



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



Miriam Wiesner

@miriamxyra

#BHASIA @BLACKHATEVENTS



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

<input type="checkbox"/> File Name	Size
<input type="checkbox"/> LGPO.zip	797 KB
<input type="checkbox"/> Office-2016-baseline.zip	4.5 MB
<input type="checkbox"/> PolicyAnalyzer.zip	1.6 MB
<input type="checkbox"/> Windows 10 Version 1507 Security Baseline.zip	904 KB
<input type="checkbox"/> Windows 10 Version 1511 Security Baseline.zip	902 KB
<input type="checkbox"/> Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB

Microsoft Security Compliance Toolkit
<https://aka.ms/SCT>

Policy Viewer - 178 items

Clipboard View Export Options

Policy Type	Policy Group or Registry Key	Policy Setting	2016_DC_Baseline	2016_MemberServer
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success and Fail...
Audit Policy	Account Management	Computer Account Management	Success	
Audit Policy	Account Management	Other Account Management Events	Success and Fail...	Success and Fail...
Audit Policy	Account Management	Security Group Management	Success and Fail...	Success and Fail...
Audit Policy	Account Management	User Account Management	Success and Fail...	Success and Fail...
Audit Policy	Detailed Tracking	PNP Activity	Success and Fail...	Success and Fail...
Audit Policy	Detailed Tracking	Process Creation	Success and Fail...	Success and Fail...
Audit Policy	DS Access	Directory Services	Success and Fail...	Success and Fail...
Audit Policy	DS Access	Directory Services	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Account Lockout	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Group Membership	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Logoff	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Special Logon	Success and Fail...	Success and Fail...
Audit Policy	Object Access	Removable Storage	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Audit Policy Change	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Authentication Policy	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Authorization Policy	Success and Fail...	Success and Fail...
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	Success and Fail...
Audit Policy	System	IPsec Driver	Success and Fail...	Success and Fail...
Audit Policy	System	Other System Events	Success and Fail...	Success and Fail...
Audit Policy	System	Security State Change	Success and Fail...	Success and Fail...

Policy Path:
 Advanced Audit Policy Configuration
 Audit Policy\Account Logon
 Credential Validation

Credential Validation
This policy setting allows you to audit events generated by validation tests on user account logon credentials.

Event ID	Task Category
4611	Security System Extensibility
4611	Security System Extensibility
5061	System Integrity
4670	Authorization Policy
4670	Authorization Policy
4662	Other Object Access
4670	Authorization Policy
4662	Other Object Access

Keywords Date and Time Source

Audit Success 5/24/2019 7:32:43 PM Microsoft Windows ...

Audit Success 5/24/2019 7:32:42 PM Microsoft Windows ...

Audit Success 5/24/2019 7:32:38 PM Microsoft Windows ...

Audit Success 5/24/2019 7:32:11 PM Microsoft Windows ...

Audit Success 5/24/2019 7:32:08 PM Microsoft Windows ...



1994. 11

1992 11

2002 11

2003 11

2002 11

2001 11

AutoSave Off H ↺ ↻ + - ☰ EventList.xlsxm - Excel Miriam Wiesner MW Share Comments

File Home Insert Draw Page Layout Formulas Data Review View Developer Help Search

Clipboard Font Alignment Protection Number Styles Cells Editing Ideas

A1

Sensitivity: General

EventList by Miriam Wiesner

Welcome to EventList - the Baseline Event Analyzer. This Excel Sheet allows you to import Microsoft Security Baselines.

