black hat ASIA 2020
OCTOBER 1-2, 2020
BRIEFINGS

What the log?! So many events, so little time...

Miriam Wiesner

@miriamxyra

Miriam Wiesner

Security Program Manager

Microsoft Defender ATP
& Microsoft Threat Protection

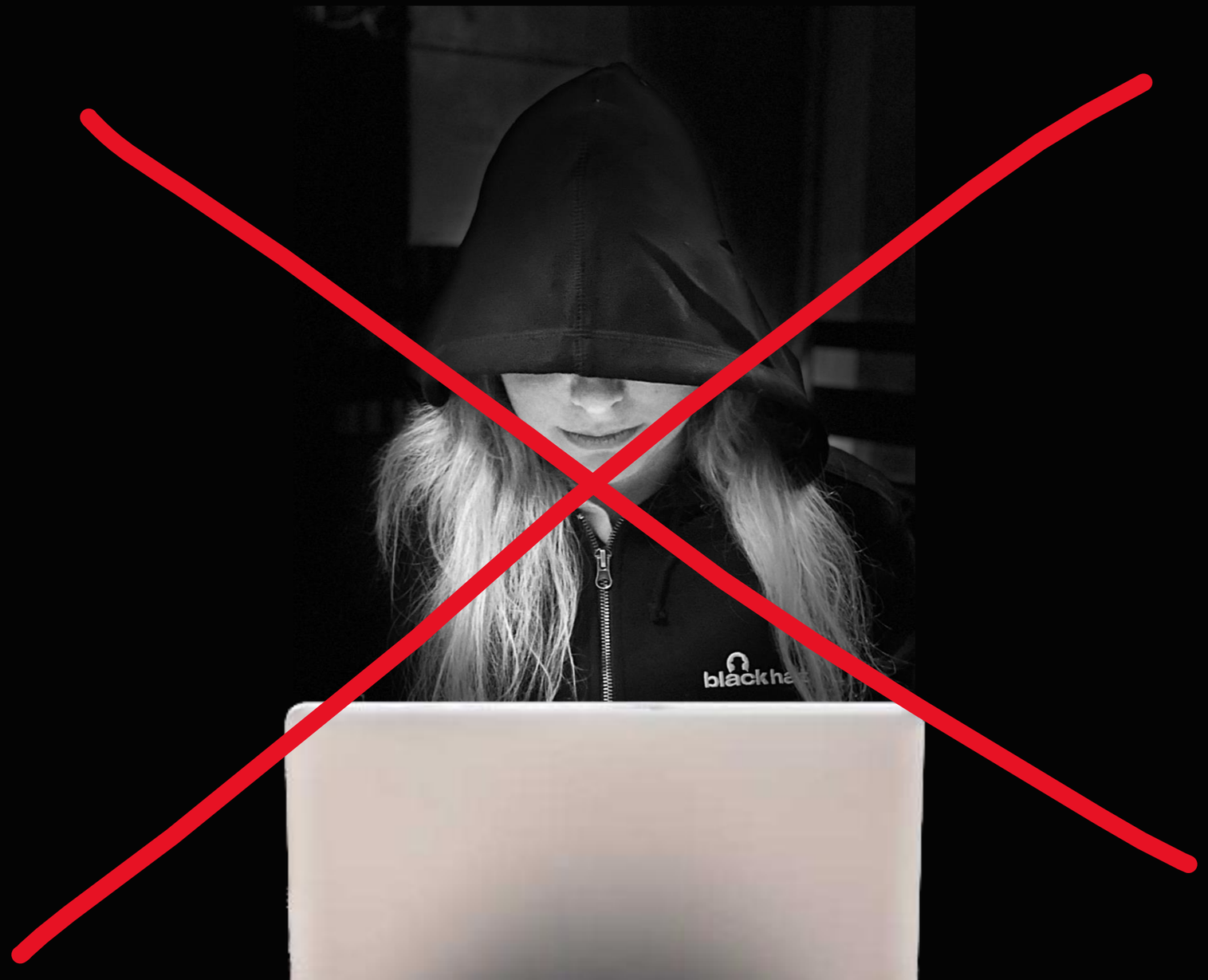
@miriamxyra

EventList:
https://github.com/miriamxyra/EventList

Disclaimer

This presentation and the tool demonstrated during the session is my personal work and not supported by Microsoft.

No Ninjacats or Unicorns were harmed in the process of creating this tool.



Microsoft Security Compliance Toolkit 1.0

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: English

Download

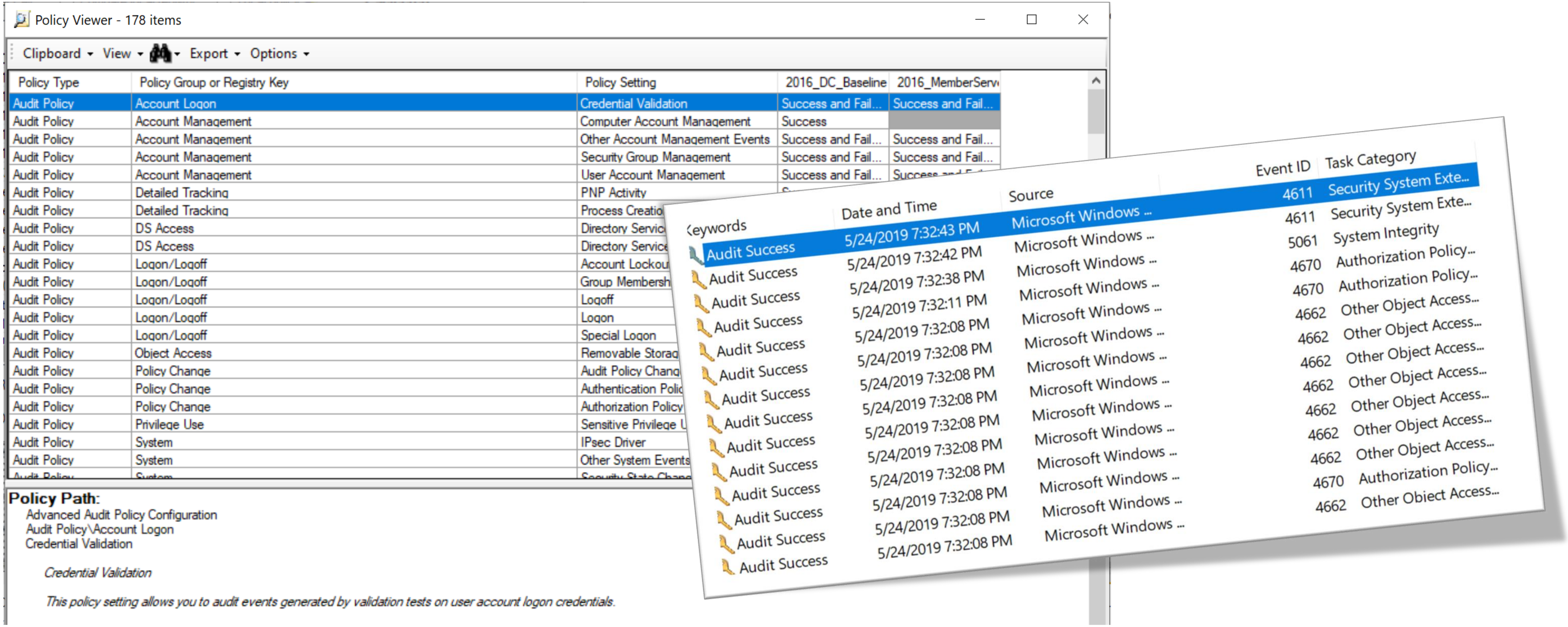
Choose the download you want

File Name	Size
LGPO.zip	797 KB
Office-2016-baseline.zip	4.5 MB
PolicyAnalyzer.zip	1.6 MB
Windows 10 Version 1507 Security Baseline.zip	904 KB
Windows 10 Version 1511 Security Baseline.zip	902 KB
Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB

