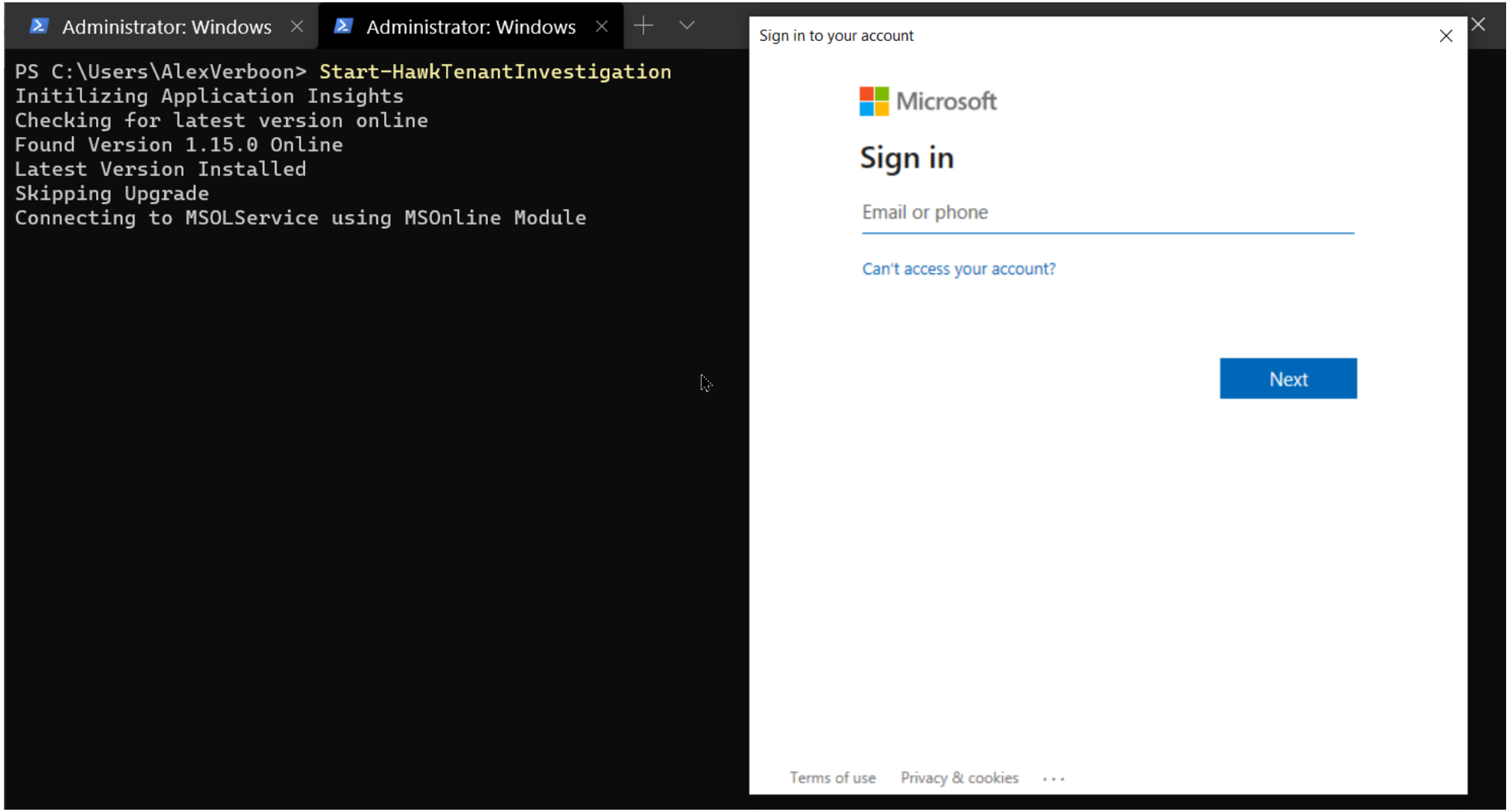
Windows PowerShell | PowerShell Core

```
PS C:\Dev\Alex\MSSecurityPowerShell\DefenderATP> Get-UrlHausData -URL | where url_status -like 'Online'

id                : 456294
urlhaus_reference : https://urlhaus.abuse.ch/url/456294/
url               : http://116.114.95.111:44570/Mozi.m
url_status        : online
host              : 116.114.95.111
date_added        : 2020-09-09 19:19:05 UTC
threat            : malware_download
blacklists        : @{spamhaus_dbl=not listed; surbl=not listed}
reporter          : lrz_security
larted            : true
tags              : {elf, Mozi}

id                : 456292
urlhaus_reference : https://urlhaus.abuse.ch/url/456292/
url               : http://182.117.98.189:47696/Mozi.m
url_status        : online
host              : 182.117.98.189
date_added        : 2020-09-09 19:19:04 UTC
threat            : malware_download
blacklists        : @{spamhaus_dbl=not listed; surbl=not listed}
reporter          : lrz_security
larted            : false
tags              : {elf, Mozi}

id                : 456293
```