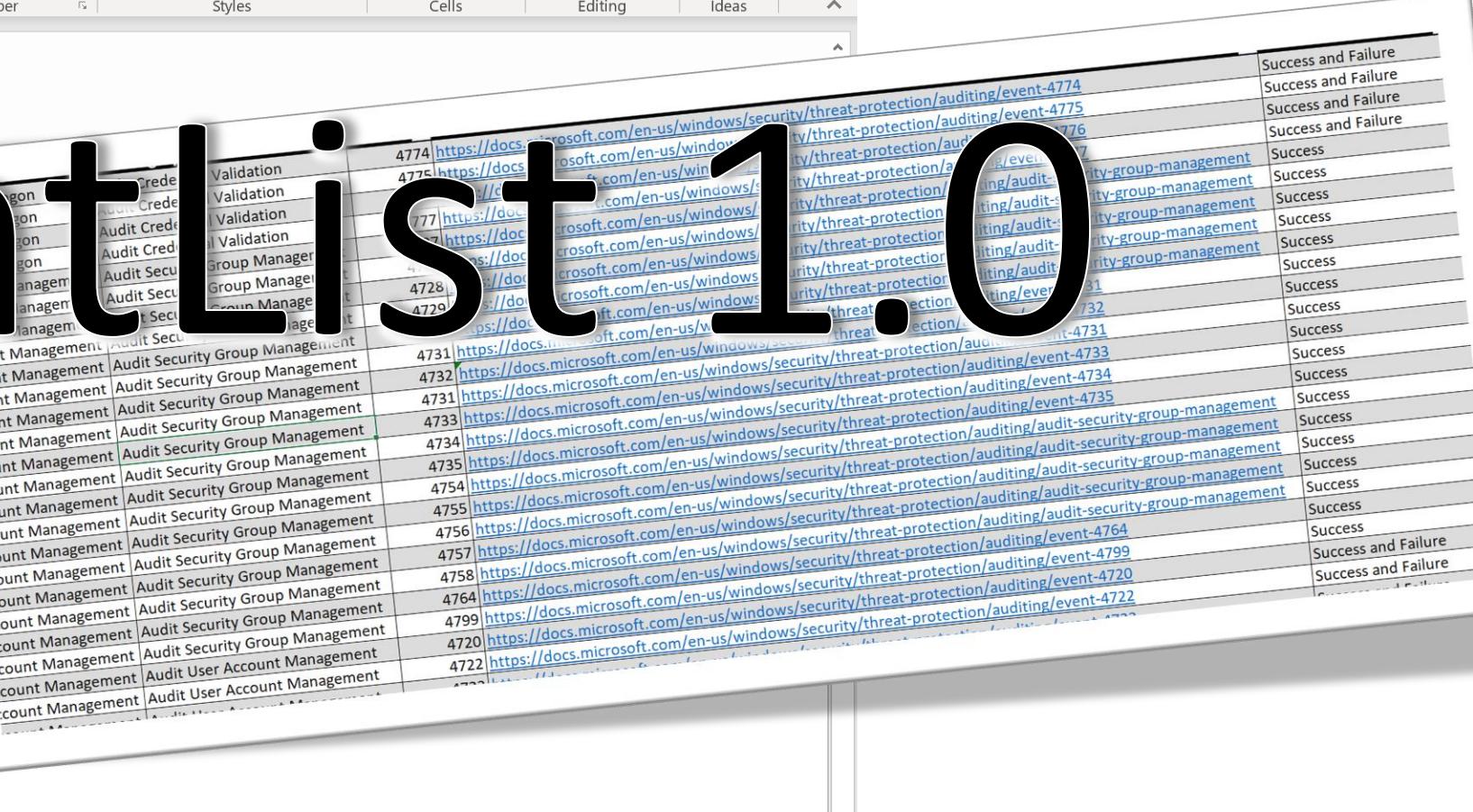
Prerequisites:
Macros must be enabled. All baselines which should be imported have to be located under C:\tmp\ for the import. Baselines are part of the **Security Compliance Toolkit** and can be downloaded from: <https://www.microsoft.com>

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

EventList 1.0



The screenshot shows the Microsoft Excel ribbon at the top with tabs like File, Home, Insert, etc. The main content area displays a large watermark of the word "EventList" and "1.0" in black, semi-transparent font. Below the watermark, there's a table with columns for event ID, URL, and status. The table contains many rows of data, mostly from Microsoft documentation URLs, with most entries marked as "Success".

Event ID	URL	Status
4774	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4774	Success and Failure
4775	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4775	Success and Failure
4776	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4776	Success and Failure
4777	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4777	Success and Failure
4778	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4778	Success and Failure
4779	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4779	Success and Failure
4780	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4780	Success and Failure
4781	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4781	Success and Failure
4782	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4782	Success and Failure
4783	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4783	Success and Failure
4784	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4784	Success and Failure
4785	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4785	Success and Failure
4786	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4786	Success and Failure
4787	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4787	Success and Failure
4788	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4788	Success and Failure
4789	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4789	Success and Failure
4790	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4790	Success and Failure
4791	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4791	Success and Failure
4792	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4792	Success and Failure
4793	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4793	Success and Failure
4794	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4794	Success and Failure
4795	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4795	Success and Failure
4796	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4796	Success and Failure
4797	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4797	Success and Failure
4798	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4798	Success and Failure
4799	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4799	Success and Failure
4800	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4800	Success and Failure