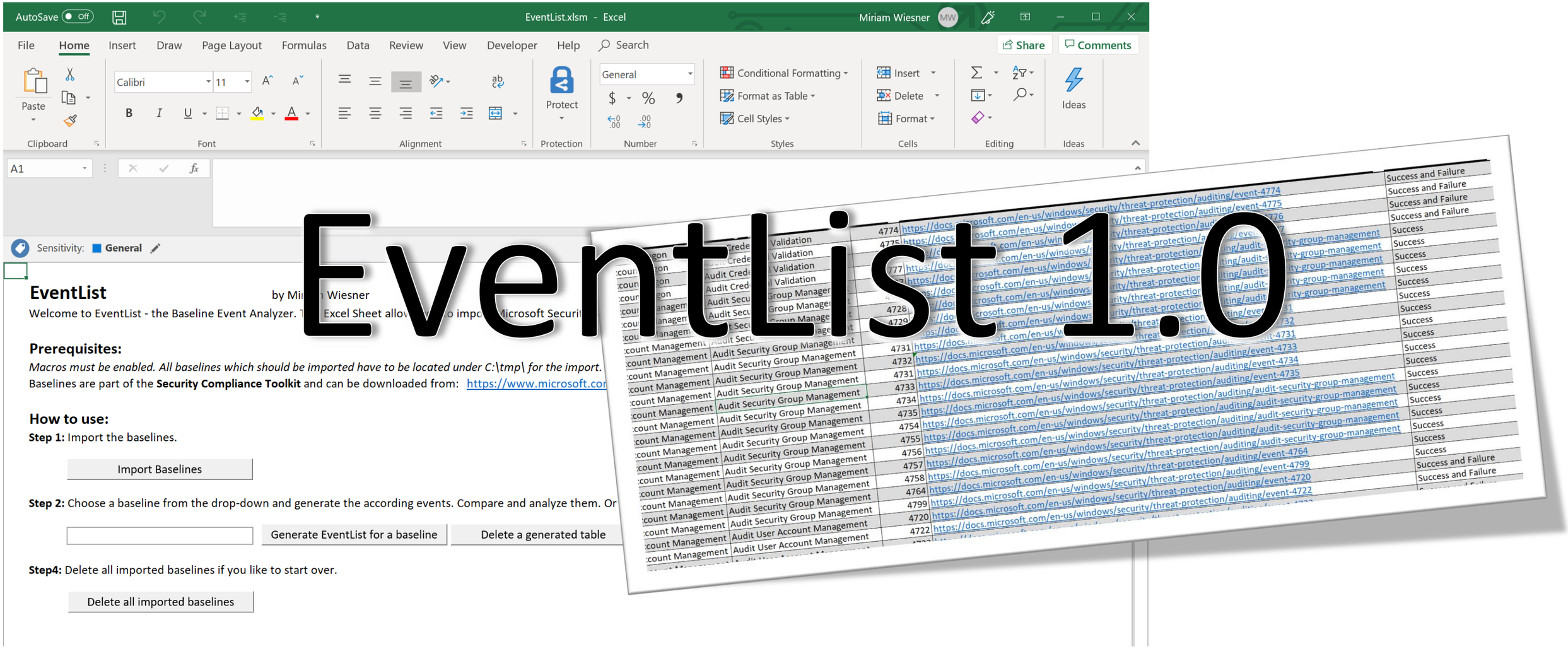
Microsoft Security Compliance Toolkit

https://aka.ms/SCT

black hat ASIA 2020




1994. II
1992 II
2003 II
2002 II
2001 II


AutoSave Off
EventList.xlsm - Excel
Miriam Wiesner
File Home Insert Draw Page Layout Formulas Data Review View Developer Help Search
Share Comments
Paste
Calibri 11
General
Conditional Formatting
Format as Table
Cell Styles
Insert
Delete
Format
Protect
Ideas
Clipboard Font Alignment Protection Number Styles Cells Editing Ideas
A1
Sensitivity: General
EventList
by Mi Wiesner
Welcome to EventList - the Baseline Event Analyzer. T Excel Sheet allo o impo Microsoft Securit
Prerequisites:
Macros must be enabled. All baselines which should be imported have to be located under C:\tmp\ for the import.
Baselines are part of the Security Compliance Toolkit and can be downloaded from: https://www.microsoft.co
How to use:
Step 1: Import the baselines.
Import Baselines
Step 2: Choose a baseline from the drop-down and generate the according events. Compare and analyze them. Or
Generate EventList for a baseline
Delete a generated table
Step4: Delete all imported baselines if you like to start over.
Delete all imported baselines
EventList1.0

MITRE ATT&CK

Impact

Execution

Initial Access

Credential Access

Persistence

Privilege Escalation

Defense Evasion

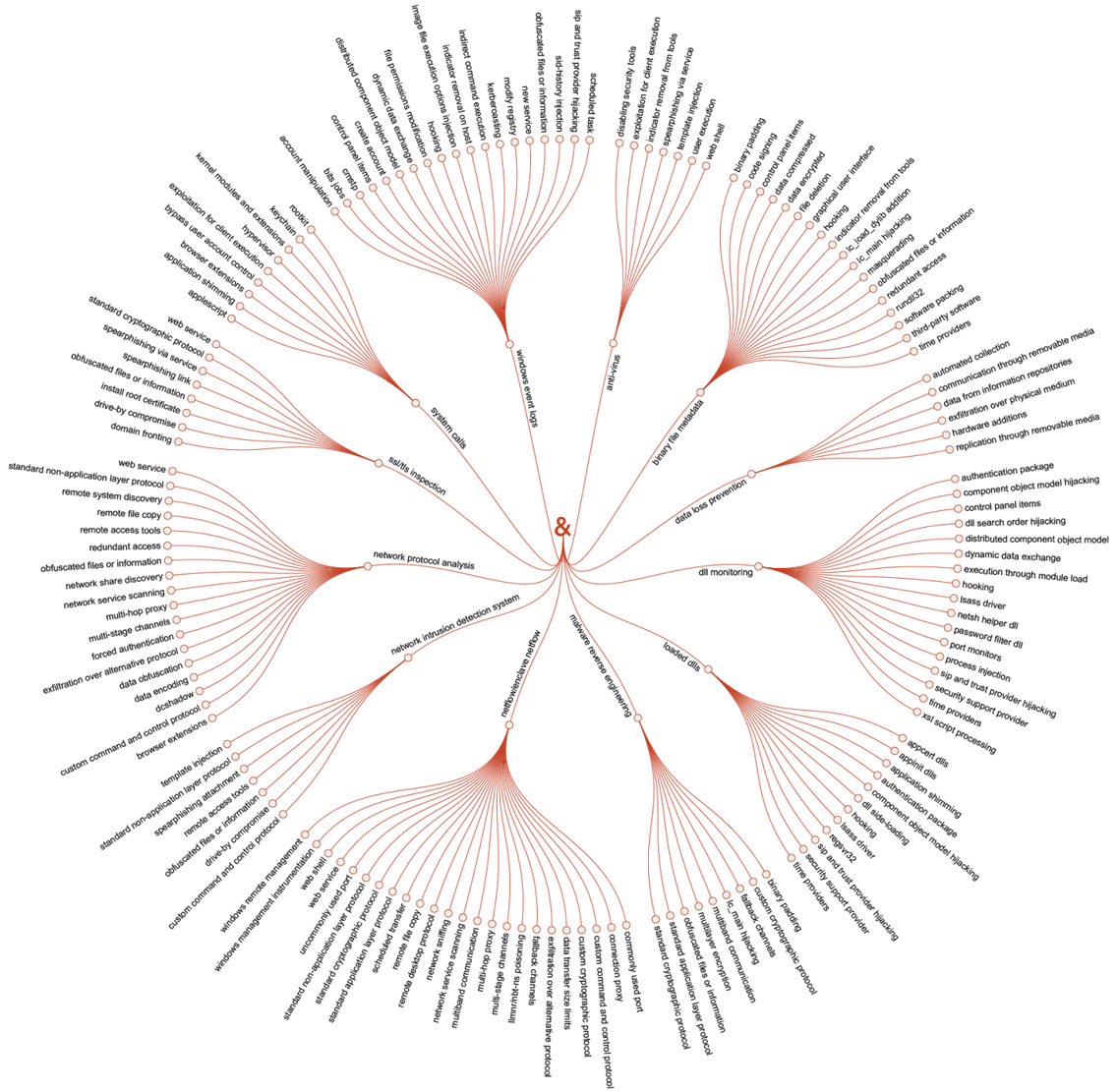
Lateral Movement

Discovery

Exfiltration

Command and Control

Collection



MATRICES

PRE-ATT&CK

Enterprise

All Platforms

Linux

macOS

Windows

Mobile

Home > Matrices > Enterprise

Enterprise Matrix

The full ATT&CK Matrix

Last Modified: 2019-04-25 20:

Initial Access	Execution									Impact
Drive-by Compromise	AppleScript									Data Destruction
Exploit Public-Facing Application	CMSTP									Data Encrypted for Impact
External Remote Services	Command-Line Interface									Defacement
Hardware Additions	Compiled HTML									Disk Content Wipe
Replication Through Removable Media	Control Panel Items									Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange									Endpoint Denial of Service
Spearphishing Link	Execution through API									Firmware Corruption
Spearphishing via Service	Execution through Module Load									Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution									Network Denial of Service
Trusted Relationship	Graphical User Interface									Resource Hijacking
Valid Accounts	InstallUtil		Weakness	Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy	Service Stop

Home > Techniques > Enterprise > Pass the Hash

Pass the Hash

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes. [1]

ID: T1075
Tactic: Lateral Movement
Platform: Windows
System Requirements: Requires Microsoft Windows as target system
Data Sources: Authentication logs
Contributors: Travis Smith, Tripwire
Version: 1.0

Examples

Name	Description
APT1	The APT1 group is known to have used pass the hash.[2]
APT28	APT28 has used pass the hash for lateral movement.[3]
APT32	APT32 has used pass the hash for lateral movement.[4]
Cobalt Strike	Cobalt Strike can perform pass the hash.[5]
Empire	Empire can perform pass the hash attacks.[6]
HOPLIGHT	HOPLIGHT has been observed loading several APIs associated with Pass the Hash. [7]
Mimikatz	Mimikatz's [illegible] module can impersonate a user, with only a password hash, to execute arbitrary commands.[8][9]