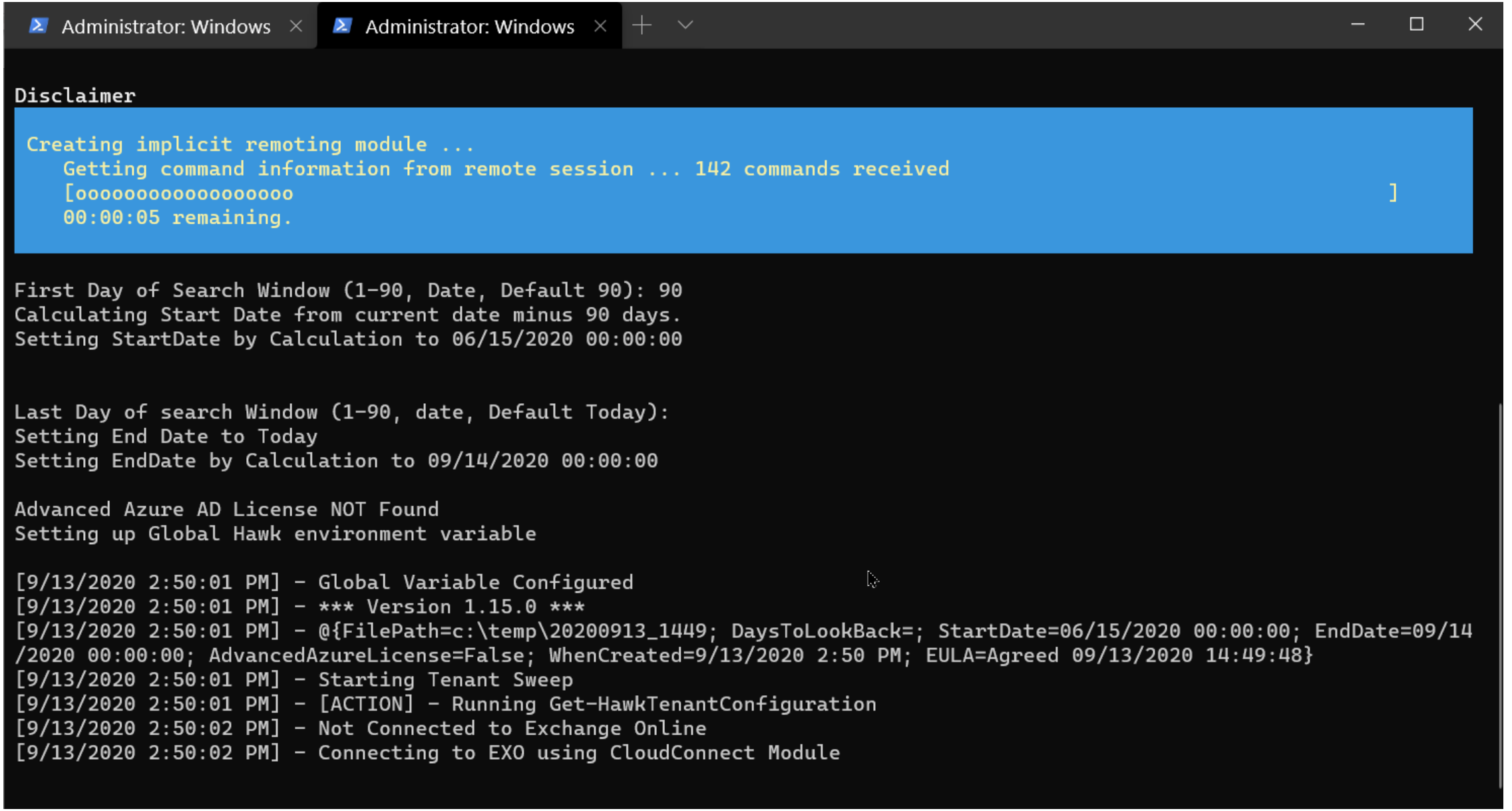
Managing the Microsoft Security stack with PowerShell – HAWK

https://github.com/Canthv0/hawk

Powershell Based tool for gathering information related to O365 intrusions and potential Breaches