MITRE ATT&CK

Initial Access

Execution

Persistence

Privilege Escalation

Lateral Movement

Exfiltration

Command and Control

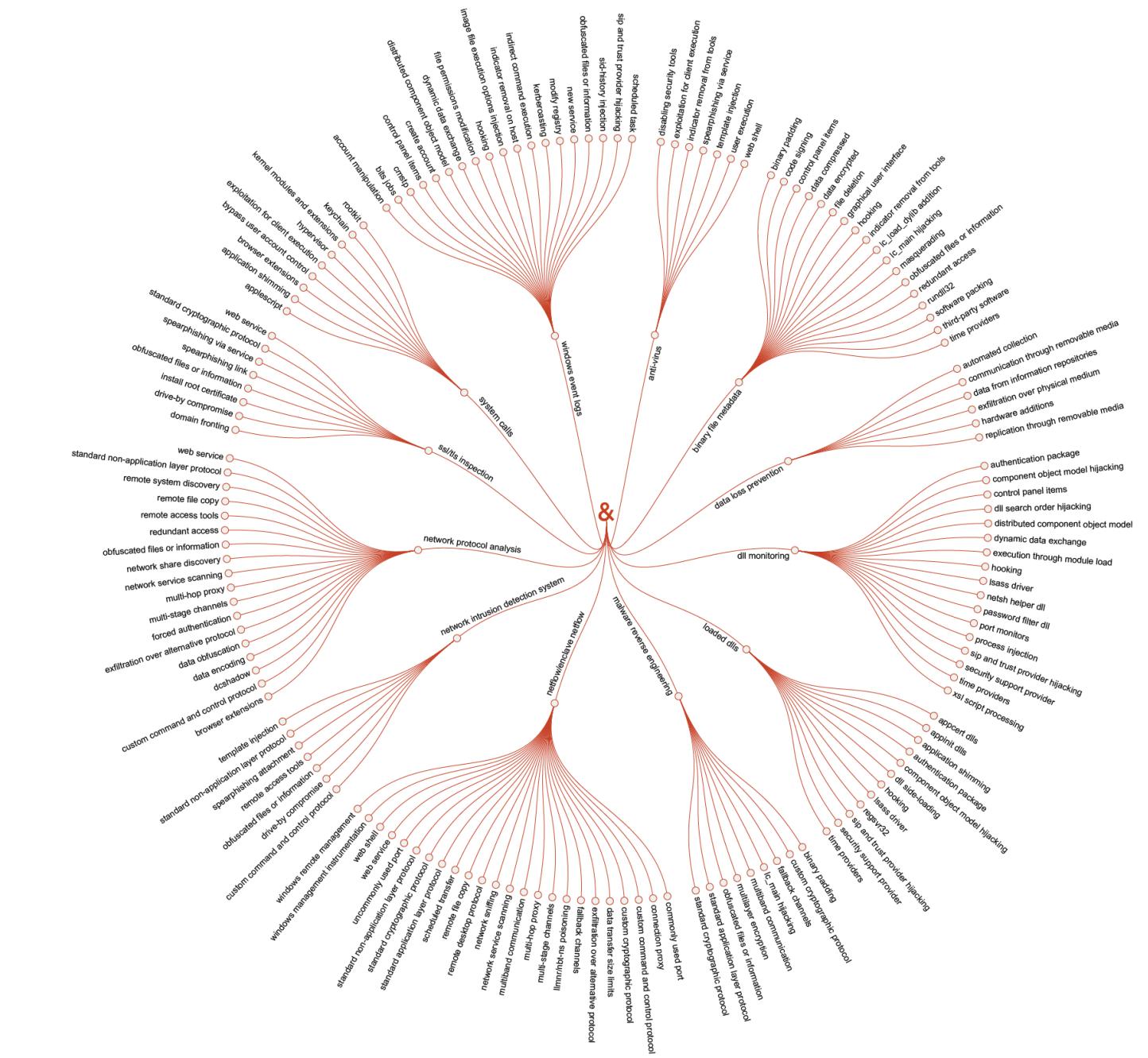
Collection

Impact

Credential Access

Defense Evasion

Discovery



MATRICES

PRE-ATT&CK

Enterprise

All Platforms

Linux

macOS

Windows

Mobile

Home > Matrices > Enterprise

&CK™ Navigator ↗

Enterprise Matrix

The full ATT&CK Matrix

Last Modified: 2019-04-25 20:

Initial Access	Execution
Drive-by Compromise	AppleScript
Exploit Public-Facing Application	CMSTP
External Remote Services	Command-Line Interface
Hardware Additions	Compiled HTML
Replication Through Removable Media	Control Panel Items
Spearphishing Attachment	Dynamic Data Exchange
Spearphishing Link	Execution through API
Spearphishing via Service	Execution through Module Load
Supply Chain Compromise	Exploitation for Client Execution
Trusted Relationship	Graphical User Interface
Valid Accounts	InstallUtil