MITRE ATT&CK

Impact

Execution

Initial Access

Credential Access

Persistence

Privilege Escalation

Defense Evasion

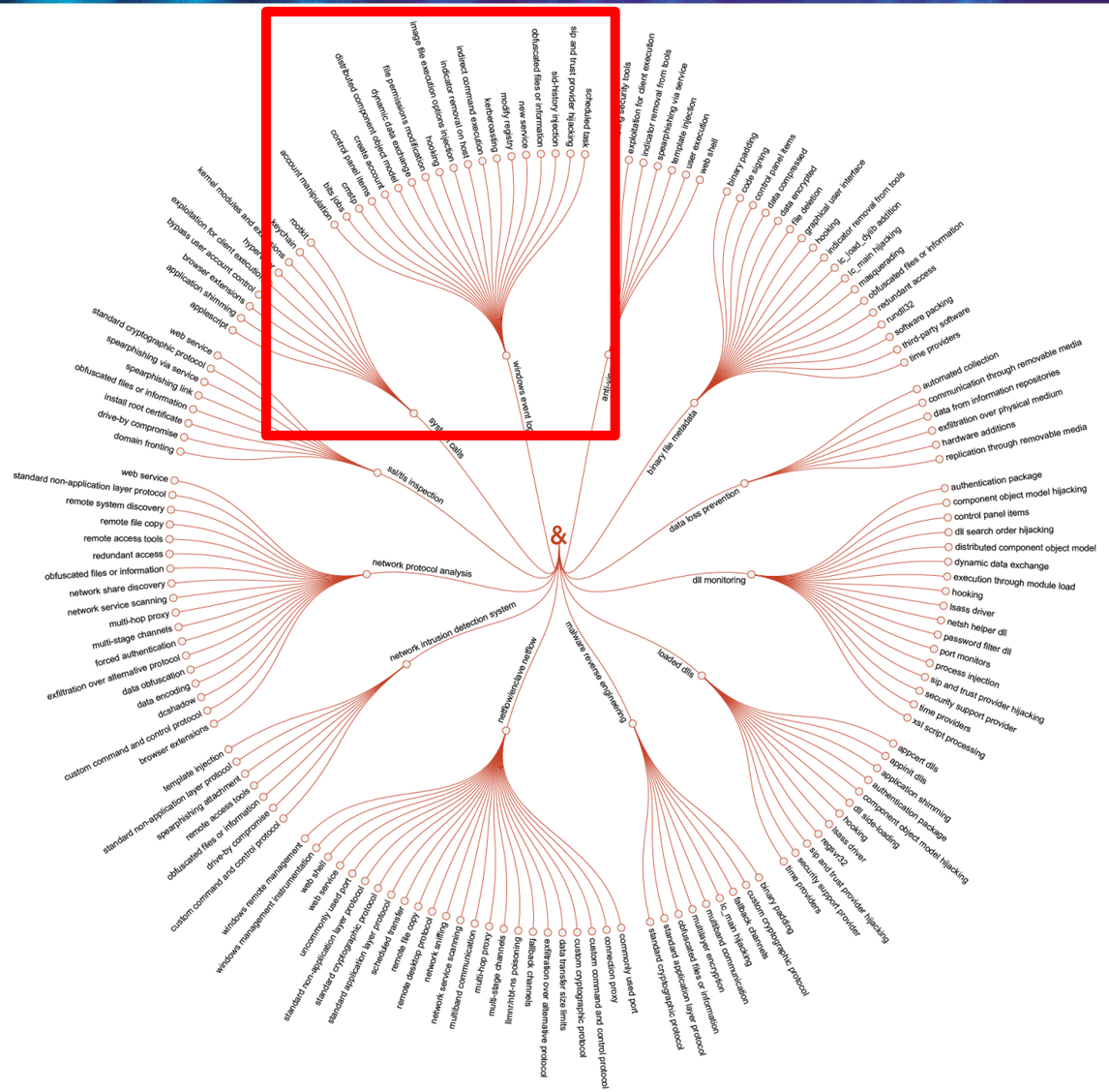
Lateral Movement

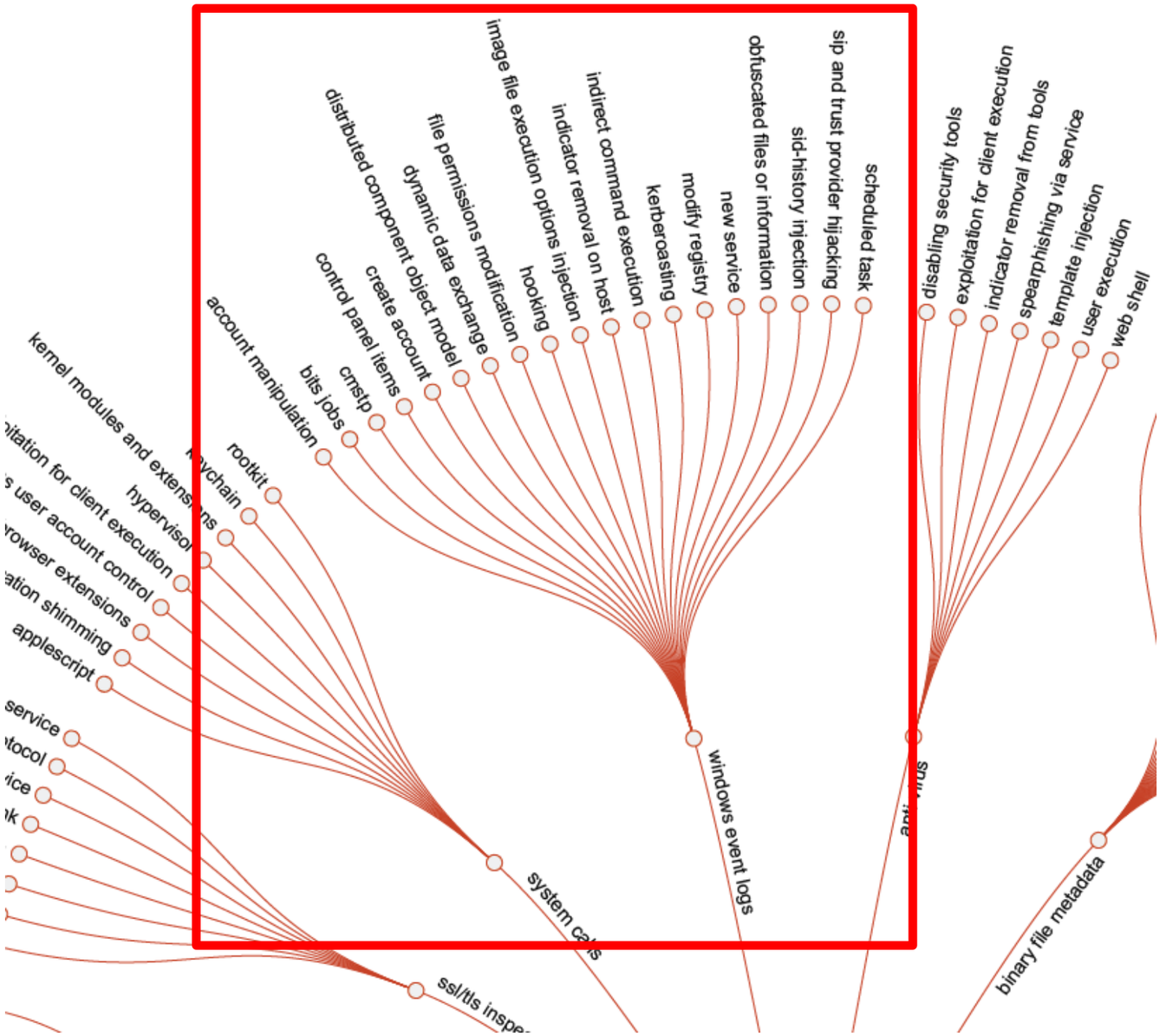
Discovery

Exfiltration

Command and Control

Collection

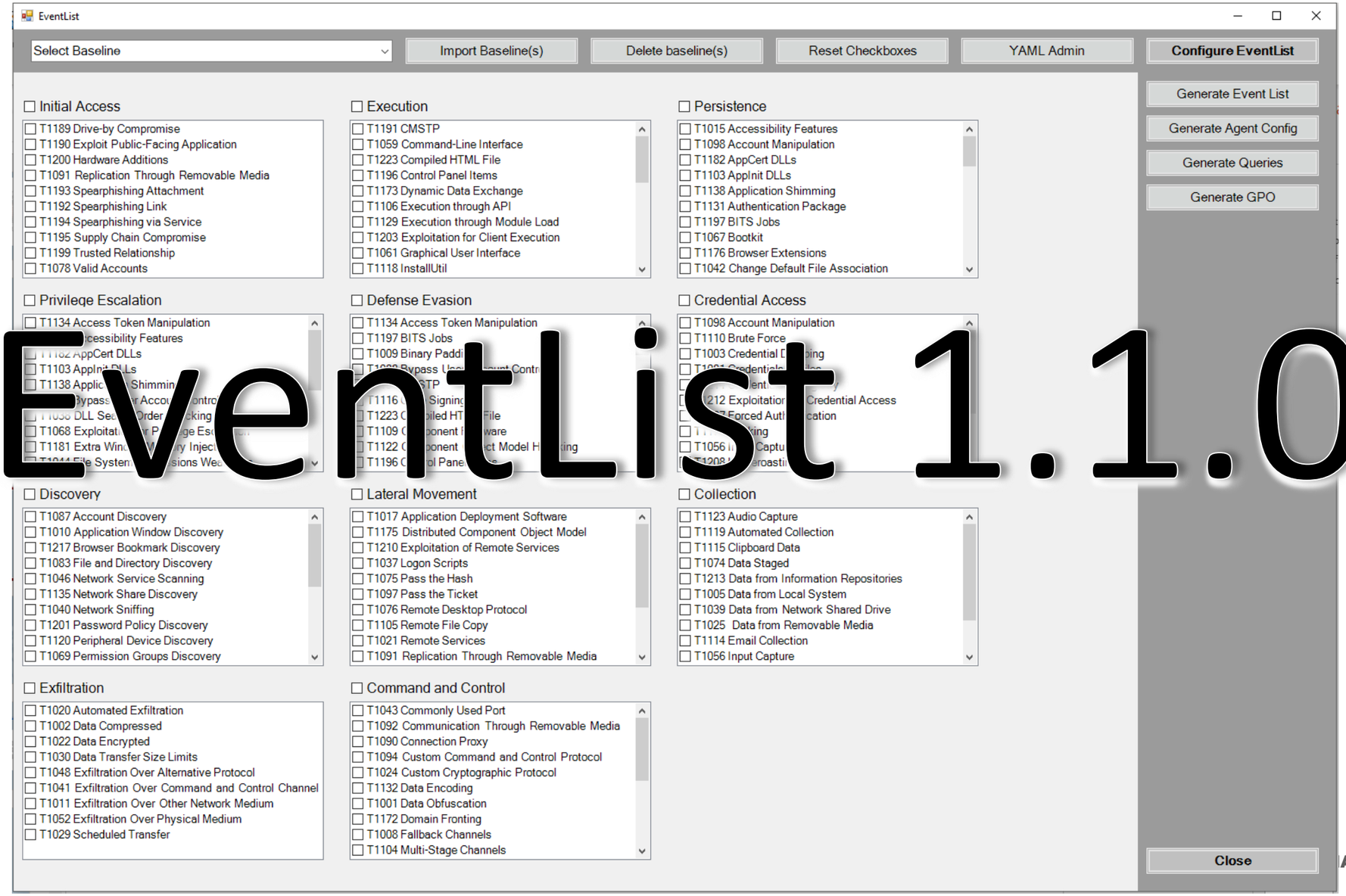



scheduled task
sip and trust provider hijacking
sid-history injection
obfuscated files or information
new service
modify registry
kerberoasting
indirect command execution
indicator removal on host
image file execution options injection
hooking
file permissions modification