Managing the Microsoft Security stack with PowerShell – HAWK



Managing the Microsoft Security stack with PowerShell – HAWK

Administrator: Windows | Administrator: Windows

```
[9/13/2020 2:51:00 PM] - Writing Data to c:\temp\20200913_1449\Tenant\XML\RBAC_Changes.xml
[9/13/2020 2:51:00 PM] - Writing Data to c:\temp\20200913_1449\Tenant\RBAC_Changes.csv
[9/13/2020 2:51:00 PM] - [ACTION] - Running Get-HawkTenantAzureAuditLog
[9/13/2020 2:51:01 PM] - [ACTION] - Searching Unified Audit Logs Azure Activities
[9/13/2020 2:51:01 PM] - Searching for Application Activities
[9/13/2020 2:51:01 PM] - Running Unified Audit Log Search
[9/13/2020 2:51:01 PM] - Search-UnifiedAuditLog -RecordType 'AzureActiveDirectory' -Operations 'Add OAuth2PermissionGran
t.','Consent to application.'  -StartDate '6/15/2020' -EndDate '9/14/2020' -SessionCommand ReturnLargeSet -resultsize 10
00 -sessionid 145101
[9/13/2020 2:51:08 PM] - Retrieved all results.
[9/13/2020 2:51:08 PM] - Retrieved:14    Total: 14
[9/13/2020 2:51:08 PM] - ## INVESTIGATE ## - Application Rights Activity found.
[9/13/2020 2:51:08 PM] - ## INVESTIGATE ## - Please review these Azure_Application_Audit.csv to ensure any changes are l
egitimate.
[9/13/2020 2:51:08 PM] - Appending Data to c:\temp\20200913_1449\Tenant\Azure_Appliction_Audit.csv
```

	A	B	C	D	E	F	G	H	
1	Id	Operation	ResultStatus	Workload	ClientIP	UserId	ActorUPN	targetName	env_time
2	bf006940-951c-4f5f-b510-459bd8564f69	Consent to application.	Success	AzureActiveDirectory	65.52.228.217			Microsoft Graph PowerShell (Preview)	2020-08-16T1
3	2898debb-a7b2-41ce-8150-b8e8327870c8	Consent to application.	Success	AzureActiveDirectory	40.112.91.238			Microsoft Graph PowerShell (Preview)	2020-08-04T1
4	eb26ca77-a20a-47f4-9bb8-3a0d0b2bfcc1	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			PSMDATP1	2020-07-18T1
5	2dff712f-2ff4-4176-b9eb-f9d12000e3ee	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			Azure AD Risk Detection API	2020-07-21T1
6	320246d4-6eaf-4d35-b966-d3f82daf3728	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			Azure AD Risk Detection API	2020-07-21T1
7	15c131b2-ad3e-4129-8ab0-908ec1a47091	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			ServicePrincipalAlex	2020-07-07T1
8	2a5f0114-4de9-47b7-8074-3d5df0b6a2ef	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			PSMDATP1	2020-07-18T0
9	8d15afbc-45f7-4adb-9ee4-4d8a3b167a53	Consent to application.	Success	AzureActiveDirectory	52.138.136.95			WD Antivirus Testground	2020-07-06T0
10	d390a0b7-c62a-45bc-8c3d-56aa69e6246a	Consent to application.	Success	AzureActiveDirectory	40.112.91.238			Windows Defender ATP for Flow	2020-07-18T1
11	a1789b73-9719-4abd-b593-53ac717e812e	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			PSMDATP1	2020-07-18T0
12	9f9aa756-9c11-4b57-88ba-4e23bfd01022	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			PSMDATP1	2020-07-18T0
13	4c9fd4ce-3946-49bc-ad2d-8f7443bc82b5	Consent to application.	Success	AzureActiveDirectory	77.56.162.123			PSMDATP1	2020-07-18T0
14	6cdd372e-5bfa-4dd3-9442-7faac6447797	Consent to application.	Success	AzureActiveDirectory	40.127.164.6			WD Antivirus Testground	2020-06-30T1
15	b5fef836-82e7-42ea-85dc-06e6efadcc6f	Consent to application.	Success	AzureActiveDirectory	65.52.228.217			Azure Notebooks	2020-06-29T2
16									

```
[9/13/2020 2:51:09 PM] - [ACTION] - Running Get-HawkTenantConsentGrants
[9/13/2020 2:51:09 PM] - Gathering Oauth / Application Grants
```