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]

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 <code>sekurlsa::pth::privilege</code> module can impersonate a user with only a password hash to execute arbitrary commands. ^{[8][9]}

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

Impact

Data Destruction

Data Encrypted for Impact

Defacement

Disk Content Wipe

Disk Structure Wipe

dpoint Denial of Service

Firmware Corruption

bit System Recovery

Work Denial Service

Resource Hijacking

Runtime Data Manipulation

Service Stop

MITRE ATT&CK

Initial Access

Execution

Impact

Persistence

Privilege Escalation

Defense Evasion

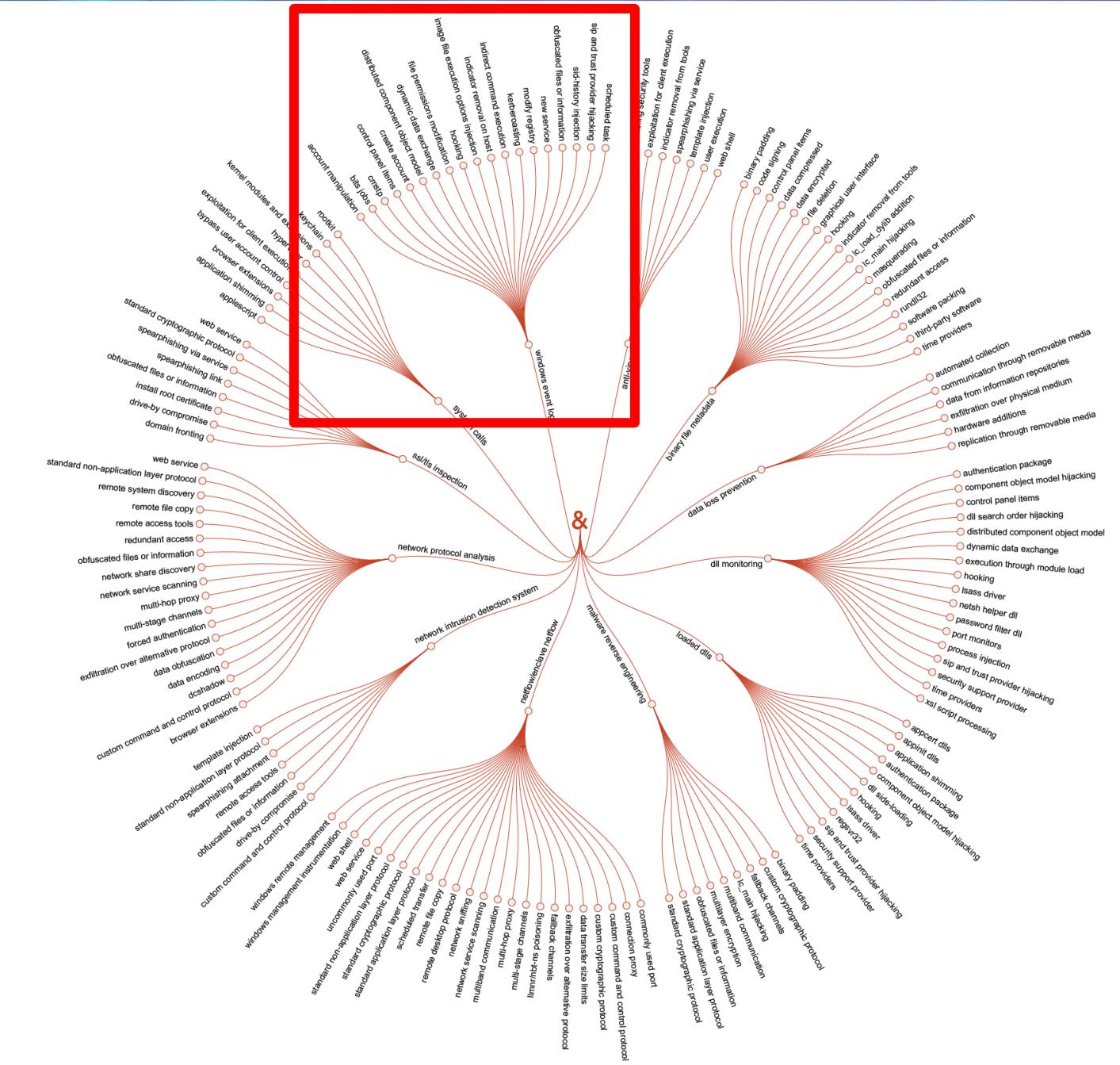
Lateral Movement

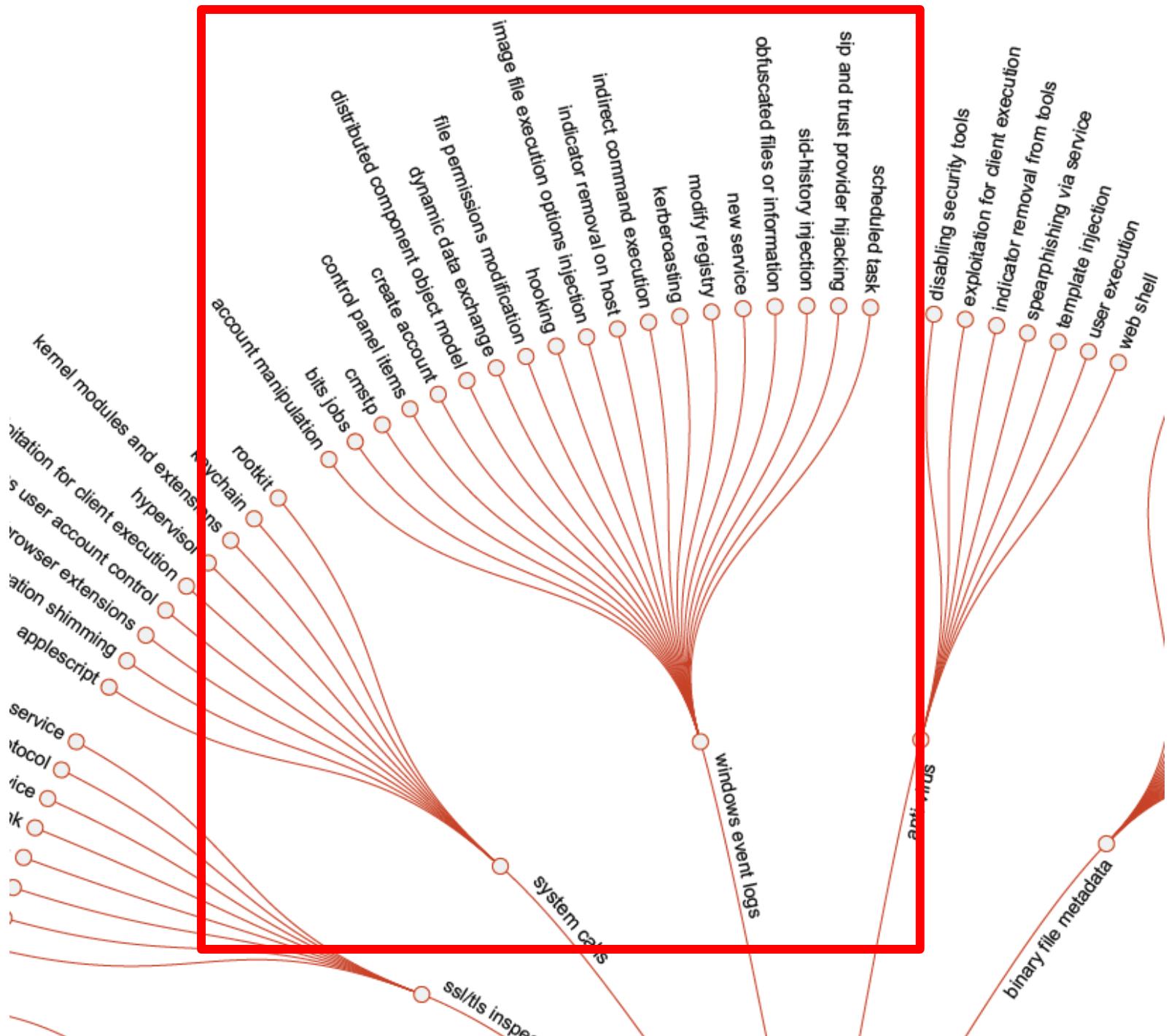
Discovery

Exfiltration

Command and Control

Collection





Hunting queries?