dynamic data exchange
distributed component object model
create account
control panel items
cmstp
bits jobs
account manipulation
rootkit
windows event logs
system calls
disabling security tools
exploitation for client execution
indicator removal from tools
spearphishing via service
template injection
user execution
web shell
binary file metadata

Hunting queries?

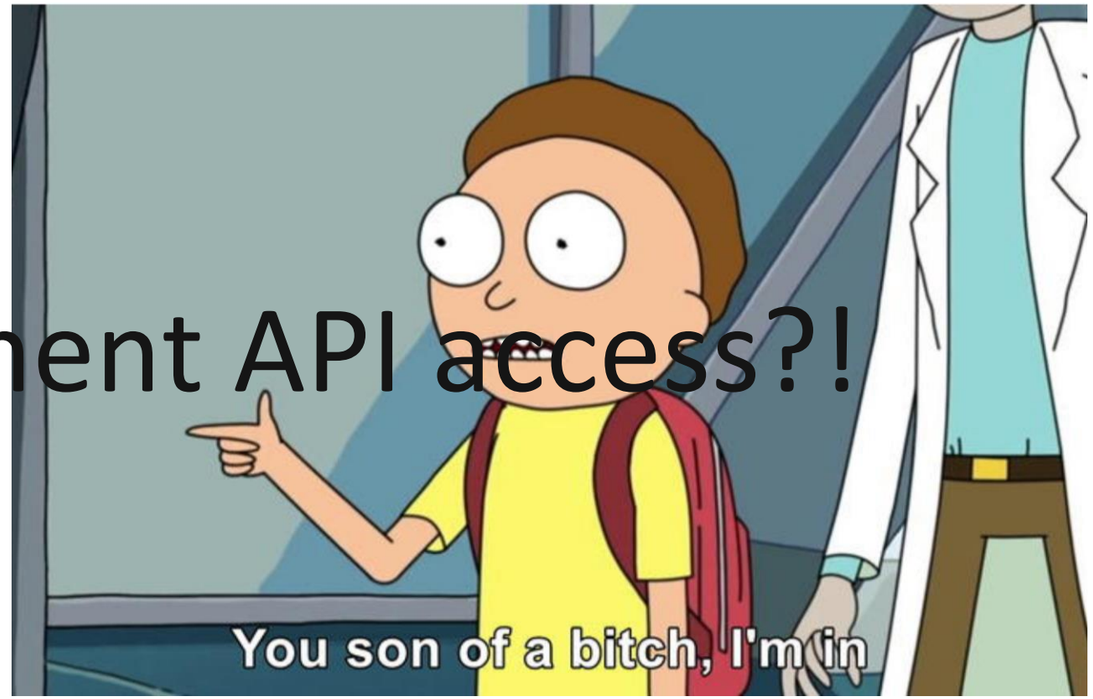
Which events should be forwarded?

Which events will be generated?

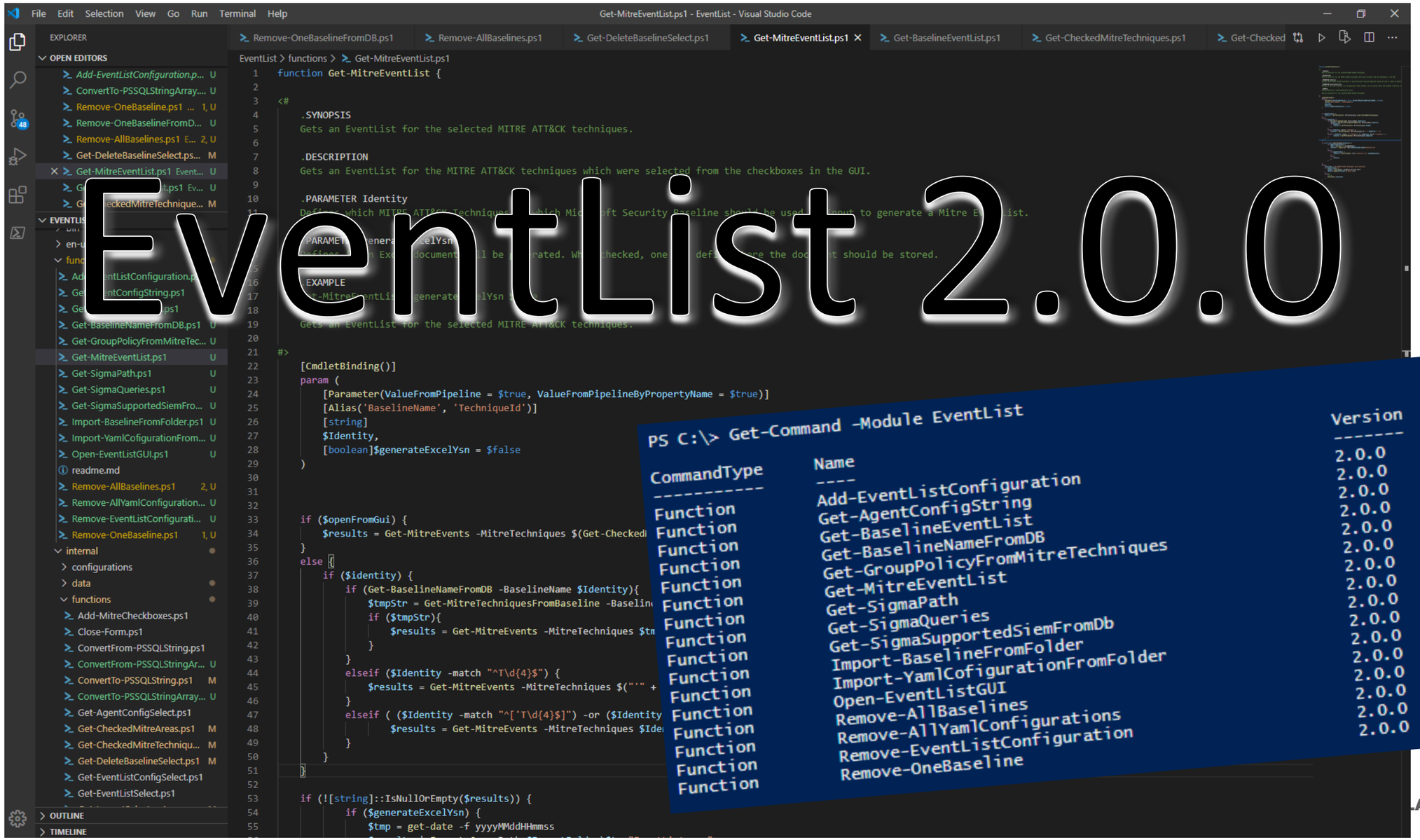


EventList 1.1.0

Can you plz implement API access?!