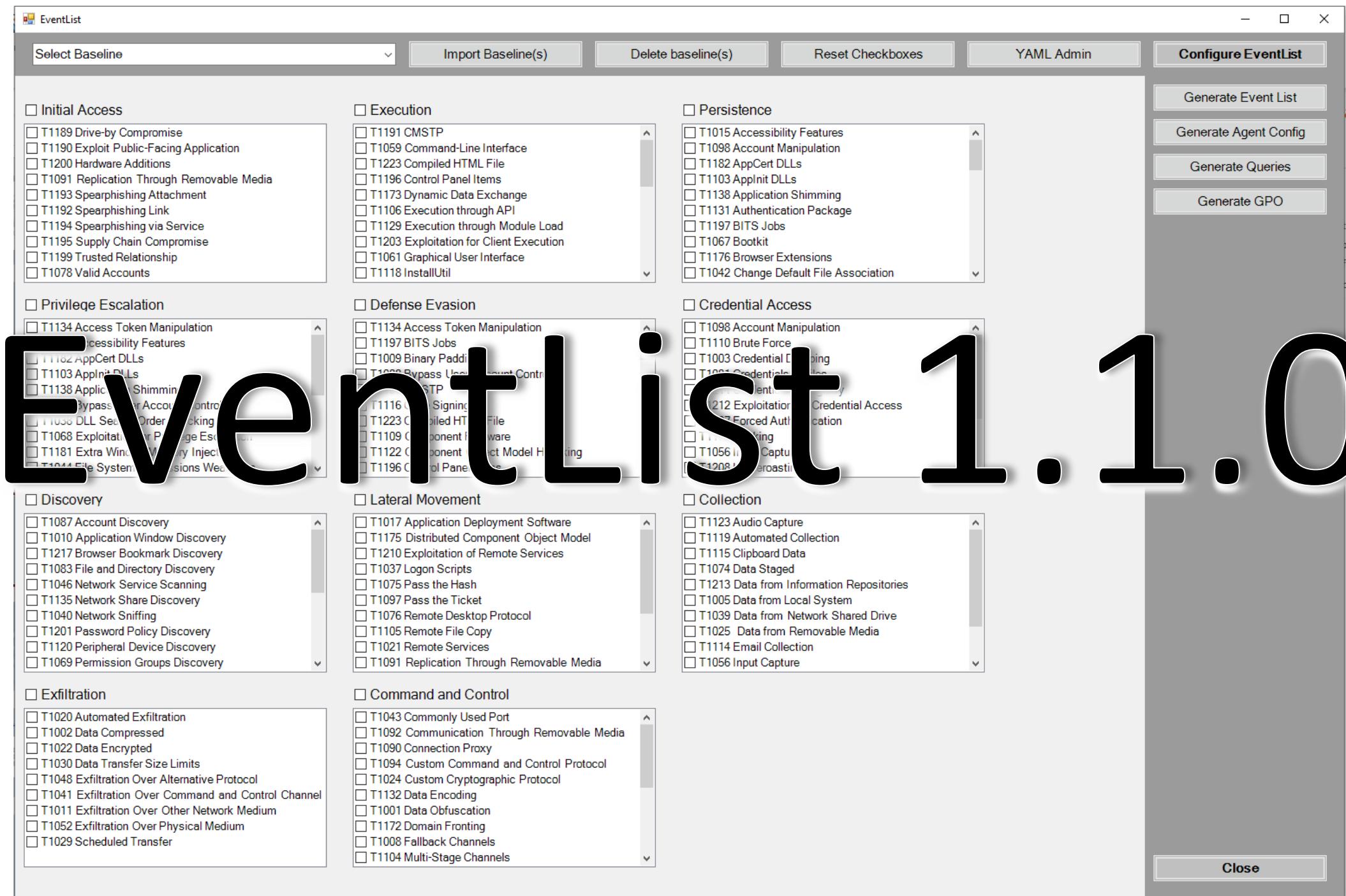


Which events will
be generated?



Which events should
be forwarded?

Eventlist 1.1.0



The screenshot shows the EventList application window. At the top, there's a toolbar with buttons for "Select Baseline", "Import Baseline(s)", "Delete baseline(s)", "Reset Checkboxes", "YAML Admin", and "Configure EventList". To the right of the toolbar is a vertical column of four buttons: "Generate Event List", "Generate Agent Config", "Generate Queries", and "Generate GPO". The main area of the window is divided into several sections, each containing a list of threat actor techniques (T1xx). The sections are:

- 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 Applnt DLLs, T1138 Application Shimming, T1131 Authentication Package, T1197 BITS Jobs, T1067 Bootkit, T1176 Browser Extensions, T1042 Change Default File Association.
- Defense Evasion:** T1134 Access Token Manipulation, T1197 BITS Jobs, T1009 Binary Padding, T1022 Bypass User Control, T1160 Code Signing, T1223 Compiled HTML File, T1109 Component Injection, T1122 Component Object Model Hijacking, T1196 Control Panel.
- Credential Access:** T1098 Account Manipulation, T1110 Brute Force, T1003 Credential Dumping, T1021 Credential Sniffing, T1212 Exploitation of Credential Access, T1177 Forced Authentication, T1111 Impersonation, 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.