EventList 2.0.0

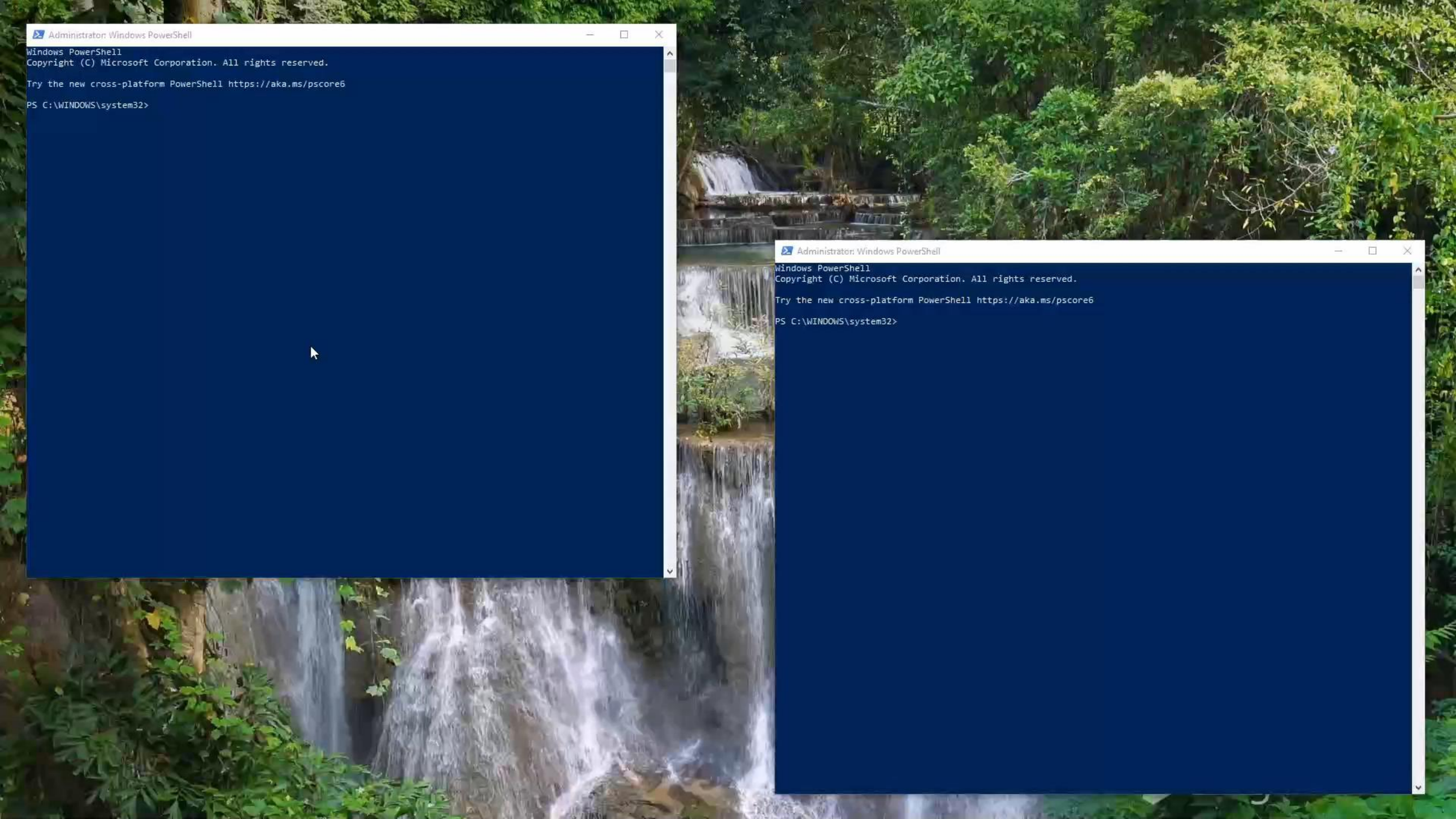


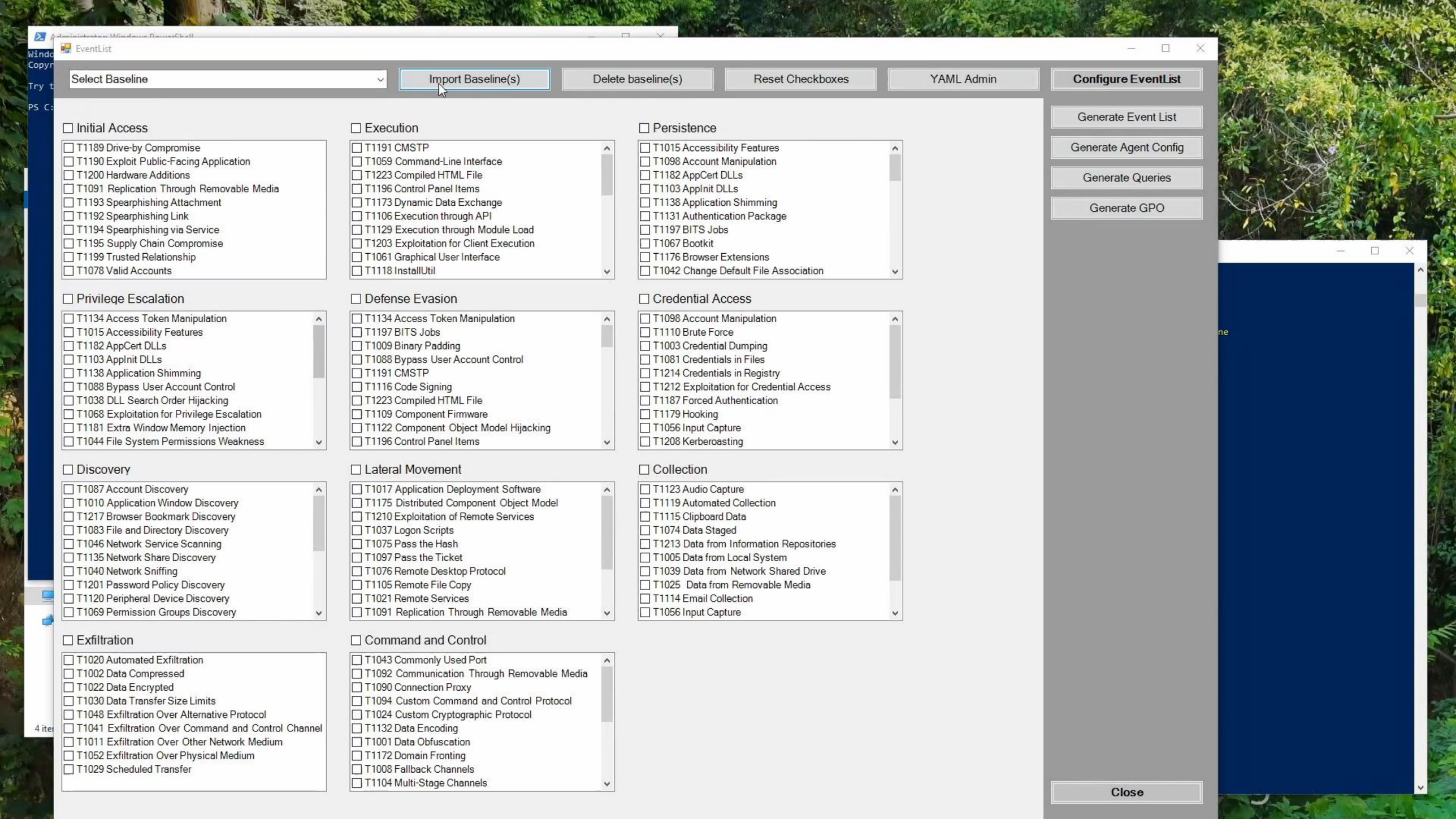

```
PS C:\> Get-Command -Module EventList

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Add-EventListConfiguration                         2.0.0      EventList
Function        Get-AgentConfigString                              2.0.0      EventList
Function        Get-BaselineEventList                              2.0.0      EventList
Function        Get-BaselineNameFromDB                             2.0.0      EventList
Function        Get-GroupPolicyFromMitreTechniques                 2.0.0      EventList
Function        Get-MitreEventList                                 2.0.0      EventList
Function        Get-SigmaPath                                      2.0.0      EventList
Function        Get-SigmaQueries                                   2.0.0      EventList
Function        Get-SigmaSupportedSiemFromDb                       2.0.0      EventList
Function        Import-BaselineFromFolder                          2.0.0      EventList
Function        Import-YamlCofigurationFromFolder                  2.0.0      EventList
Function        Open-EventListGUI                                  2.0.0      EventList
Function        Remove-AllBaselines                                2.0.0      EventList
Function        Remove-AllYamlConfigurations                       2.0.0      EventList
Function        Remove-EventListConfiguration                      2.0.0      EventList
Function        Remove-OneBaseline                                 2.0.0      EventList
```

DEMO

EventList

https://github.com/miriamxyra/EventList

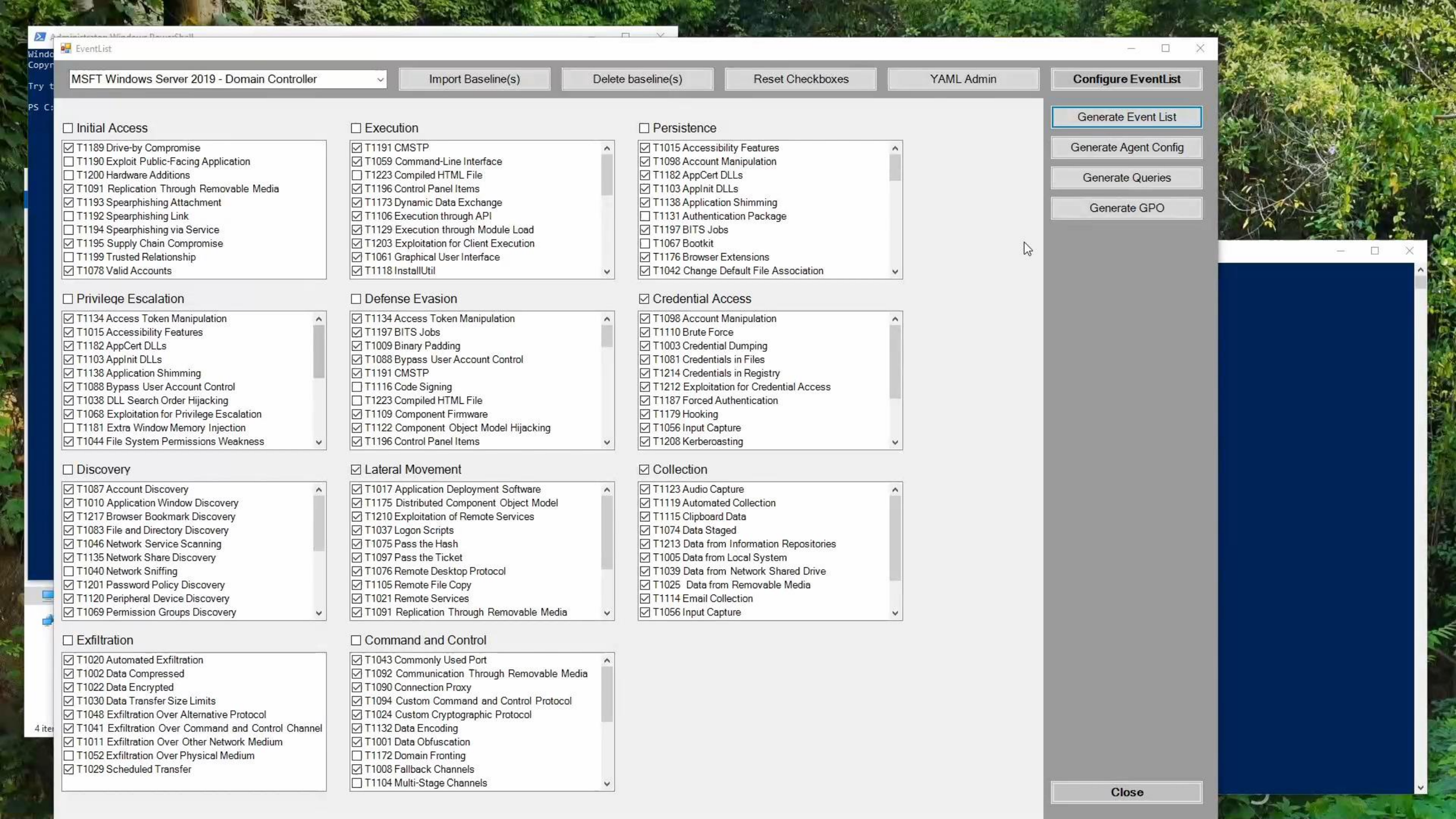

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32>
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32>


EventList
Select Baseline
Import Baseline(s)
Delete baseline(s)
Reset Checkboxes
YAML Admin
Configure EventList
Generate Event List
Generate Agent Config
Generate Queries
Generate GPO
Close
Initial Access
T1189 Drive-by Compromise
T1190 Exploit Public-Facing Application
T1200 Hardware Additions
T1091 Replication Through Removable Media
T1193 Spearphishing Attachment
T1192 Spearphishing Link
T1194 Spearphishing via Service
T1195 Supply Chain Compromise
T1199 Trusted Relationship
T1078 Valid Accounts
Execution
T1191 CMSTP
T1059 Command-Line Interface
T1223 Compiled HTML File
T1196 Control Panel Items
T1173 Dynamic Data Exchange
T1106 Execution through API
T1129 Execution through Module Load
T1203 Exploitation for Client Execution
T1061 Graphical User Interface
T1118 InstallUtil
Persistence
T1015 Accessibility Features
T1098 Account Manipulation
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1131 Authentication Package
T1197 BITS Jobs
T1067 Bootkit
T1176 Browser Extensions
T1042 Change Default File Association
Privilege Escalation
T1134 Access Token Manipulation
T1015 Accessibility Features
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1088 Bypass User Account Control
T1038 DLL Search Order Hijacking
T1068 Exploitation for Privilege Escalation
T1181 Extra Window Memory Injection
T1044 File System Permissions Weakness
Defense Evasion
T1134 Access Token Manipulation
T1197 BITS Jobs
T1009 Binary Padding
T1088 Bypass User Account Control
T1191 CMSTP
T1116 Code Signing
T1223 Compiled HTML File
T1109 Component Firmware
T1122 Component Object Model Hijacking
T1196 Control Panel Items
Credential Access
T1098 Account Manipulation
T1110 Brute Force
T1003 Credential Dumping
T1081 Credentials in Files
T1214 Credentials in Registry
T1212 Exploitation for Credential Access
T1187 Forced Authentication
T1179 Hooking
T1056 Input Capture
T1208 Kerberoasting
Discovery
T1087 Account Discovery
T1010 Application Window Discovery
T1217 Browser Bookmark Discovery
T1083 File and Directory Discovery
T1046 Network Service Scanning
T1135 Network Share Discovery
T1040 Network Sniffing
T1201 Password Policy Discovery
T1120 Peripheral Device Discovery
T1069 Permission Groups Discovery
Lateral Movement
T1017 Application Deployment Software
T1175 Distributed Component Object Model
T1210 Exploitation of Remote Services
T1037 Logon Scripts
T1075 Pass the Hash
T1097 Pass the Ticket
T1076 Remote Desktop Protocol
T1105 Remote File Copy
T1021 Remote Services
T1091 Replication Through Removable Media
Collection
T1123 Audio Capture
T1119 Automated Collection
T1115 Clipboard Data
T1074 Data Staged
T1213 Data from Information Repositories
T1005 Data from Local System
T1039 Data from Network Shared Drive
T1025 Data from Removable Media
T1114 Email Collection
T1056 Input Capture
Exfiltration
T1020 Automated Exfiltration
T1002 Data Compressed
T1022 Data Encrypted
T1030 Data Transfer Size Limits
T1048 Exfiltration Over Alternative Protocol
T1041 Exfiltration Over Command and Control Channel
T1011 Exfiltration Over Other Network Medium
T1052 Exfiltration Over Physical Medium
T1029 Scheduled Transfer
Command and Control
T1043 Commonly Used Port
T1092 Communication Through Removable Media
T1090 Connection Proxy
T1094 Custom Command and Control Protocol
T1024 Custom Cryptographic Protocol
T1132 Data Encoding
T1001 Data Obfuscation
T1172 Domain Fronting
T1008 Fallback Channels
T1104 Multi-Stage Channels

Hunting queries?

Which events should be forwarded?

Which events will be generated?


EventList
MSFT Windows Server 2019 - Domain Controller
Import Baseline(s)
Delete baseline(s)
Reset Checkboxes
YAML Admin
Configure EventList
Initial Access
T1189 Drive-by Compromise
T1190 Exploit Public-Facing Application
T1200 Hardware Additions
T1091 Replication Through Removable Media
T1193 Spearphishing Attachment
T1192 Spearphishing Link
T1194 Spearphishing via Service
T1195 Supply Chain Compromise
T1199 Trusted Relationship
T1078 Valid Accounts
Execution
T1191 CMSTP
T1059 Command-Line Interface
T1223 Compiled HTML File
T1196 Control Panel Items
T1173 Dynamic Data Exchange
T1106 Execution through API
T1129 Execution through Module Load
T1203 Exploitation for Client Execution
T1061 Graphical User Interface
T1118 InstallUtil
Persistence
T1015 Accessibility Features
T1098 Account Manipulation
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1131 Authentication Package
T1197 BITS Jobs
T1067 Bootkit
T1176 Browser Extensions
T1042 Change Default File Association
Privilege Escalation
T1134 Access Token Manipulation
T1015 Accessibility Features
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1088 Bypass User Account Control
T1038 DLL Search Order Hijacking
T1068 Exploitation for Privilege Escalation
T1181 Extra Window Memory Injection
T1044 File System Permissions Weakness
Defense Evasion
T1134 Access Token Manipulation
T1197 BITS Jobs
T1009 Binary Padding
T1088 Bypass User Account Control
T1191 CMSTP
T1116 Code Signing
T1223 Compiled HTML File
T1109 Component Firmware
T1122 Component Object Model Hijacking
T1196 Control Panel Items
Credential Access
T1098 Account Manipulation
T1110 Brute Force
T1003 Credential Dumping
T1081 Credentials in Files
T1214 Credentials in Registry
T1212 Exploitation for Credential Access
T1187 Forced Authentication
T1179 Hooking
T1056 Input Capture
T1208 Kerberoasting
Discovery
T1087 Account Discovery
T1010 Application Window Discovery
T1217 Browser Bookmark Discovery
T1083 File and Directory Discovery
T1046 Network Service Scanning
T1135 Network Share Discovery
T1040 Network Sniffing
T1201 Password Policy Discovery
T1120 Peripheral Device Discovery
T1069 Permission Groups Discovery
Lateral Movement
T1017 Application Deployment Software
T1175 Distributed Component Object Model
T1210 Exploitation of Remote Services
T1037 Logon Scripts
T1075 Pass the Hash
T1097 Pass the Ticket
T1076 Remote Desktop Protocol
T1105 Remote File Copy
T1021 Remote Services
T1091 Replication Through Removable Media
Collection
T1123 Audio Capture
T1119 Automated Collection
T1115 Clipboard Data
T1074 Data Staged
T1213 Data from Information Repositories
T1005 Data from Local System
T1039 Data from Network Shared Drive
T1025 Data from Removable Media
T1114 Email Collection
T1056 Input Capture
Exfiltration
T1020 Automated Exfiltration
T1002 Data Compressed
T1022 Data Encrypted
T1030 Data Transfer Size Limits
T1048 Exfiltration Over Alternative Protocol
T1041 Exfiltration Over Command and Control Channel
T1011 Exfiltration Over Other Network Medium
T1052 Exfiltration Over Physical Medium
T1029 Scheduled Transfer
Command and Control
T1043 Commonly Used Port
T1092 Communication Through Removable Media
T1090 Connection Proxy
T1094 Custom Command and Control Protocol
T1024 Custom Cryptographic Protocol
T1132 Data Encoding
T1001 Data Obfuscation
T1172 Domain Fronting
T1008 Fallback Channels
T1104 Multi-Stage Channels
Generate Event List
Generate Agent Config
Generate Queries
Generate GPO
Close

Hunting queries?