At the bottom right of the window is a "Close" button. The background of the application window features large, semi-transparent text elements: "Eventlist" and "1.1.0".





The screenshot shows the Visual Studio Code interface with the following details:

- File Bar:** File, Edit, Selection, View, Go, Run, Terminal, Help.
- Title Bar:** Get-MitreEventList.ps1 - EventList - Visual Studio Code.
- Explorer:** Shows the project structure under EventList, including functions like Get-MitreEventList.ps1, Get-CheckedMitreTechniques.ps1, and Get-EventListConfigSelect.ps1.
- Code Editor:** The main editor pane displays the PowerShell script for Get-MitreEventList.ps1. The script defines a function that gets an EventList for selected MITRE ATT&CK techniques based on checkboxes in a GUI or command-line input. It includes parameters for Identity, generateExcelYsn, and \$tmpStr, and handles both GUI and command-line execution paths.
- Terminal:** A floating terminal window shows the command PS C:\> Get-Command -Module EventList, followed by a table of command details.

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

```
ineByPropertyName = $true)]  
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-YamlConfigurationFromFolder	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>

Administrator: Windows PowerShell

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

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

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

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

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

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

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

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

Configure EventList

- Generate Event List
- Generate Agent Config
- Generate Queries
- Generate GPO

Close

Hunting queries?



Which events should
be forwarded?

Which events will
be generated? ✓



Administrator: Windows Defender Client

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

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

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

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

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

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

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