Which events should be forwarded?

Which events will be generated?

SIGMA

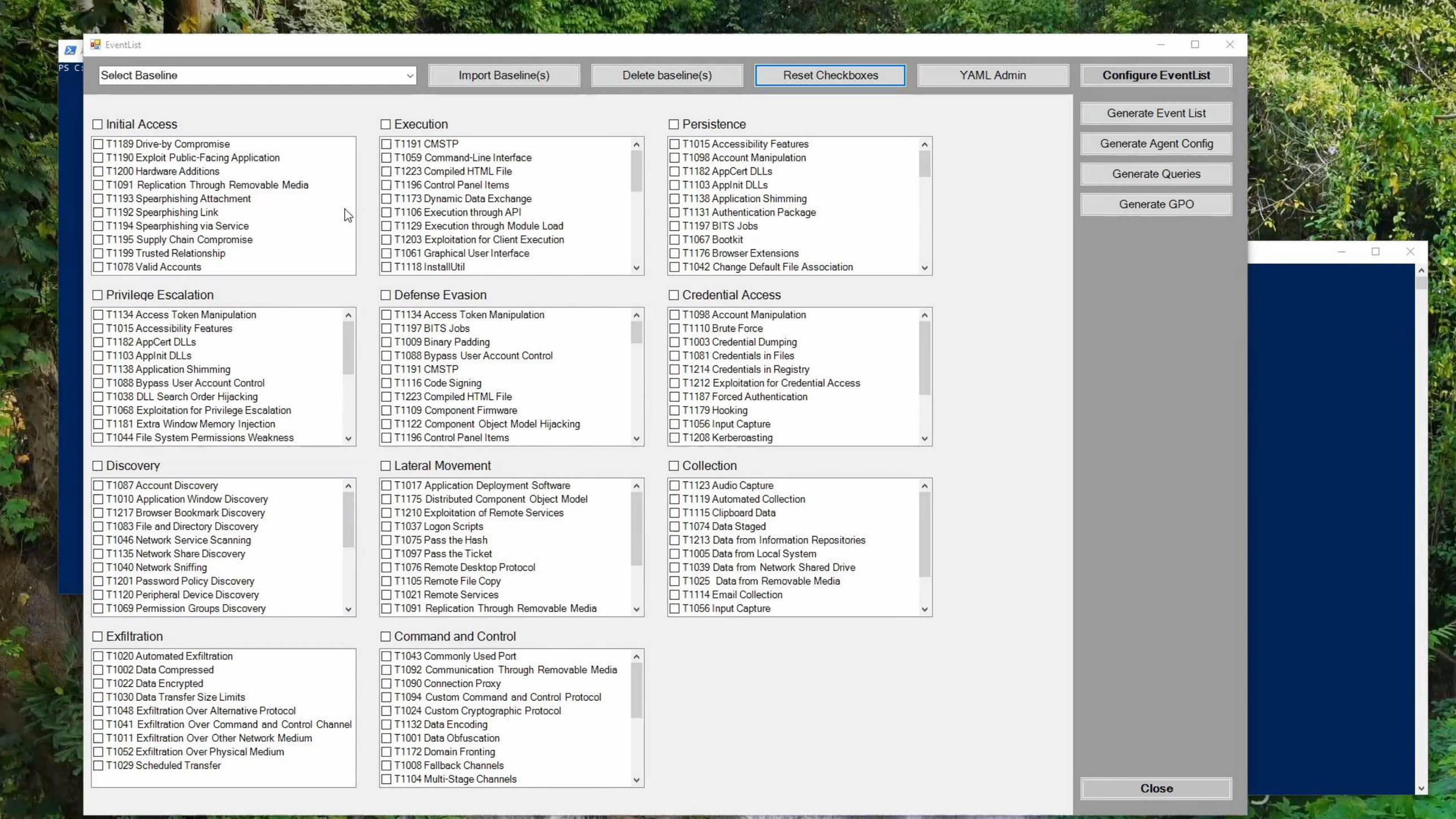
https://github.com/Neo23x0/sigma

Supported Targets

- Splunk (plainqueries and dashboards)
- ElasticSearch Query Strings
- ElasticSearch Query DSL
- Kibana
- Elastic X-Pack Watcher
- Logpoint
- Windows Defender Advanced Threat Protection (WDATP)
- Azure Sentinel / Azure Log Analytics
- ArcSight
- QRadar
- Qualys
- RSA NetWitness
- PowerShell
- Grep with Perl-compatible regular expression support

Current work-in-progress

- Splunk Data Models

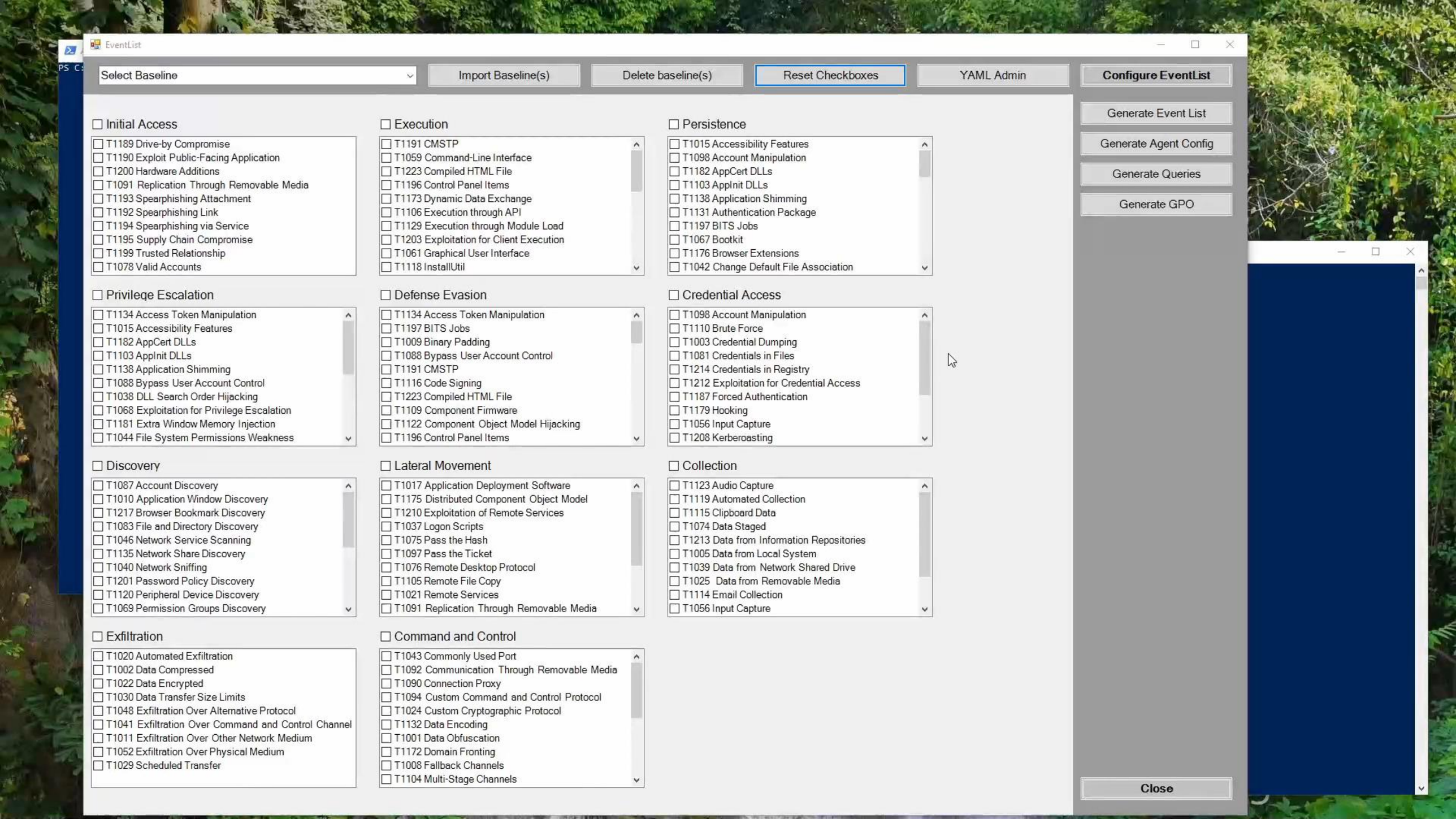

EventList
Select Baseline
Import Baseline(s)
Delete baseline(s)
Reset Checkboxes
YAML Admin
Configure EventList
Generate Event List
Generate Agent Config
Generate Queries
Generate GPO
Close
Initial Access
T1189 Drive-by Compromise
T1190 Exploit Public-Facing Application
T1200 Hardware Additions
T1091 Replication Through Removable Media
T1193 Spearphishing Attachment
T1192 Spearphishing Link
T1194 Spearphishing via Service
T1195 Supply Chain Compromise
T1199 Trusted Relationship
T1078 Valid Accounts
Execution
T1191 CMSTP
T1059 Command-Line Interface
T1223 Compiled HTML File
T1196 Control Panel Items
T1173 Dynamic Data Exchange
T1106 Execution through API
T1129 Execution through Module Load
T1203 Exploitation for Client Execution
T1061 Graphical User Interface
T1118 InstallUtil
Persistence
T1015 Accessibility Features
T1098 Account Manipulation
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1131 Authentication Package
T1197 BITS Jobs
T1067 Bootkit
T1176 Browser Extensions
T1042 Change Default File Association
Privilege Escalation
T1134 Access Token Manipulation
T1015 Accessibility Features
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1088 Bypass User Account Control
T1038 DLL Search Order Hijacking
T1068 Exploitation for Privilege Escalation
T1181 Extra Window Memory Injection
T1044 File System Permissions Weakness
Defense Evasion
T1134 Access Token Manipulation
T1197 BITS Jobs
T1009 Binary Padding
T1088 Bypass User Account Control
T1191 CMSTP
T1116 Code Signing
T1223 Compiled HTML File
T1109 Component Firmware
T1122 Component Object Model Hijacking
T1196 Control Panel Items
Credential Access
T1098 Account Manipulation
T1110 Brute Force
T1003 Credential Dumping
T1081 Credentials in Files
T1214 Credentials in Registry
T1212 Exploitation for Credential Access
T1187 Forced Authentication
T1179 Hooking
T1056 Input Capture
T1208 Kerberoasting
Discovery
T1087 Account Discovery
T1010 Application Window Discovery
T1217 Browser Bookmark Discovery
T1083 File and Directory Discovery
T1046 Network Service Scanning
T1135 Network Share Discovery
T1040 Network Sniffing
T1201 Password Policy Discovery
T1120 Peripheral Device Discovery
T1069 Permission Groups Discovery
Lateral Movement
T1017 Application Deployment Software
T1175 Distributed Component Object Model
T1210 Exploitation of Remote Services
T1037 Logon Scripts
T1075 Pass the Hash
T1097 Pass the Ticket
T1076 Remote Desktop Protocol
T1105 Remote File Copy
T1021 Remote Services
T1091 Replication Through Removable Media
Collection
T1123 Audio Capture
T1119 Automated Collection
T1115 Clipboard Data
T1074 Data Staged
T1213 Data from Information Repositories
T1005 Data from Local System
T1039 Data from Network Shared Drive
T1025 Data from Removable Media
T1114 Email Collection
T1056 Input Capture
Exfiltration
T1020 Automated Exfiltration
T1002 Data Compressed
T1022 Data Encrypted
T1030 Data Transfer Size Limits
T1048 Exfiltration Over Alternative Protocol
T1041 Exfiltration Over Command and Control Channel
T1011 Exfiltration Over Other Network Medium
T1052 Exfiltration Over Physical Medium
T1029 Scheduled Transfer
Command and Control
T1043 Commonly Used Port
T1092 Communication Through Removable Media
T1090 Connection Proxy
T1094 Custom Command and Control Protocol
T1024 Custom Cryptographic Protocol
T1132 Data Encoding
T1001 Data Obfuscation
T1172 Domain Fronting
T1008 Fallback Channels
T1104 Multi-Stage Channels

Hunting queries?

Which events should be forwarded?

Which events will be generated?


Additional
goodies


EventList
Select Baseline
Import Baseline(s)
Delete baseline(s)
Reset Checkboxes
YAML Admin
Configure EventList
Initial Access
T1189 Drive-by Compromise
T1190 Exploit Public-Facing Application
T1200 Hardware Additions
T1091 Replication Through Removable Media
T1193 Spearphishing Attachment
T1192 Spearphishing Link
T1194 Spearphishing via Service
T1195 Supply Chain Compromise
T1199 Trusted Relationship
T1078 Valid Accounts
Execution
T1191 CMSTP
T1059 Command-Line Interface
T1223 Compiled HTML File
T1196 Control Panel Items
T1173 Dynamic Data Exchange
T1106 Execution through API
T1129 Execution through Module Load
T1203 Exploitation for Client Execution
T1061 Graphical User Interface
T1118 InstallUtil
Persistence
T1015 Accessibility Features
T1098 Account Manipulation
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1131 Authentication Package
T1197 BITS Jobs
T1067 Bootkit
T1176 Browser Extensions
T1042 Change Default File Association
Privilege Escalation
T1134 Access Token Manipulation
T1015 Accessibility Features
T1182 AppCert DLLs
T1103 AppInit DLLs
T1138 Application Shimming
T1088 Bypass User Account Control
T1038 DLL Search Order Hijacking
T1068 Exploitation for Privilege Escalation
T1181 Extra Window Memory Injection
T1044 File System Permissions Weakness
Defense Evasion
T1134 Access Token Manipulation
T1197 BITS Jobs
T1009 Binary Padding
T1088 Bypass User Account Control
T1191 CMSTP
T1116 Code Signing
T1223 Compiled HTML File
T1109 Component Firmware
T1122 Component Object Model Hijacking
T1196 Control Panel Items
Credential Access
T1098 Account Manipulation
T1110 Brute Force
T1003 Credential Dumping
T1081 Credentials in Files
T1214 Credentials in Registry
T1212 Exploitation for Credential Access
T1187 Forced Authentication
T1179 Hooking
T1056 Input Capture
T1208 Kerberoasting
Discovery
T1087 Account Discovery
T1010 Application Window Discovery
T1217 Browser Bookmark Discovery
T1083 File and Directory Discovery
T1046 Network Service Scanning
T1135 Network Share Discovery
T1040 Network Sniffing
T1201 Password Policy Discovery
T1120 Peripheral Device Discovery
T1069 Permission Groups Discovery
Lateral Movement
T1017 Application Deployment Software
T1175 Distributed Component Object Model
T1210 Exploitation of Remote Services
T1037 Logon Scripts
T1075 Pass the Hash
T1097 Pass the Ticket
T1076 Remote Desktop Protocol
T1105 Remote File Copy
T1021 Remote Services
T1091 Replication Through Removable Media
Collection
T1123 Audio Capture
T1119 Automated Collection
T1115 Clipboard Data
T1074 Data Staged
T1213 Data from Information Repositories
T1005 Data from Local System
T1039 Data from Network Shared Drive
T1025 Data from Removable Media
T1114 Email Collection
T1056 Input Capture
Exfiltration
T1020 Automated Exfiltration
T1002 Data Compressed
T1022 Data Encrypted
T1030 Data Transfer Size Limits
T1048 Exfiltration Over Alternative Protocol
T1041 Exfiltration Over Command and Control Channel
T1011 Exfiltration Over Other Network Medium
T1052 Exfiltration Over Physical Medium
T1029 Scheduled Transfer
Command and Control
T1043 Commonly Used Port
T1092 Communication Through Removable Media
T1090 Connection Proxy
T1094 Custom Command and Control Protocol
T1024 Custom Cryptographic Protocol
T1132 Data Encoding
T1001 Data Obfuscation
T1172 Domain Fronting
T1008 Fallback Channels
T1104 Multi-Stage Channels
Generate Event List
Generate Agent Config
Generate Queries
Generate GPO
Close

```
Get-Command -Module EventList
```

CommandType	Name	Version	Source
Function	Add-EventListConfiguration	2.0.0	EventList
Function	Get-AgentConfigString	2.0.0	EventList
Function	Get-BaselineEventList	2.0.0	EventList
Function	Get-BaselineNameFromDB	2.0.0	EventList
Function	Get-GroupPolicyFromMitreTechniques	2.0.0	EventList
Function	Get-MitreEventList	2.0.0	EventList
Function	Get-SigmaPath	2.0.0	EventList
Function	Get-SigmaQueries	2.0.0	EventList
Function	Get-SigmaSupportedSiemFromDb	2.0.0	EventList
Function	Import-BaselineFromFolder	2.0.0	EventList
Function	Import-YamlCofigurationFromFolder	2.0.0	EventList
Function	Open-EventListGUI	2.0.0	EventList
Function	Remove-AllBaselines	2.0.0	EventList
Function	Remove-AllYamlConfigurations	2.0.0	EventList
Function	Remove-EventListConfiguration	2.0.0	EventList
Function	Remove-OneBaseline	2.0.0	EventList

Contribute to EventList

Are you interested in contributing to EventList...

- ...to improve it?
- ...to implement new features?
- ...to implement cross-platform support?

What are your ideas and suggestions for EventList?

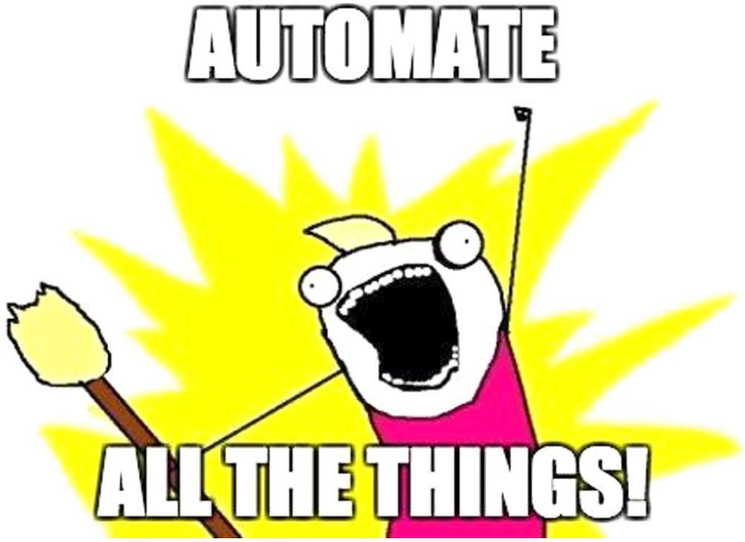
GitHub: https://github.com/miriamxyra/EventList

- Make sure that tests are running without errors
- Create a Pull Request for the „development branch“

Contact me:

- @miriamxyra

- Security Auditing is amazing!
- EventList can help you with that – now with CLI support
- Automate all things! – What's your use case?



Thanks and have fun with EventList!

EventList

https://github.com/miriamxyra/EventList

Follow me on Twitter: **@miriamxyra**