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 will
be generated? ✓



Which events should
be forwarded? ✓



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](#)

<https://github.com/Neo23x0/sigma>



EventList

PS C:\

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

Privilege Escalation

- T1134 Access Token Manipulation
- T1015 Accessibility Features
- T1182 AppCert DLLs
- T1103 ApnInit 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

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

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

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 ApnInit DLLs
- T1138 Application Shimming
- T1131 Authentication Package
- T1197 BITS Jobs
- T1067 Bootkit
- T1176 Browser Extensions
- T1042 Change Default File Association

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

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

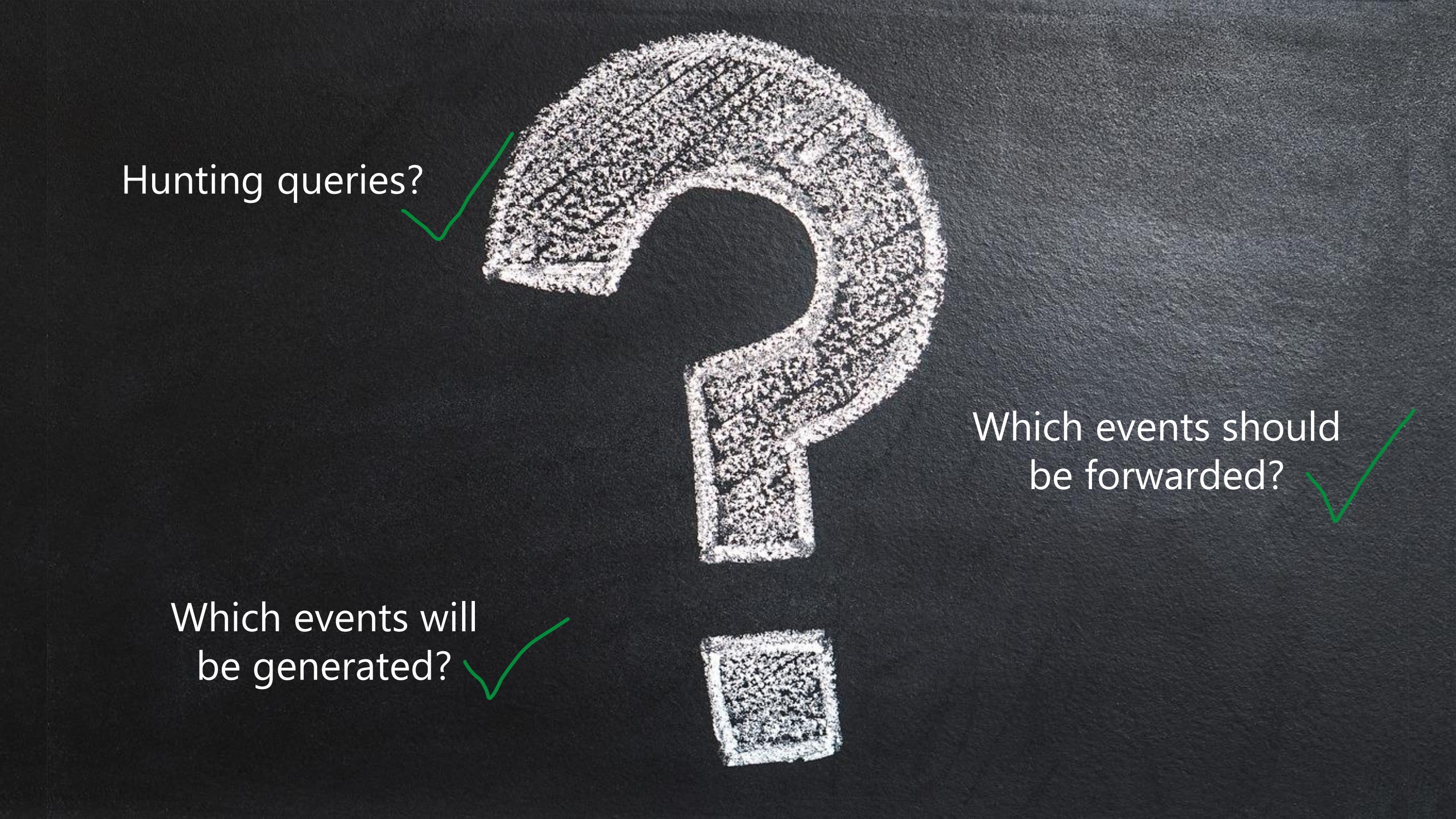
- T1123 Audio Capture
- T1119 Automated Collection
- T1115 Clipboard Data
- T1074 Data Staged
- T1213 Data from Information Repositories
- T1005 Data from Local System
- T1039 Data from Network Shared Drive
- T1025 Data from Removable Media
- T1114 Email Collection
- T1056 Input Capture

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? ✓



Additional
goodies

EventList

PS C:\

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

Privilege Escalation

- T1134 Access Token Manipulation
- T1015 Accessibility Features
- T1182 AppCert DLLs
- T1103 ApnInit 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

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

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

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 ApnInit DLLs
- T1138 Application Shimming
- T1131 Authentication Package
- T1197 BITS Jobs
- T1067 Bootkit
- T1176 Browser Extensions
- T1042 Change Default File Association

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

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

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-YamlConfigurationFromFolder	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?

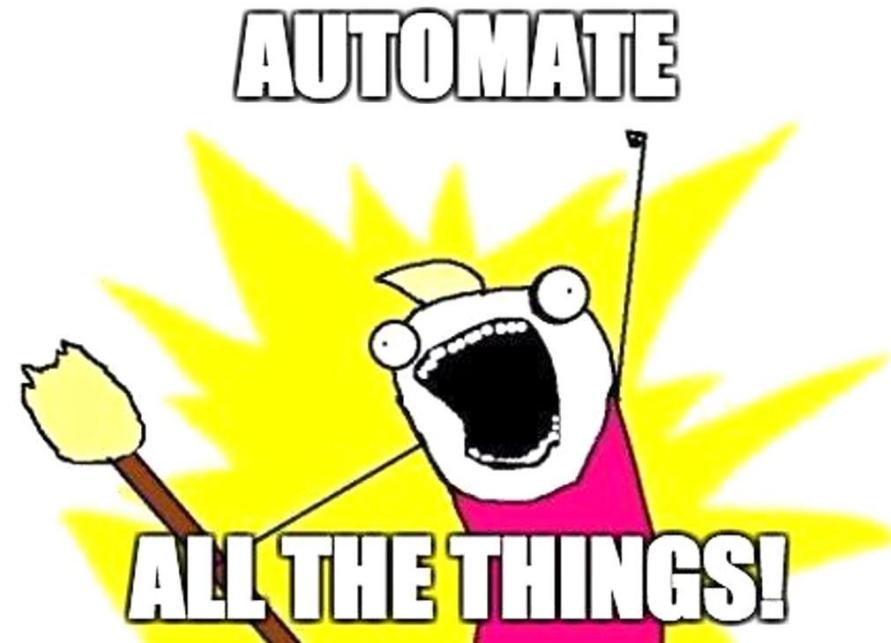
GitHub: <https://github.com/miriamxyra/EventList>

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

Contact me:

- [@miriamxyra](https://twitter.com/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**